Cybercrime Judicial Monitor

Issue 10 – July 2025

Criminal justice across borders

EUROJUST

European Union Agency for Criminal Justice Cooperation

EUROPEAN JUDICIAL CYBERCRIME NETWORK

Executive summary

Eurojust presents the tenth issue of the *Cybercrime Judicial Monitor* (CJM). The CJM is published once per year and distributed to judicial and law enforcement authorities active in the field of combating cyber-dependent and cyber-enabled crimes. It is produced on the basis of information provided by the members of the European Judicial Cybercrime Network (EJCN). All issues of the CJM are available on the Eurojust website.

Last year, a number of legislative developments at the EU, international and national levels were observed. Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (EU Artificial Intelligence Act) entered into force on 1 August 2024 and will be fully applicable on 2 August 2026, with some exceptions. Regulation (EU) 2023/1113 on information accompanying the transfers of funds and certain crypto assets and Regulation (EU) 2023/1114 on markets in crypto-assets (MiCA Regulation) became fully applicable on 30 December 2024. Also in December 2024, the United Nations General Assembly adopted the United Nations Convention against Cybercrime, aimed at strengthening international cooperation in preventing and combating cybercrime and protecting societies from digital threats. The convention will open for signature on 25 October 2025 and stay open until 31 December 2026. Some EU Member States also reported amendments to existing legislation or the introduction of new cybercrime-related offences in their legislation.

Both the Court of Justice of the European Union (CJEU) and the European Court of Human Rights (ECtHR) rendered judgments pertaining to the legality of the use of EncroChat data in criminal proceedings. Also, a number of both EU and non-EU countries reported court rulings on matters relevant to cybercrime and electronic evidence, including the responsibility of administrators of online platforms selling or offering illegal services, cryptocurrencies and remote computer searches.

In the past year, the CJEU further provided additional guidance concerning data retention rules in the Member States. A limited number of countries reported new pieces of legislation and / or court rulings in the area of data retention.

The topic of interest in this tenth issue of the CJM is artificial intelligence (AI). The chapter first takes a closer look at the use of AI for criminal purposes, the ways in which crimes committed through the use of AI can be prosecuted and the responsibility of developers, providers and users of AI systems / general-purpose AI (GPAI) models designed for criminal purposes. It then continues by looking at the use and regulation of AI for the purposes of law enforcement and administration of justice. Finally, it explores some considerations regarding the admissibility of evidence gathered through the use of AI systems / GPAI models.

Contents

1. Introduction 3
2. Legislation 4
2.1. International level 4
2.2. EU level 4
2.3. EU Member States and non-EU countries 7
3. Judicial analysis 14
3.1. Court of Justice of the European Union (CJEU) 14
3.2. European Court of Human Rights (ECtHR) 14
3.3. National court rulings 15
4. Data retention developments 21
4.1. Developments at EU level 21
4.2. Developments at national level 23
5. Topic of interest: artificial intelligence (AI) 26
6. Future of the Cybercrime Judicial Monitor 31

1. Introduction

Eurojust presents the tenth issue of the *Cybercrime Judicial Monitor* (CJM). The CJM is published once per year and distributed to judicial and law enforcement authorities active in the field of preventing and combating cyber-dependent and cyber-enabled crime. All issues of the CJM are also publicly available on the Eurojust website.

The CJM is produced on the basis of information provided by the members of the European Judicial Cybercrime Network (EJCN). Eighteen EJCN members, including fifteen EU and three non-EU countries, replied to this year's questionnaire.

As in previous editions, the CJM consists of three main sections, followed by a section dedicated to a topic of interest. For this tenth issue of the CJM, Eurojust selected artificial intelligence (AI) as the topic of interest.

2. Legislation

The objective of this chapter is to provide information on developments in international, EU and national legal instruments and policies, in particular in relation to cybercrime, electronic evidence (e-evidence) and crypto-assets in 2024 and early 2025. The main sources for the national legislative developments presented in Section 2.3 are contributions collected through the EJCN.

2.1. International level

- *United Nations Convention against Cybercrime*

On 24 December 2024, the United Nations (UN) General Assembly adopted the United Nations Convention against Cybercrime. This treaty is aimed at strengthening international cooperation in preventing and combating cybercrime and protecting societies from digital threats.

The convention defines criminal offences such as illegal access to information and communications technology (ICT) systems, interference with electronic data and ICT systems, cyber-enabled crimes such as ICT-related theft and fraud, and offences related to online child sexual abuse and child sexual exploitation material. It further includes procedural measures for the investigation and prosecution of cybercrime and the collection of electronic evidence, including expedited preservation of stored electronic data, production orders for data, search and seizure of stored electronic data, real-time collection of traffic data and interception of content data. To enhance international cooperation, it sets out, among other things, general principles and procedures for mutual legal assistance, extradition, transfer of sentenced persons and criminal proceedings, and cross-border evidence sharing, while also establishing a 24/7 network of contact points among the States Parties. The convention also promotes technical assistance and capacity building to strengthen national responses to cyber threats while upholding privacy, data protection and due process guarantees.

The convention will be open for signature at a signing ceremony to be held in Hanoi, Viet Nam, on 25 October 2025 and thereafter at the UN Headquarters in New York until 31 December 2026. It will enter into force 90 days after the 40th ratification, acceptance, approval or accession. Following its entry into force, a Conference of the States Parties will be established to oversee the convention's implementation and carry out capacity-building activities.

2.2. EU level

Artificial intelligence

- *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)*

Proposed by the European Commission in April 2021 and agreed by the European Parliament and the Council of the EU in December 2023, Regulation (EU) 2024/1689 (AI Act) entered into force on 1 August 2024. It will be fully applicable on 2 August 2026, with some exceptions ([1]).

([1]) Prohibitions and AI literacy obligations entered into application from 2 February 2025. The governance rules and the

The AI Act sets out a uniform legal framework for the development, marketing and use of AI within the EU, aiming to foster responsible AI innovation while ensuring trustworthiness, safety and fundamental rights compliance. To address the potential risks associated with AI, the act adopts a risk-based approach, classifying AI systems into four risk levels: minimal, limited, high and unacceptable risk. While minimal-risk AI – constituting the vast majority of AI systems currently used in the EU – remains unregulated, high-risk AI must comply with strict transparency and accountability requirements. AI systems posing an unacceptable risk, such as those threatening safety, livelihoods or fundamental rights, are prohibited.

The European AI Office, established in February 2024 within the European Commission, and the national market surveillance authorities are responsible for implementing, supervising and enforcing the AI Act.

Crypto-assets

- *Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets;*
- *Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets (MiCA Regulation); and*
- *Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (DORA)*

Regulation (EU) 2023/1113 on information accompanying the transfers of funds and certain crypto-assets requires crypto-asset-service providers (CASPs) to collect and make available information on the sender and beneficiary of crypto-asset transfers for the purposes of preventing, detecting and investigating money laundering and terrorist financing. Regulation (EU) 2023/1114 on markets in crypto-assets (MiCA Regulation) sets out rules for issuing and trading crypto-assets, as well as for service providers' authorisation, supervision, operation and governance. Both instruments became fully applicable on 30 December 2024. More information about the two legal instruments can be found in Chapter 2 of the previous edition of this report.

The full implementation of the MiCA Regulation is pending completion of the adoption of a number of delegated and implementing acts, as well as guidelines setting out with more specificity how the obligations laid out in the Regulation are to be complied with.

Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA) establishes uniform requirements concerning the security of network and information systems supporting the business processes of financial entities. It aims to ensure that banks, insurance companies, investment firms and other financial entities can withstand, respond to and recover from information and communication technology (ICT) disruptions, such as cyberattacks or system failures. The Regulation applies to a broad range of financial entities, including CASPs authorised under the MiCA Regulation and issuers of asset-referenced tokens.

DORA sets out obligations in areas such as ICT risk management, incident reporting, digital operational resilience testing and oversight of critical third-party providers. It also enables the exchange of cyber threat information and intelligence, including indicators of compromise, tactics, techniques and

obligations for general-purpose AI (GPAI) models will become applicable on 2 August 2025; and the rules for high-risk AI systems will become applicable on 2 August 2027.

procedures, cybersecurity alerts and configuration tools, within trusted communities of financial entities. Public authorities may also participate in these exchanges under defined conditions.

DORA complements the MiCA framework by addressing the operational resilience and cybersecurity of CASPs. It became fully applicable on 17 January 2025.

Cross-border access to data

- *High-Level Group on Access to Data for Effective Law Enforcement*

While it does not constitute a legislative development as such, it is of relevance to note the work of the High-Level Group (HLG) on Access to Data for Effective Law Enforcement, which may lead to legislative developments in the future. The HLG was established by the European Commission in June 2023 to examine the challenges law enforcement practitioners face in accessing data, and to explore potential solutions. Co-chaired by the European Commission and the rotating Presidency of the Council, it aimed to ensure that law enforcement has effective tools to combat crime and enhance public security in the digital age while fully respecting fundamental rights.

