EUROJUST

EUROPEAN JUDICIAL CYBERCRIME NETWORK

Cybercrime Judicial Monitor

Issue 11

June 2026

Executive summary

Eurojust presents the 11th issue of the *Cybercrime Judicial Monitor* (CJM). Published yearly, the CJM is distributed to judicial and law enforcement authorities active in the field of combating cyber-dependent and cyber-enabled crime. 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.

This issue introduces a refreshed and more streamlined structure. It focuses on key legislative and policy developments and relevant case-law in the areas of cybercrime, electronic evidence (e-evidence) gathering, crypto-assets and artificial intelligence (AI). It also includes a dedicated chapter on data retention.

Last year, a number of relevant legislative and policy developments were observed at the international, EU and national levels. At the international level, the United Nations Convention against Cybercrime was opened for signature on 25 October 2025. At the EU level, legislative and policy developments took place in the area of lawful access to data, including e-evidence gathering, and in relation to AI. At the national level, EJCN members reported a broad range of legislative developments. These included, among others, amendments to criminal law provisions on cybercrime, new offences addressing the misuse of identity and AI-generated sexual material, and legislation implementing EU rules on crypto-assets.

Significant judicial developments also took place in 2025. At the EU level, the Court of Justice of the European Union delivered two judgments concerning the processing and transfer of personal data in the context of the Sky ECC operation, while the European Court of Human Rights issued a ruling concerning the transmission and use of data obtained through the interception of telecommunications in criminal proceedings and their subsequent use in administrative proceedings. At the national level, courts in several jurisdictions issued judgments on relevant topics, including the liability of administrators of platforms enabling the sale of illegal products, the admissibility of evidence from the ANOM messaging platform, and the procedural classification of intercepted communications. In the field of AI, rulings covered the criminal qualification of AI-generated sexual material involving minors and the dissemination of digitally altered content portraying adults as minors.

As far as data retention is concerned, the European Commission has initiated a process to assess whether further action at the EU level is warranted by launching an impact assessment aimed at examining the obstacles arising from the current state of play and identifying possible policy responses.

The CJM is mainly based on input from practitioners, and this collaborative approach will continue in future issues. Eurojust would like to thank the experts of the EJCN for their valuable contributions to this issue.

Table of Contents

1. Introduction 3
2. Legislation 4
2.1. Cybercrime 4
2.2. e-Evidence gathering 10
2.3. Crypto-assets 13
2.4. Artificial intelligence 17
3. Judicial analysis 20
3.1. Cybercrime 20
3.2. e-Evidence gathering 22
3.3. Crypto-assets 30
3.4. Artificial intelligence 32
4. Data retention 34
4.1. EU level 34
4.2. National level 35
5. Future of the Cybercrime Judicial Monitor 37

1. Introduction

Eurojust presents the 11th issue of the *Cybercrime Judicial Monitor* (CJM). Published annually, the CJM is distributed to judicial and law enforcement authorities active in the field of combating cyber-dependent and cyber-enabled crime. All issues of the CJM are also publicly available on the Eurojust website.

The CJM is prepared on the basis of contributions from members of the European Judicial Cybercrime Network (EJCN). For this issue, 21 EJCN members responded to the questionnaire, representing 18 EU Member States and 3 non-EU countries.

The 11th issue of the CJM introduces a refreshed and more streamlined structure. It focuses on key legislative and policy developments in the areas of cybercrime, electronic evidence (e-evidence) gathering, crypto-assets and artificial intelligence (AI), followed by an overview of relevant judicial decisions in these fields. In addition, a dedicated chapter examines developments related to data retention.

As part of this revamped approach, certain topics that were previously covered as a 'topic of interest' within the CJM will now be addressed through dedicated, self-standing flash reports. This will allow for more timely and focused analysis of emerging issues, while keeping the CJM focused on legislative, policy and case-law developments in the relevant areas.

2. Legislation

This chapter provides an overview of key developments in international, EU and national legal instruments and policy initiatives in 2025 and early 2026. The developments are structured around four main areas: cybercrime, e-evidence gathering, crypto-assets and AI.

Given the cross-cutting nature of many legislative initiatives, certain instruments may be relevant to more than one of these areas. For the purposes of clarity and consistency, each development has been included under a single heading, reflecting either its primary focus or the area to which it is most closely connected.

The national legislative developments presented in Section 2.1.2 are based on contributions provided by members of the EJCN.

2.1. Cybercrime

2.1.1. International level

➢ *United Nations Convention against Cybercrime*

Following its adoption by the United Nations (UN) General Assembly on 24 December 2024, the United Nations Convention against Cybercrime was opened for signature at a ceremony held in Hanoi, Viet Nam, on 25 October 2025, where 72 states signed the convention ([1]). The convention remains open for signature at the UN Headquarters in New York until 31 December 2026.

The convention aims to strengthen international cooperation in preventing and combating cybercrime and to enhance the protection of societies against digital threats. It establishes a framework of criminal offences, including offences against information and communications technology (ICT) systems, cyber-enabled crimes such as ICT-related fraud, and offences related to online child sexual abuse and child sexual exploitation material. The convention also provides for procedural measures to support investigations and prosecutions, 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. In addition, it sets out 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 will enter into force 90 days after the deposit of the 40th instrument of ratification, acceptance, approval or accession. Upon its entry into force, a Conference of the States Parties will meet periodically to promote cooperation, strengthen capacity and review the implementation of the convention. The rules of procedure for the Conference of the States Parties are currently under negotiation by the Ad Hoc Committee, with a view to ensuring the effective functioning and implementation of the convention.

([1]) For a full list of signatories and States Parties, please see here.

2.1.2. National level

Bulgaria

- *Regulation of cybercrime in Articles 319a–319f of the Bulgarian Criminal Code and the Cybersecurity Act, as amended and supplemented by State Gazette No 17 of 13 February 2026*

Cybercrimes are regulated in the Bulgarian Criminal Code, Chapter Nine 'A' – *Crimes against computer information and computer systems* (Articles 319a–319f), which criminalise unlawful access to a computer system, unlawful copying or destruction of computer data, distribution of malicious software and obstruction of the functioning of information systems. Additional provisions are contained in the Cybersecurity Act (promulgated in the *State Gazette*, issue 94 of 13 November 2018), which regulates the national cybersecurity system and measures for the protection of network and information systems, and in the Electronic Communications Act. The latter two acts were amended and supplemented by *State Gazette* No 17 of 13 February 2026.

Czechia

- *Article 191a of the Czech Criminal Code*

A new criminal offence concerns the misuse of identity for the production and dissemination of pornography, set out in Article 191a of the Czech Criminal Code, which reads as follows:

(1) Whoever produces, imports, exports, transports, offers, makes publicly available, brokers, puts into circulation, sells or otherwise provides to another a photographic, film, computer, electronic or other pornographic work that depicts or otherwise uses a person who he knows has not given consent to such depiction or use, shall be punished by imprisonment for up to two years, a ban on activity or forfeiture of property.

(2) The offender shall be punished by imprisonment for six months to three years:

a) if he causes significant harm to another by the act referred to in paragraph 1,

b) if he commits such an act as a member of an organised group,

c) if he commits such an act through the press, film, radio, television, a publicly accessible computer network or in another similarly effective manner, or

d) if he commits such an act with the intention of obtaining significant benefit for himself or for another.

(3) The offender shall be punished by imprisonment for one to five years if:

a) he causes extensive harm to another by the act referred to in paragraph 1,

b) he commits such an act as a member of an organised group operating in several states, or

c) he commits such an act with