The HLG issued 42 recommendations, which were endorsed at the 4th Plenary meeting on 21 May 2024, to support the development of EU policies and legislation to enhance and improve access to data for effective law enforcement. They are structured around three key areas: capacity building, cooperation with industry and standardisation, and legislative measures. The recommendations highlight the difficulties law enforcement faces in accessing data in a readable format due to the lack of harmonised data retention obligations, the growing use of end-to-end encryption and the lack of cooperation by certain non-traditional telecommunications services. The recommendations further call for stronger cooperation between law enforcement and judicial authorities and service providers, as well as legislative obligations ensuring service providers' cooperation while preserving encryption security for users.

Following the recommendations, a Concluding Report was produced to provide further context and outline possible implementation steps. The report was endorsed at the 5th Plenary meeting of the HLG on 15 November 2024 and highlights key challenges law enforcement faces in accessing digital evidence, focusing on digital forensics, data retention and lawful interception. It outlines how encryption, cross-border legal conflicts and technological advances hinder investigations while stressing the need for harmonised data retention rules, improved forensic capabilities and balanced lawful access measures that uphold fundamental rights, cybersecurity and privacy.

The HLG has concluded its work and it is now up to the European Commission, Member States, the European Parliament and all relevant stakeholders to develop measures to address the issue of access to data for effective law enforcement. In this context, the European Commission will prepare a roadmap for the implementation of concrete initiatives by the summer of 2025.

EU Internal Security Strategy

- *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on ProtectEU: a European Internal Security Strategy*

Similarly, while not a legislative development as such, it is also noteworthy that, on 1 April 2025, the European Commission presented ProtectEU: a European Internal Security Strategy, setting out a renewed and comprehensive approach to internal security across the EU. Developed in response to an increasingly complex threat landscape, including hybrid threats, organised crime and digital

criminality, the strategy aims to enhance resilience and cooperation among Member States, while equipping EU institutions and agencies with more effective legal and operational tools.

The Strategy's key objectives include an upgraded EU approach to internal security, anticipating security threats through new ways of sharing intelligence, more effective tools for law enforcement and stronger Justice and Home Affairs Council (JHA) agencies, building resilience against hybrid threats, fighting serious and organised crime, combating terrorism and violent extremism, and establishing the EU as a strong global player on security.

Among other things, the Strategy notes that Eurojust's mandate will be assessed and strengthened to enhance its effectiveness in judicial cooperation and improve cooperation with Europol, including through more proactive support and analysis for Member States' national authorities. In addition, the European Commission announced its intention to propose the signature and conclusion of the new United Nations Convention against Cybercrime.

In follow-up to the HLG recommendations (see above), the European Commission will prepare an EU-level impact assessment on data retention in 2025 with a view to updating rules on data retention at the EU level. It will also present a Technology Roadmap on encryption in 2026 to identify lawful access solutions for law enforcement that safeguard cybersecurity and fundamental rights.

On ransomware, the Strategy highlights that the NIS 2 Directive (Directive (EU) 2022/2555) and the Cyber Resilience Act (Regulation (EU) 2024/2847) will significantly improve the security posture of entities, making it more costly for ransomware networks to carry out their attacks. The Strategy further notes that the European Commission will work closely with Member States to ensure that more ransomware attacks, in particular advanced persistent threats, and ransom payments are reported to law enforcement, facilitating investigations.

The Strategy also emphasises the importance of addressing the financial dimension of organised crime and terrorism by 'following the money'. It highlights the need for close collaboration between the new EU Anti-Money Laundering Authority (AMLA), the EU Anti-Fraud Office (OLAF), the European Public Prosecutor's Office (EPPO), Eurojust and Europol and notes that dismantling the financial incentives behind organised crime requires effective asset seizure and the confiscation of criminal proceeds. The recently adopted, stronger rules on asset recovery and confiscation should be swiftly transposed by Member States and used to their full potential. In addition, combating parallel financial systems that circumvent the EU anti-money laundering framework, including crypto-based systems, requires innovative approaches, the sharing of best practices among Member States and enhanced support from Europol and Eurojust.

2.3. EU Member States and non-EU countries

Country	Summary of the legal provision(s)
Czechia Amendments to the Act on the Right to Digital Services	➢ The Act on the Right to Digital Services was amended, primarily concerning the obligations of providers of 'very large online platforms' and 'very large online search engines'.

Upcoming legislative amendments	➢ Czechia is finalising the enactment of a new Cybersecurity Act to implement the NIS 2 Directive. This legislation will strengthen the role of the National Office for Cybersecurity and introduce two duty regimes for service providers, with a higher regime specifically targeting strategically important services. The text is not yet fully finalised. ➢ An amendment to the Criminal Procedure Code is also foreseen, which will introduce a new definition of key elements in criminal proceedings, including an explicit definition of electronically stored data. The procedure for obtaining such data will also be amended. ➢ Lastly, a new Bill on the Designation of Establishments and Appointment of Representatives for certain providers, aimed at implementing Directive (EU) 2023/1544 on e-evidence in criminal proceedings (E-Evidence Directive), is currently being discussed by the legislative body.
France Law No 2024-449 of 21 May 2024 on Securing and Regulating the Digital Space (SREN Law)	➢ The SREN Law aims to provide a more targeted and appropriate response to offences committed in the digital space, particularly in light of recent technological developments. In this respect, the following changes were introduced. — Article 15 of the SREN Law extended the scope of the offence under Article 226-8 of the French Criminal Code (CC), which penalises the publication of edited content featuring a person's words or image without their consent, to include cases where the content has been generated through algorithmic processing, where the editing is not immediately apparent or where no explicit mention of the modification is made. A new aggravating circumstance applicable to the offences covered by Article 226-8 of the CC also increased the penalties to two years' imprisonment and a EUR 45 000 fine when the publication is made via an online public communication service (including social networks); — Article 226-8-1 of the CC was introduced, creating a new offence of publishing a sexual edit without the person's consent, thereby criminalising the publication of sexual deepfakes; — Article 16 of the SREN Law introduced several measures aimed at enabling the digital banishment of a person suspected to have committed or having committed certain offences online. These measures fall into two categories: (i) an additional penalty involving the suspension of access accounts to the online platform services used to commit the offence, now codified in Article 131-5-1 of the CC; and (ii) a ban on using the access account to the online platform services used to commit the offence, which may be imposed at various stages of the proceedings; and

	— Article 17 of the SREN Law introduced an aggravating circumstance to the offence of blackmail, punishable under Article 312-10 of the CC, when the offence is committed via an online public communication service.
Ordinance No 2024-936 of 15 October 2024 on Crypto-Asset Markets (Ordinance of 15 October 2024) *Entry into force on 30 December 2024 ([2])*	➢ The Ordinance of 15 October 2024 transposed the MiCA Regulation into French law, establishing a legal framework for digital assets and harmonising the regulations governing the activity of virtual-asset-service providers (VASPs) with regard to their obligations to combat money laundering and the financing of terrorism through crypto-assets.
Hungary Amendments to Act XC of 2017 on the Code of Criminal Procedure (CCP) of Hungary *Entry into force on 1 March 2024*	➢ Cryptocurrency-related legislation was amended to facilitate the freezing of cryptocurrencies handled by unreachable or uncooperative providers. Specifically, Section 328, subsection (5) of the CCP grants investigators the right to issue payment orders themselves on behalf of the person concerned to freeze assets, including cryptocurrency held by a provider, if the provider fails to comply with law enforcement requests or is unreachable or unresponsive.
Act XVIII of 2024 (Cyberfraud Act) *Entry into force on 1 August 2024*	➢ The Cyberfraud Act introduced amendments to the CCP, specifically to cybercrime- and digital-evidence-related legal provisions. These amendments aim to improve the effectiveness and timeliness of investigations into online fraud. In this regard, the following changes were introduced. — In Section 21, subsection (5) of the CCP, the former exclusive competence of central district courts and district prosecution offices in cases of crimes against information systems and fraud committed via an information system was removed, meaning that more district courts and prosecution offices can now proceed in these cases under the general rules of competence. This change has been introduced to eliminate the overburden of central district courts and prosecution offices, distribute and balance workload and enhance timeliness and efficiency; and — Section 262, subsection (4) of the CCP now allows investigators to request data from electronic communications providers without prior authorisation from the prosecutor, provided that only subscriber data is requested or that the person concerned has consented to the request (the prosecutor supervising or directing the investigation still retains the right to oversee the legality of evidence collection). The purpose of this amendment is to

([2]) With some exceptions.

	accelerate 'follow the money' investigations and facilitate the reparation of damages suffered by victims.
Latvia Amendments to Criminal Procedure Law *Entry into force on 22 October 2024*	➢ The Criminal Procedure Law was amended to permit the use of machine translation tools for documents, with the exception of testimony, and with a note indicating the use of such translation. A full or partial human translation is required only when deemed necessary by the person directing the proceedings and documents so translated can be used as evidence in criminal proceedings. The amendment is intended to enhance efficiency in criminal proceedings, allowing for the faster and cheaper translation of e-evidence.
Lithuania Law on Cryptocurrency Markets No XIV-2879 of 11 July 2024	➢ The law was adopted, among other legal acts, to implement the MiCA Regulation and Regulation (EU) 2023/1113 on information accompanying transfers of funds and certain crypto-assets (TRF Regulation). The purpose of the law is to ensure the guaranteed, fair, open and efficient functioning of cryptocurrency markets under the MiCA Regulation, the protection of the interests of holders of cryptocurrencies that are not asset-linked tokens or electronic money tokens, holders of asset-linked tokens or electronic money tokens and customers of cryptocurrency-service providers, in order to make the cryptocurrency market stable, reliable, efficient and secure.
Luxembourg Law of 28 February 2024 amending the Penal Code to transpose Directive 2013/40/EU on attacks against information systems (Law of 28 February 2024) *Entry into force on 8 March 2024*	➢ The Law of 28 February 2024 introduced a specific provision criminalising illegal access, illegal data interference, illegal system interference and illegal interception committed against a critical infrastructure information system, in line with the requirements of Article 9(4) of Directive 2013/40/EU. Pursuant to Article 509-4, paragraph 2 of the Penal Code, such offences are punishable by imprisonment for a term ranging from four months to five years and a fine between EUR 1 250 and 30 000.
Law of 24 July 2024 implementing Regulation (EU) 2021/784 on combating the dissemination of terrorist content	➢ The Law of 24 July 2024 implements Regulation (EU) 2021/784, which sets out uniform rules to address the misuse of hosting services for the dissemination to the public of terrorist content online. The law grants the Luxembourg police (*Police Grand-ducale*) the authority to analyse online terrorist content and report such analyses to the Minister of the Interior, who has the competence to issue orders for the removal or disabling of access to such content.

online (Law of 24 July 2024) *Entry into force on 29 July 2024*	➢ Additionally, Article 6 of the law provides for criminal penalties against hosting service providers that: (i) do not comply with orders for removing or disabling access to terrorist content; or (ii) fail to inform promptly the competent authorities about terrorist content involving an imminent threat to life, in accordance with Article 14(5) of Regulation 2021/784. Such offences are punishable by imprisonment for a term ranging from one to five years and / or a fine between EUR 25 000 and 350 000. In case of systematic or persistent failure to remove terrorist content or disable access within one hour of receipt of a removal order, as required by Article 3(3) of Regulation 2021/784, hosting service providers are subject to financial penalties of up to 4 % of their global turnover for the preceding business year.
Malta Act No I of 2024 – Communications Laws (Amendment) Act	➢ The act introduced amendments to Chapter 399 of the Laws of Malta (Electronic Communications Regulation Act), Chapter 418 of the Laws of Malta (Malta Communications Authority Act) and Chapter 426 of the Laws of Malta (Electronic Commerce Act). These amendments primarily focus on the provisions governing infringements under these chapters and the corresponding penalties.
Act No V of 2024 – Criminal Code (Amendment No 2) Act	➢ The act transposed Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography. Of particular relevance is the amendment to Article 346 of the Criminal Code, which now allows the prosecution to present the statement of any minor who is a victim of a sexual offence, as well as that of any vulnerable victim or witness, in court as admissible evidence.
Act No XIV of 2024 – Virtual Financial Assets (Amendment) Act	➢ The act amended Chapter 590 of the Laws of Malta (Virtual Financial Assets Act) to align its provisions with the MiCA Regulation.
Act No XXXVI of 2024 – Markets in Crypto-assets Act	➢ The act introduced Chapter 647 (Markets in Crypto-Assets Act) into the Maltese legal framework, transposing the MiCA Regulation. It establishes a comprehensive regulatory framework for the issuance, trading and oversight of crypto-assets, while setting clear operational standards for CASPs.

Norway Electronic Communications Act of 13 December 2024 *Entry into force on 1 January 2025*	➢ This legislation is based on the previous Electronic Communications Act, with certain relevant additions. Notably, the scope of the act has been broadened to include number-independent person-to-person services. These services are now obliged to provide information about end users and electronic communications. Furthermore, providers are obliged to disclose subscriber information to the police upon request. The act also includes provisions related to data centres.
Slovakia Act No 248/2024 Coll. of 11 September 2024 on Certain Obligations and Powers in the Field of Crypto-Assets and Amending Certain Laws *Entry into force on 1 November 2024 ([3])*	➢ The legislation implements, among others, the MiCA Regulation. The changes were also made in the Slovak Code of Criminal Procedure (CCP) and the Criminal Code (CC). As regards the CCP: — The term 'virtual currency' was replaced by 'crypto-asset'; and — A new Section 96d on the seizure of crypto-assets was introduced, with the most important change being in paragraph 7, which states that: *'The owner of a crypto-asset that has been seized or another person from whom the crypto-asset has been seized has the right to request the cancellation or limitation of the seizure. The presiding judge of the panel and, in the preliminary proceedings, the prosecutor, must decide on such a request without delay. An appeal against this decision is admissible. […]'* As regards the CC: — The term 'virtual currency' was replaced by 'crypto-asset'; and — The definition of 'virtual currency' was deleted.
Slovenia Law on Amendments and Supplements to the Criminal Procedure Act (ZKP-P) *Entry into force on 13 July 2024*	➢ The amendment of the Criminal Procedure Act (ZKP-P) modified the rules for acquiring traffic data. The new legislation sets a maximum period for which traffic data can be retrospectively obtained at six months and introduces shorter time frames for accessing such data in certain cases. Additionally, the standard of proof required to order the disclosure of traffic data has been raised.

([3]) With some exceptions.

Sweden Act (2024:1234) on Independent Forfeiture *Entry into force on 8 November 2024*	➢ Among other things, the act: — Introduces new provisions which allow assets, including cryptocurrency, that are more likely than not to be derived from criminal activity to be forfeited in connection with a conviction for an offence that can generate criminal proceeds; — Permits the forfeiture of assets that are clearly more likely than not to be derived from criminal activity by court decision, even in the absence of a direct link to a specific crime; and — Introduced new provisions regarding the confiscation of criminal tools, enabling a prosecutor to order the confiscation of items that clearly have no lawful use, such as drugs, weapons, explosives or data carriers containing child sexual abuse material (CSAM) files (that cannot be permanently deleted). If there is uncertainty regarding an item's lawful use, a court decision is required.

3. Judicial analysis

The objective of this analytical chapter is to provide insight into judgments related to cybercrime / e-evidence / cryptocurrencies rendered within the EU and at international level. It aims to help practitioners offering relevant case studies and / or comparative analyses. The analyses focus on the most interesting aspects of the cases, rather than covering all issues and arguments addressed by the courts.

This chapter has been created to meet practitioners' demands to get a periodic overview of court rulings in other countries, so that court motivations and justifications regarding the evidence trail could also possibly be used in cybercrime cases in other countries. The analysed judgments have been mainly selected from the court decisions that have been sent to Eurojust on a voluntary basis by practitioners in EU Member States and non-EU countries.

3.1. Court of Justice of the European Union (CJEU)

- **Judgment:** ***M.N. (EncroChat)***

  Case C-670/22

On 30 April 2024, the CJEU issued its judgment in Case C-670/22 – *M.N. (EncroChat),* following questions referred to it by the German Court (Landgericht Berlin) regarding the lawfulness of European Investigation Orders (EIOs) issued by the German public prosecutor's office to obtain EncroChat data from France for use in criminal proceedings.

The CJEU clarified that a public prosecutor can issue an EIO for the transmission of EncroChat data which has been already gathered in the executing Member State, as long as the same conditions apply as in a domestic case. The Court also emphasised that national courts must be able to review EIOs for compliance with the fundamental rights of the persons concerned. Additionally, it ruled that 'interception of telecommunications', pursuant to Article 31 of Directive 2014/41/EU, covers a measure entailing the infiltration of terminal devices for the purpose of gathering traffic, location and communication data from an internet-based communication service, as done by French authorities in the case at stake. Such a measure must be notified in advance to the EU Member State where the target is located, allowing authorities to object or impose conditions.

Finally, the CJEU ruled that information obtained in breach of EU law must only be disregarded if a court finds the EIO unlawful. While the admissibility of evidence is a matter of national law, the rights of the defence and the right to a fair trial should be guaranteed. Therefore, if a defendant cannot review or comment on important information or evidence, obtained through an EIO, and this information and evidence are likely to have a preponderant influence on the findings of fact, the national court must exclude them from the criminal proceedings.

More information about the ruling can be found in Chapter 3 of the previous edition of this report.

3.2. European Court of Human Rights (ECtHR)

On 24 September 2024, the ECtHR issued a decision in the case *A.L. and E.J. v France* concerning the remote retrieval of EncroChat data by French authorities and its subsequent transfer to the United Kingdom (UK) following the issuance of an EIO. The applicants, two British nationals imprisoned in the

UK, challenged the legality of the measures and claimed a violation of their rights under the European Convention on Human Rights (ECHR).

While the ECtHR ultimately ruled the case inadmissible due to the applicants' failure to exhaust domestic remedies in France by which effective challenge could have been brought against the data transfer pursuant to the EIO issued by the UK and against the data retrieval measures carried out by France, it also made a number of relevant findings.

One of the questions at stake in the case concerned whether France had jurisdiction over the applicants' data, considering that the remote retrieval operation had produced part of its effects outside French territory. The ECtHR found that, since the retrieval was conducted by French authorities (i.e. French investigators acting under the authority of French judges and prosecutors) from French territory, the operation was attributable to France. Furthermore, the fact that the EncroChat users located in the UK had been identified only after enforcement of the EIO did not render the transferred data any less personal and did not release France from its obligation to respect the data subjects' rights.

The ECtHR noted that this conclusion was consistent with the CJEU's findings in Case C-670/22 – *M.N. (EncroChat)*, according to which the principle of mutual recognition of judgments and judicial decisions prohibited the authorities having issued an EIO for the transmission of such data as evidence from reviewing the lawfulness of the separate procedure by which the executing Member State had gathered that evidence.

Another issue concerned the question whether the applicants could be recognised as victims under Article 34 of the ECHR, as the data retrieval measure concerned only a specific set of individuals (i.e. EncroChat users) and the applicants had denied having used EncroChat before the UK authorities and did not claim to have been users before the ECtHR. In this regard, the ECtHR held that requiring them to prove that they were EncroChat users would have effectively amounted to self-incrimination and would have constituted a disproportionate obstacle to their rights under the ECHR.

3.3. National court rulings

❖ Czechia

Supreme Court of Czechia – 25 June 2024 (ruling in Czech language)

Background

Under Czech criminal law, the offence of unauthorised access to a computer system and unauthorized interference with a computer system or an information medium requires the circumvention of a security measure. Section 230(1) of the Czech Criminal Code criminalises gaining unauthorised access to a computer system or network by breaching a security measure, even if the system itself is not further damaged or misused.

The case concerned an individual who gained unauthorised access to a computer system by filling in a registration form with false information. The question arose whether a registration form constitutes a true security barrier and whether, therefore, a criminal offence had been committed.

Supreme Court ruling

The Supreme Court held that a registration form does qualify as a security measure, although with a low level of security. What matters is that the very existence of such a security measure makes it clear to the user that he or she is not authorised to access the system or any part of it. By providing false data to obtain access credentials, the accused intentionally circumvented a measure designed to restrict access, satisfying the criteria for unauthorised access under the Criminal Code.

❖ Japan

Supreme Court of Japan – 16 July 2024 (ruling in Japanese language)

Background

Article 246-2 of the Japanese Penal Code criminalizes the act of illegally obtaining a profit by inputting false data to a computer utilised for the business process of another person and this crime is one of the predicate offences of money laundering (violation of the Act on Punishment of Organised Crimes and Control of Proceeds of Crime). In the context of the NEM crypto-asset, participants in the NEM network are only able to conduct transactions by signing off transaction data with a private key linked to their own NEM address. This signature is essential for verifying that the transaction is authorised by the legitimate holder of the private key and thus ensuring the legitimacy of the transaction.

Supreme Court ruling

In this case, the accused received NEM crypto-asset from an unknown person who used an illegally obtained private key for the signature in submitting transaction data to the NEM network in order to execute a crypto-asset transfer from the legitimate holder of the private key. The Supreme Court found that this act by an unknown person constituted the input of 'false data' within the meaning of Article 246-2 of the Japanese Penal Code (computer fraud), because signing off with the private key when submitting transaction data to the NEM network is required in order to confirm that the transaction is carried out by the legitimate holder of the private key.

❖ Netherlands

District Court of Rotterdam – 21 February 2025 (rulings in Dutch language: ECLI:NL:RBROT:2025:2488; ECLI:NL:RBROT:2025:2492; ECLI:NL:RBROT:2025:2515)

Background

The District Court of Rotterdam issued three rulings pertaining to the responsibility of hosting providers (two natural persons and one legal person) accused of complicity in cybercrime by providing servers and Internet Protocol (IP) addresses used to facilitate the Mirai botnet. The botnet was mainly employed for Distributed Denial-of-Service (DDoS) attacks and other malicious activities.

District Court of Rotterdam rulings

In all three cases, the District Court found that the defendants, through their involvement in the distribution of the Mirai botnet, were complicit in computer breach and aiding and abetting the commission of a crime as referred to in Articles 138ab(1), 138b and 139c of the Dutch Criminal Code. The core issue was the defendants' failure to take appropriate action against known misuse of their services, despite having received multiple abuse reports about activities related to the Mirai botnet. The District Court emphasised that hosting providers are responsible for ensuring that their services are not used for cybercrime, as set out in the applicable Code of Conduct. The defendants, in each case, were aware that their infrastructure was being used for illegal purposes, such as hosting the Mirai botnet, and failed to respond to these reports effectively. Therefore, in each instance, the District Court concluded that the defendants had conditional intent to facilitate cybercrime.

Supreme Court of the Netherlands – 18 March 2025

Background

The case involved a complex criminal investigation, including fraud through phishing, commonly known as 'Tikkie fraud', whereby fraudulent payment requests were sent to victims. The investigation involved the seizure and examination of electronic data carriers, in this case smartphones, belonging to the defendants.

An appeal was lodged against the ruling of the Court of Appeal in The Hague on 13 October 2022. Through this ruling, the Supreme Court updated its case-law on the examination of electronic data carriers and automated works in response to the CJEU's ruling in *CG* v *Bezirkshauptmannschaft Landeck* (Landeck judgment).

Conclusions of the Attorney General – 19 November 2024 (conclusions in Dutch language)

The Attorney General assessed the requirements for investigating electronic data carriers and automated works following their lawful seizure in the Dutch legal framework while also considering the Landeck judgment. In this regard, it was noted that the question whether, in case of objects lawfully seized, it also follows from the exercise of that power that the data carriers may be examined without restriction reveals a divergence of views in both case-law and relevant literature. However, after reviewing existing legislation and the Landeck judgment, the Attorney General concluded that a reasonably coherent system can be established. Investigating officers are competent to conduct only a limited investigation of mobile phones, electronic data carriers and automated works. If it is reasonably foreseeable that the investigation will cause more than a limited invasion of privacy, an investigation by the examining magistrate is required. The examining magistrate may also commission investigations by specialised officers, who will operate under the responsibility of the magistrate. The authorisation must specify the scope of the investigation, particularly whether all data stored or available should be examined.

Supreme Court ruling – 18 March 2025 (ruling in Dutch language)

The Supreme Court similarly examined the significance of recent case-law of the CJEU, particularly the Landeck judgment, regarding the requirements for the seizure and subsequent examination of electronic data carriers and automated works, including smartphones, and agreed with the Court of Appeal's earlier findings in the case.

The Court of Appeal had found that when the examination of data from seized electronic data carriers is so intrusive that it can provide a complete picture of an individual's personal life, the mere decision to seize the data does not automatically permit its examination. The examining magistrate must assess whether the data examination should be subject to restrictions, which should be explicitly considered before proceeding. In its reasoning, the Court of Appeal emphasised that factors such as the seriousness of the infringement on the privacy of the data carrier's user, and the proportionality and subsidiarity of the investigative acts, must be considered in determining whether restrictions are needed. These restrictions may include limits on the number of data carriers to be examined, the types of data to be reviewed (such as images, communication and internet behaviour) and the period during which the data was generated or stored. Furthermore, the examining magistrate may opt to phase the investigative acts, with the possibility of extending or further limiting the investigation as it progresses. In the circumstances of the case, there was no indication that such restrictions were properly assessed, making the examination of the seized data unlawful.

❖ Norway

Oslo District Court – 19 April 2024

Background

Norway's National Authority for Investigation and Prosecution of Economic and Environmental Crime requested court approval to secure compensation from a large amount of cryptocurrency previously seized from an unidentified individual. The assets had been moved between different cryptocurrencies and passed through the mixing service Tornado Cash, which is designed to obscure transaction histories. Subsequently, blockchain tracing tools were used to 'demix' the transactions in order to assess whether the assets had likely originated from criminal activity.

Oslo District Court ruling

The Oslo District Court approved the request to secure compensation from the seized cryptocurrency. The court accepted that the demixing analysis provided a sufficient basis to conclude that the assets likely originated from cybercrime targeting foreign victims, even though the funds could not be directly traced back to a specific criminal offence. This decision marked the first time a Norwegian court has ruled on the use of demixing techniques for the purpose of asset recovery.

❖ Portugal

Court of Appeal of Porto – 11 December 2024 (ruling in Portuguese language)

Background

The ruling concerns the extension of searches under Article 19(2) of the Council of Europe Convention on Cybercrime (Budapest Convention). According to the text of the Budapest Convention, extension of searches is allowed only to computer systems in the territory of the respective State. However, the Portuguese Cybercrime Law, which transposes this provision into the national legal framework, removed the territorial limitation. Therefore, according to Portuguese law, the extension of searches is permitted also to computer systems outside the national territory. The ruling concerned the legality of the extension of searches beyond Portugal's borders under Portuguese law and its compatibility with the principles of territoriality and national sovereignty.

Court of Appeal of Porto ruling

The Court of Appeal of Porto held that interpreting Articles 19, 22, and 32 of the Budapest Convention must be done in a modern context, in light of their object and purpose, and taking into account the systematic and teleological elements, as well as the relevant international case-law, in particular the judgments of the Supreme Federal Court of Switzerland (24 May 2017) and the Supreme Court of Norway (29 March 2019 – Tidal Case), both of which are States Parties to the Budapest Convention. It concluded that there is no violation of the principle of territoriality when accessing and receiving computer data stored in the cloud on a server located in a foreign territory when, in accordance with the national legislation, such access is made with credentials that legitimately allow the access to the data by the entity under investigation. Also, such a remote computer search does not infringe the principle of sovereignty of another state.

The Court of Appeal further emphasised that the principle of territoriality, as set out in the Budapest Convention, and the supremacy of international law over national law, do not apply when the computer search to be carried out concerns data from a computer system located in a 'virtual space', the physical location of which is either not known or not relevant due to a country's lack of ratification of the Budapest Convention. Therefore, the evidence obtained from such searches is not considered illegal due to a conflict between international law norms and domestic law provisions.

❖ Sweden

Stockholm Court of Appeal – 5 April 2024

Background

The case concerned the Flugsvamp 3.0 darknet marketplace, a platform used for the illicit sale of narcotics, and its associated chat forum Flugforum. For a period of nearly three years, the marketplace functioned as a hub for the sale and purchase of narcotics using cryptocurrency, specifically Bitcoin. The use of encryption and cryptocurrencies enabled users to trade illicit goods while maintaining anonymity. The main issue in the proceedings was the extent to which the three defendants were involved in the operation and administration of the marketplace and / or the associated forum.

Stockholm Court of Appeal ruling

The Stockholm Court of Appeal confirmed the District Court's assessment that Flugsvamp 3.0 and Flugforum were components of a single criminal enterprise scheme with a common goal, namely the effective sale of illegal narcotics. The Court of Appeal further agreed with the assessment that one defendant had acted as an administrator of both the marketplace and the forum and was therefore responsible for their operation. For this, he was convicted of a particularly serious drug offence. The other two defendants were found to have acted as moderators on Flugforum, which played a key role in supporting the marketplace by enabling communication, negotiation and coordination among users. The Court of Appeal agreed that their involvement contributed significantly to the functioning of the platform and upheld the District Court's findings in this regard. Both defendants were convicted of aiding and abetting particularly serious narcotics offences. The Court of Appeal's conclusions were supported by various forms of electronic evidence, including blockchain analysis linking cryptocurrency transactions to the defendants.

❖ Switzerland

Supreme Court of Switzerland – 6 November 2024 (ruling in German language)

Background

The ruling concerned a case in which IP-log history was obtained from a service provider based in the United States of America (US) by Austrian authorities under Article 32 of the Budapest Convention. The investigation was transferred to Swiss authorities because the suspect resided in Switzerland at the time of the alleged crime. One of the core issues in the case was whether judicial authorisation was required for the collection of traffic data, such as IP logs, under Austrian and Swiss law, and whether this criterion should apply when evidence is collected abroad under the Budapest Convention.

Supreme Court ruling

The Swiss Supreme Court ruled that, in line with both Austrian and Swiss legal frameworks, the collection of traffic data, including IP logs, from abroad must comply with domestic legal requirements, particularly with regard to the need for judicial authorisation. If such authorisation is not obtained, the evidence collected is deemed inadmissible. The Supreme Court further held that these requirements also apply when evidence is collected abroad pursuant to the Budapest Convention.

In the circumstances of the case, the evidence collected from the US-based service provider by Austrian authorities could not be used in Swiss legal proceedings because it had not undergone the necessary judicial authorisation, as required by Swiss law. Therefore, the collected evidence was ruled inadmissible in Switzerland.

Supreme Court of Switzerland – 15 January 2025 (ruling in German language)

Background

The ruling concerned the necessity of informing a person under investigation about their rights, specifically the right to remain silent (*nemo tenetur*), during the execution of a search warrant. In the case, a police officer asked the person under investigation to provide the access code (PIN code) for his mobile phone during a house search, without first informing him of his right to remain silent.

Supreme Court ruling

The Swiss Supreme Court ruled that a police officer is not entitled to request the access code for a mobile phone during a search without first informing the person under investigation of their right to remain silent. The request for the code is not a question which merely serves to facilitate the house search. According to Article 158 of the Swiss Code of Criminal Procedure, the individual must be explicitly informed of their right to refuse to cooperate, including refusing to provide access codes. In the absence of information on this right, it cannot be assumed that the person has voluntarily and validly waived the privilege of self-incrimination.

The Supreme Court emphasised that failure to inform the person of their rights, particularly their right to remain silent, invalidates any subsequent disclosure of the mobile phone access code. As a result, the evidence obtained from the mobile phone, including subsequent evidence based on the code disclosure, is deemed inadmissible.

4. Data retention developments

The objective of this section is to provide an overview of the legislative and / or case-law developments in the EU in the area of data retention, following the ruling of the CJEU in 2014, invalidating the Data Retention Directive (Directive 2006/24/EC) and the subsequent CJEU rulings in relation to data retention. Developments in non-EU countries may also be covered, as relevant.

4.1. Developments at EU level

- **Judgment: *La Quadrature du Net and Others***

  Case C-470/21

On 30 April 2024, the CJEU issued its judgment in Case C-470/21 – *La Quadrature du Net and Others* v *Premier ministre and Others*, following a request for a preliminary ruling from the French Council of State. The case concerned the compatibility with EU law of French legislation requiring the retention of IP addresses and enabling access to associated civil identity data by a public authority combating online copyright offences.

Questions referred

The national court referred three questions to the CJEU:

> *(1) Are the civil identity data corresponding to an IP address included among the traffic and location data to which, in principle, the requirement [of] prior review by a court or an independent administrative entity [whose decisions are binding] applies?*
>
> *(2) If the first question is answered in the affirmative, and having regard to the fact that the data relating to the civil identity of users, including their contact details, are not particularly sensitive data, is Directive [2002/58], read in the light of the [Charter of Fundamental Rights of the European Union (Charter)], to be interpreted as precluding national legislation which provides for the collection of those data, corresponding to the IP addresses of users, by an administrative authority, without prior review by a court or an independent administrative entity [whose decisions are binding]?*
>
> *(3) If the second question is answered in the affirmative, and having regard to the fact that the data relating to civil identity are not particularly sensitive data, that only those data may be collected and they may be collected solely for the purposes of preventing failures to fulfil obligations which have been defined precisely, exhaustively and restrictively by national law, and that the systematic review of access to the data of each user by a court or a third-party administrative entity [whose decisions are binding] would be liable to jeopardise the fulfilment of the public service [mission] entrusted to the administrative authority which collects those data, which is itself independent, does [Directive 2002/58] preclude the review from being performed in an adapted fashion, for example as an automated review, as the case may be under the supervision of a department within the body which offers guarantees of independence and impartiality in relation to the officials who have the task of collecting the data?*

CJEU ruling

The Court clarified that the general and indiscriminate retention of IP addresses by internet access providers, for the purpose of combating criminal offences, does not necessarily amount to a serious interference with fundamental rights. Such retention is permitted if national legislation ensures a clear and effective separation between IP addresses and other categories of personal data, in particular civil identity data, so that no precise conclusions can be drawn about the private life of individuals.

Regarding access to civil identity data associated with IP addresses, the Court held that EU law does not preclude national legislation, allowing competent public authorities to obtain such data for the sole purpose of identifying individuals suspected of having committed a criminal offence. Officials with such access must, however, be prohibited from disclosing information on the content of the files consulted, tracking the clickstream on the basis of IP addresses and using those IP addresses for any purpose other than identifying their holders.

Furthermore, access to civil identity data for the sole purpose of identifying the user concerned may, in principle, take place without prior review by a court or independent administrative body, since the interference entailed by that access cannot be classified as serious. However, if features of the national access procedure – such as the linking of the data and information collected at different stages of the proceedings – may lead to more detailed insights into an individual's private life, and therefore to a serious interference with fundamental rights, then access must be subject to prior review. That review should take place before the linking takes place, while preserving the effectiveness of the procedure. In particular, it should still allow authorities to identify cases where repeated offending may occur.

- **Judgment: *Bezirkshauptmannschaft Landeck***

  Case C-548/21

On 4 October 2024, the CJEU issued its judgment in Case C-548/21 – *CG v Bezirkshauptmannschaft Landeck*, following a request for a preliminary ruling by the Regional Administrative Court in Tyrol, Austria. The case involved the seizure of a mobile telephone during a narcotics investigation and the subsequent attempts by Austrian authorities to unlock that telephone in order to access the data contained therein.

Questions referred

The national court referred three questions to the CJEU:

> *(1) Is Article 15(1) [of Directive 2002/58 – as the case may be, in combination with Article 5 thereof –], read in the light of Articles 7 and 8 of the [Charter], to be interpreted as meaning that [access by public authorities] to data stored on mobile telephones [constitutes an] interference with [the] fundamental rights enshrined in those articles of the Charter which is sufficiently serious to [require] that that access [be] limited, in areas of prevention, investigation, detection and prosecution of criminal offences, to the objective of fighting serious crime?*
>
> *(2) Is Article 15(1) of Directive [2002/58], read in the light of Articles 7, 8 and 11 and Article 52(1) of the [Charter], to be interpreted as meaning that it precludes a national rule, such as that enacted in Paragraph 18 of the [StPO], read in combination with Paragraph 99(1) thereof, which allows security authorities to grant themselves full and uncontrolled access to all digital data stored on a mobile telephone in the course of a criminal investigation without the authorisation of a court or independent administrative body?*
>
> *(3) Is Article 47 of the [Charter], [as the case may be,] read in combination with Articles 41 and 52 thereof, to be interpreted, from the point of view of equality of arms and from the point of view of an effective remedy, as meaning that it precludes a national rule, such as that enacted in Paragraph 18 of the [StPO], read in combination with Paragraph 99(1) thereof, which allows [data stored on a mobile telephone to be exploited] without advising the data subject [of the measure concerned beforehand or, at the very least, after it is taken]?*

The first and second question were reformulated by the Court in light of the provisions of Directive (EU) 2016/680 (Law Enforcement Directive) relevant to the case, recalling that, where the 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/EC (ePrivacy Directive), but by national law only, subject to the application of the Law Enforcement Directive.

The CJEU noted that:

> *[B]y its first and second questions […] the referring court asks, in essence, whether Article 4(1)(c) of Directive 2016/680, read in the light of Articles 7 and 8 of the Charter and Article 52(1) thereof, precludes national legal rules which afford the competent authorities the possibility of accessing data contained in a mobile telephone, for the purposes of preventing, investigating, detecting and prosecuting criminal offences in general, and which do not make reliance on that possibility subject to prior review by a court or an independent administrative body.*

CJEU ruling

At the outset, the CJEU clarified that an attempt by the police to access the data contained in a mobile telephone falls within the scope of the Law Enforcement Directive, even if they do not, for technical reasons, succeed in accessing the data.

As concerns the first and second question, the CJEU held that Article 4(1)(c) of the Law Enforcement Directive, read in the light of Articles 7 and 8 and Article 52(1) of the Charter of Fundamental Rights of the European Union (Charter), does not preclude national legal rules which afford the competent authorities the possibility to access data contained in a mobile telephone for the purposes of the prevention, investigation, detection and prosecution of criminal offences in general, provided that those rules:

- Define with sufficient precision the nature or categories of offences concerned;
- Ensure respect for the principle of proportionality; and
- Make reliance on that possibility, except in duly justified cases of urgency, subject to prior review by a judge or an independent administrative body.

The Court emphasised that any limitation on the rights to privacy and data protection must be necessary and proportionate to the objectives pursued. It stressed that access to data, particularly sensitive data, must be subject to strict conditions, and that the authorities must ensure that any access is limited to what is necessary for the investigation.

As regards the third question, the CJEU held that Articles 13 and 54 of the Law Enforcement Directive, read in the light of Article 47 and Article 52(1) of the Charter, preclude national rules which authorise the competent authorities to attempt to access data contained in a mobile telephone without informing the data subject of the grounds on which the authorisation to access such data, issued by a court or an independent administrative body, is based, once the communication of that information is no longer liable to jeopardise the tasks of those authorities under that directive. This ensures that the data subject has the opportunity to challenge the decision in court if necessary.

4.2. Developments at national level

❖ France

Law No 2024-449 of 21 May 2024 on Securing and Regulating the Digital Space (SREN Law)

The SREN Law, also referred to in Chapter 2.3, introduced a number of legislative changes to fight abuses and illegal behaviour in the digital environment. Some of these provisions address data retention.

Article 46 of the SREN Law provides for the creation of a personal data processing control authority within the French Supreme Court (Court of Cassation). This authority is responsible for controlling personal data processing operations carried out by judicial courts and public prosecutors in the exercise of their jurisdictional functions, and by the Superior Counsel of Magistracy in the exercise of its disciplinary functions.

The supervisory authority for the processing of personal data is incorporated into Article L453-1 of the French Code of Judicial Organisation.

At this stage, this authority does not deal with the storage of and access to data obtained as part of a criminal investigation, but solely with personal data processing operations done by the judicial authorities in the exercise of their functions. The aim is to preserve the independence of the judicial authorities in overseeing their operations of personal data processing. The specific details of this provision will be outlined in a decree to be issued by the Council of State.

At the time of writing of this report, the provisions have not come into force. A decree from the Council of State, required to set the entry into force date, must be issued no later than 31 December 2025.

Court of Cassation, Appeal No 23-81.061, 27 February 2024 (ruling in French language)

In 2024, the French judicial authorities issued a significant ruling regarding access to real-time location data. In a decision handed down on 27 February 2024, the Criminal Division of the French Court of Cassation examined the compliance of Articles 230-32 and subsequent provisions of the French Code of Criminal Procedure concerning real-time geolocation with EU law, as interpreted by the CJEU, which makes access to connection data in the context of criminal investigations subject to prior control by a court or an independent administrative authority. The ruling clarified the conditions under which judicial authorities can access connection data in the context of criminal investigations.

With this ruling, the Court of Cassation made a procedural distinction based on the purpose of the real-time geolocation measure. The geolocation of a vehicle does not fall within the scope of the ePrivacy Directive (as amended by Directive 2009/136/EC), as this directive applies only to operators of publicly accessible electronic communications services. However, as regards the geolocation of a telephone line, it can be inferred from Article 15 of the ePrivacy Directive (as amended by Directive 2009/136/EC and interpreted in light of Articles 7, 8 and 11, and 52(1) of the Charter) that Articles 230-32 and 230-33 of the French Code of Criminal Procedure are contrary to EU law. These provisions authorise the public prosecutor to order the geolocation of a telephone line and grant investigators real-time access to the line's location data without prior review by a court or independent administrative body. Nevertheless, as per the CJEU's ruling of 12 July 2022 on access to traffic and location data in the context of criminal investigations, the nullity of the measure is conditional upon the demonstration of a grievance.

❖ Luxembourg

The Bill of Law No 8148 on the retention of personal data, referred to in the previous edition of the CJM, is still under debate in Parliament.

❖ Norway

Electronic Communication Act of 13 December 2024

A recast of the Electronic Communication Act was enacted in 2024. The existing retention regime for the link between IP addresses and subscribers remains unchanged in this new legislation.

Section 3-13 titled 'Obligation to store public IP addresses' provides as follows:

The provider of electronic communications networks used for public electronic communications services and the provider of such services shall store, for the purposes of serious crime investigation, the information necessary to identify the subscribers on the basis of:

a. public IP address and a time of communication; or

b. public IP address, a time of communication and port number used in communication, if the same public IP address is assigned to multiple subscribers at the same time.

Destination information should not be stored.

Data shall be stored for 12 months from the date of termination of communication.

❖ Portugal

Law No 18/2024 of 5 February 2024

The legal framework on data retention was amended in 2024 following a ruling of the Portuguese Constitutional Court, which found the previous data retention regime (Law No 32/2008, transposing the Data Retention Directive) to be unconstitutional.

The new law, Law No 18/2024 of 5 February 2024, amended the former provisions to align with the guidance provided by the jurisprudence of the Constitutional Court. Under this revised framework, the data retention regime for billing purposes, established by Law No 41/2004 of 18 August 2004, remains in force. This law transposes the ePrivacy Directive and provides for the storage of such data for six months, in line with Article 6 of the Directive. The Prosecution Service is permitted to access this type of data within the context of a criminal investigation, pursuant to Article 14 of the Cybercrime Law (Law No 109/2009 of 15 September 2009).

In addition, a separate regime for the general retention of subscriber data was introduced (Article 6(1) of Law No 32/2008, as amended by Law No 18/2024). This regime extends the data retention period for such data from six months to one year. However, access to such data requires a reasoned order from an investigative judge and can only be authorised if there are reasons to believe that it is indispensable for discovering the truth or that the evidence would otherwise be impossible or very difficult to obtain. Furthermore, such access is only permitted within the scope of the investigation, detection and prosecution of serious crimes.

Finally, the new framework introduced a special procedure, outside the scope of criminal proceedings, for the selective retention of traffic and location data. This special procedure requires a reasoned decision by the Portuguese Supreme Court and must respect the principles of necessity and proportionality. It applies only to future data.

5. Topic of interest: artificial intelligence (AI)

Introduction

Artificial intelligence (AI) is increasingly shaping various aspects of society, including the criminal justice sector. AI systems ([4]) and general-purpose AI models (GPAI models) ([5]) can offer significant possibilities for enhancing law enforcement capabilities and the administration of justice, provided they are used responsibly, while respecting all applicable legal requirements, including those pertaining to data protection. AI tools can, however, also be leveraged for illegitimate purposes, and law enforcement and judicial authorities in the EU and beyond are increasingly facing new challenges in investigating AI-enabled crimes.

Given the advances in AI development, the EU adopted the AI Act, which entered into force on 1 August 2024 and will be fully applicable on 2 August 2026 ([6]). The AI Act sets out a uniform legal framework for the development, marketing and use of AI within the EU, including certain rules and exceptions regarding the use of AI for law enforcement purposes ([7]). However, many areas remain unaddressed by legislation at both the EU and national levels, including practical aspects concerning AI deployment for the purposes of law enforcement and administration of justice. Further, crimes committed with or through AI are subject to various forms of regulation under the existing legal frameworks and may require the further development of legislation to address upcoming challenges.

This section explores how different EU Member States and non-EU countries address the criminal use of AI and how they deal with the liability of developers, providers and users of AI systems / GPAI models designed specifically for criminal purposes. It further examines existing or emerging practices and legal frameworks pertaining to the use of AI for law enforcement purposes and in connection with the administration of justice. Last but not least, it briefly delves into considerations regarding the admissibility of evidence gathered by AI systems / GPAI models.

The information presented is based on responses gathered through a questionnaire distributed to experts of the EJCN. In total, replies from EJCN members from 18 countries were received, including three non-EU countries (Japan, Norway and Switzerland).

Criminal use of AI systems / GPAI models

Based on the responses received from the EJCN members, it can be noticed that national legislative approaches to addressing the criminal use of AI systems / GPAI models differ.

None of the respondents reported having **specific legislation** in place in their country directly addressing the criminal use of AI systems / GPAI models. The only exception is the criminal use of deepfake technology and AI-generated misinformation, which is further discussed below. Instead, countries rely on **general substantive laws** for prosecuting crimes involving the use of AI. Depending

([4]) For the purposes of this report, 'AI system' means a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations or decisions that can influence physical or virtual environments (see Article 3(1) of the AI Act).

([5]) For the purposes of this report, 'GPAI model' means an AI model, including where such an AI model is trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable of competently performing a wide range of distinct tasks regardless of the way the model is placed on the market, and that can be integrated into a variety of downstream systems or applications [...] (see Article 3(63) of the AI Act).

([6]) For more information on the AI Act, see Chapter 2 of this report.

([7]) For the purposes of this report, 'law enforcement' means activities carried out by law enforcement authorities or on their behalf for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including safeguarding against and preventing threats to public security (see Article 3(46) of the AI Act).

on the purpose for which AI is employed, this may entail the application of provisions regarding computer misuse, fraud, defamation and other relevant offences. However, a small number of respondents indicated that the need to more specifically legislate the criminal use of AI is currently under consideration in their country.

As regards the **need for the adoption of legislation addressing the criminal use of AI systems / GPAI models**, the majority of respondents expressed support for the adoption of legislation addressing specifically the use of AI systems / GPAI models for criminal purposes. However, some respondents indicated that the existing, technology-neutral legislation is sufficient and does not require further adaptation. It was also pointed out that AI systems / GPAI models are constantly evolving and can be used for an unknown number of different purposes, which may make the adoption of national legislation on the matter difficult.

One way in which AI systems / GPAI models can be deployed for criminal purposes is through the **creation of deepfakes and AI-generated misinformation**. With regard to this matter, national legislative approaches vary significantly. In France, the legislation has been adapted to introduce specific criminal offences addressing the dissemination of false information through deepfakes, particularly when such content is designed to appear credible and deceive the public. Additionally, the publication of non-consensual sexual deepfakes has been criminalised and the definition of illegal image editing expanded to include algorithmically generated content that is not clearly identified as such. France has also revised existing legislation aimed at preventing foreign interference by establishing the use of deepfakes for certain crimes or offences – when committed to serve the interests of a foreign power or under foreign influence – as an aggravating circumstance. Latvia has also specifically criminalised influencing the electoral process using deepfake technology, such as by deliberately creating or disseminating false information about a political party or candidate.

Many countries, however, do not have specific legal provisions in this regard. In these cases, crimes involving the creation of deepfakes and AI-generated misinformation are generally prosecuted under existing laws, such as those concerning the misuse of computer systems or identity fraud / identity theft, depending on the circumstances of the case. In at least one Member State, discussions on the matter are still ongoing.

In addition to defining the crimes which may be committed through the use of AI systems / GPAI models, another key issue is the **attribution of criminal responsibility to the developers, providers and users of AI systems / GPAI models designed for illegal purposes** (i.e. with the purpose of **facilitating criminal activities**). This would include, for instance, a large language model (LLM) ([8]) designed without ethical safeguards, which could be employed by cybercriminals to generate, for example, phishing emails and malware code, and to evade spam filters or an AI-powered password-cracking tool.

Regarding the **criminal responsibility of developers** of such AI systems / GPAI models, the legal approaches vary among the countries surveyed. Criminal responsibility may also depend on the provider's involvement in the system or model's creation and the technical specificities of the AI system / GPAI model. In some countries, persons may be held responsible for the production of a device – including software – primarily designed or adapted for committing offences established under the Budapest Convention ([9]), or for providing tools intended to facilitate cybercrime more broadly, which would therefore include AI systems / GPAI models designed for criminal purposes.

In other countries, developers may be held responsible as accessories to a crime, such as aiders and abettors or accomplices. In one Member State, the requirement of double intent may apply – regarding both the developer's own conduct and the conduct of the primary perpetrator. Overall, the attribution

([8]) For the purposes of this report, an LLM means a GPAI model trained on vast amounts of text data to generate, comprehend and manipulate human language for various applications, including text generation, translation and summarisation (e.g. ChatGPT, Gemini).
([9]) See Budapest Convention, Articles 2–10.

of responsibility depends heavily on the specific circumstances of the case. In several countries, the mere act of developing an AI system / GPAI model – even if intended for criminal purposes – may not, on its own, be sufficient to warrant prosecution. Rather, responsibility may arise based on the developer's subsequent actions, whether as a direct perpetrator or as an accessory to a particular crime.

Regarding the **criminal responsibility of providers** of AI systems / GPAI models designed for criminal purposes, such as those hosting or distributing the systems/models, similar considerations apply as for developers. In some countries, in addition to criminalising the production of devices, including software, primarily designed or adapted for the commission of offences established in accordance with the Budapest Convention, the legislation also criminalises the sale, procurement for use, import, distribution or any other form of making such devices available. As such, providers of AI systems / GPAI models designed for criminal purposes already fall within the scope of existing legislation. The key challenge, however, lies in establishing intent – specifically, demonstrating that the provider was aware of the criminal use of their service. Responsibility may also arise where the provider is found to have contributed to the commission of an offence, which similarly requires prior knowledge of the intended illicit use of the AI system / GPAI model.

In France, a new offence targeting, under certain circumstances, the administration of online platforms that knowingly enable the transfer of illegal products, services or content was introduced in 2023. By broadly interpreting the term 'provider', responsibility could extend to administrators of platforms knowingly facilitating the distribution of AI systems / GPAI models designed for criminal purposes, such as those intended for generating CSAM, if they are considered manifestly illegal products or services.

In other countries, providers may be held responsible as accessories to a crime, which may typically imply certain requirements concerning the establishment of intent. As in the case of developers, providers' liability may also depend on the extent of their involvement in the preparation of the offence and the technical characteristics of the AI system / GPAI model.

The **criminal responsibility of users** of AI systems / GPAI models designed for criminal purposes has been widely acknowledged across the countries surveyed. In general, users who employ AI technologies for illegal activities can be prosecuted under national laws related to the different types of crimes committed or attempted through the use of AI. The establishment of their responsibility would generally depend on the specifics of the case, such as the user's intent and their awareness of the illegal nature of their actions. Furthermore, several countries specifically indicated that the mere possession or non-criminal use of such an AI system / GPAI model would not, in itself, constitute a criminal offence.

Across the responses, a common theme appears to emerge. While there is broad agreement that developers, providers and users should be held responsible for their particular roles with regard to AI systems / GPAI models designed for criminal purposes, the legal frameworks currently in place – and perhaps even more so their practical application – differ.

Use of AI systems / GPAI models for law enforcement purposes

As also recognised by the AI Act, the **responsible use of AI for law enforcement purposes** can enhance authorities' ability to prevent, investigate, detect and prosecute criminal offences more efficiently while upholding fundamental rights. Based on the responses received, it appears that several countries have already implemented AI tools for these purposes, while others are in the early stages of development or are conducting pilot projects in this regard. The systems deployed are often adapted from commercial tools, although some have been specifically designed to meet law enforcement needs.

Examples of AI systems / GPAI models currently in use or under development include tools primarily intended to enhance investigative work by automating routine tasks, speeding up data processing and

improving analytical capabilities. Applications are being used for tasks such as transcription, language processing, video analysis, analysing protocol recognition and the management of large datasets relevant to criminal investigations. In one non-EU country, AI is also being used – albeit on a limited scale and often within scientific research settings – for tasks such as LLM-assisted transcription and translation during interrogations, and the identification of individuals in CSAM using machine vision. While AI-assisted translations have not yet replaced official translations, they may help identify relevant sections to be translated by authorised translators in large volumes of text. Overall, these technologies aim to assist law enforcement authorities in managing complex information more efficiently and effectively throughout the investigative process.

As regards the **regulation of the use of AI systems / GPAI models for law enforcement purposes**, it appears that many of the countries surveyed have not established a dedicated legal framework or guidelines for such use. In these cases, the **use of AI must comply with existing legal provisions**, particularly those related to information technology, data protection and privacy. One non-EU country reported having internal guidelines for the use of publicly available AI services. Meanwhile, in 2024 Lithuania adopted a resolution outlining principles for the use of AI technologies in the public sector, emphasising that only the proper use of such tools can ensure the full protection of human rights and freedoms, as well as economic and national security interests, in line with the then-forthcoming AI Act.

The question **whether the adoption of a legal framework or guidelines for the use of AI systems / GPAI models for law enforcement purposes would be necessary** has received mixed responses. Some respondents see the need for binding legislation, some favour non-binding guidelines, while others believe existing laws are currently sufficient.

Two respondents provided particularly comprehensive positions. One emphasised that the adoption of a legal framework regulating AI use for law enforcement purposes is essential to safeguard fundamental rights, including the right to privacy, data protection, and non-discrimination, as well as to ensure public trust. Such a framework would help establish clear and practical rules for practitioners, including the conditions under which AI tools may be used, and would require the use of auditable and explainable systems to avoid reliance on opaque technologies. It would also help ensure clarity and consistency in the use of AI-generated data, reducing the risk of legal challenges to its admissibility. The other respondent stressed that any such framework must balance legal and ethical safeguards with the operational flexibility needed to effectively respond to increasingly complex and technologically advanced criminal threats. Both respondents highlighted the risks associated with the misuse of AI, noting that it can enable manipulative or abusive practices if not properly regulated.

Overall, while there are positive steps being made towards the integration of AI systems / GPAI models into law enforcement, variations remain across the different countries surveyed regarding the types of AI used, their specific applications and the regulatory frameworks supporting their deployment. Further guidelines and frameworks are expected to emerge as the use of AI for law enforcement purposes continues to evolve.

Use of AI systems / GPAI models for the purposes of administration of justice

Responses from the countries surveyed show that, as of now, the integration of AI systems / GPAI models into the justice system is still in its early stages. Most countries have not yet adopted specific legal frameworks or guidelines governing the use of AI for the administration of justice. Several countries, however, indicated that discussions and exploratory efforts are under way, which may reflect a growing interest in the area.

Regarding specific examples of use, one non-EU country indicated that courts have been piloting LLM-assisted transcription of proceedings, in accordance with internal assessments and guidelines. The Netherlands reported that AI was used in a criminal case as a supporting language tool to assist in drafting a criminal judgment. It was emphasised that AI was not used to assist in the judicial decision-

making itself. Latvia highlighted a new provision introduced into its criminal procedural law in late 2024 allowing the use of machine translation tools in criminal proceedings. Under this provision, documents that do not contain testimony may be translated using automated tools, with human translation required only when deemed necessary by the authority conducting the proceedings.

Considerations regarding the admissibility of evidence gathered through the use of AI systems / GPAI models

A consensus emerged across the countries surveyed: there are no specific legal barriers that inherently prevent the use of evidence gathered using AI systems / GPAI models in criminal proceedings. In most cases, evidence gathered through the use of AI is or would be subject to the same legal standards as other forms of evidence, including requirements related to relevance, reliability and the chain of custody. The principle of free assessment of evidence often applies, allowing courts to evaluate the weight and credibility of any type of evidence, regardless of the manner in which it was obtained, on a case-by-case basis. Specific concerns raised include the need for human oversight to verify AI-generated conclusions, the risks associated with potential biased or discriminatory outputs and the importance of ensuring that AI systems / GPAI models do not compromise the integrity of the evidence. Additional considerations involve the transparency of the algorithms used, the explainability of their outputs in court and compliance with data protection rules, particularly when personal data is being processed. As the case-law will inevitably evolve, future court decisions will likely play a critical role in shaping the legal frameworks governing the admissibility and use of AI-generated evidence.

Conclusion

Overall, the way in which different countries address the use of AI for criminal purposes and the criminal responsibility of developers, providers and users of AI systems / GPAI models designed for criminal purposes varies. With the exception of specific provisions related to the criminal use of deepfake technology and AI-generated misinformation, none of the countries surveyed have laws that specifically address the particularities of AI-related crimes. Instead, they rely on general legal provisions and technology-neutral legislation. Depending on the circumstances of a case, provisions on offences such as computer misuse, fraud and identity theft may apply. Countries are also divided on whether more specific legislation addressing the criminal use of AI would be required. While some respondents referred to the need for a tailored approach that takes into account the characteristics of AI technologies and the various entities involved in their deployment, others are of the view that existing laws currently suffice. The attribution of criminal responsibility to developers, providers and users of AI systems / GPAI models designed for criminal purposes also remains a complex issue and will often depend on intent and the technical characteristics of the system.

The use of AI systems / GPAI models for law enforcement and administration of justice purposes is progressing, although it remains at an early stage in many countries. While several applications of AI have already been deployed to support investigative work and administrative tasks, others are still in development or limited to pilot projects. Regulatory approaches differ, with many countries relying on existing legal frameworks, such as ones relating to information technology and data protection, while some countries are engaged in ongoing discussions on the adoption of dedicated guidelines or legislation. The question whether specific legal frameworks are needed has also elicited mixed opinions.

Finally, while no specific legal barriers were identified concerning the admissibility of evidence gathered through the use of AI systems / GPAI models, the importance of compliance with general evidentiary standards has been emphasised and future case-law is expected to further clarify the applicable legal frameworks.

6. Future of the Cybercrime Judicial Monitor

The CJM is produced once per year and reports mainly on information related to the previous year. The CJM is published on the Eurojust website and distributed to judicial and law enforcement authorities active in the cybercrime domain.

The focus of future issues of the CJM will largely remain on legislative developments in the area of cybercrime, data retention and e-evidence, and the assessment of certain relevant court decisions. Each issue's topic of interest will be determined based on ongoing or emerging trends.

The CJM is mainly based on input from practitioners, and this will continue to be the case for future issues of the CJM. We thank the experts of the EJCN who have contributed to this issue of the CJM.

Eurojust, Johan de Wittlaan 9, 2517 JR The Hague, The Netherlands
www.eurojust.europa.eu • info@eurojust.europa.eu • +31 70 412 5000
Follow Eurojust on X, LinkedIn and YouTube @Eurojust

Catalogue number: QP-01-25-007-EN-N • ISBN: 978-92-9404-407-5 • ISSN: 2600-0113 • DOI: 10.2812/8276156

Eurojust is an agency of the European Union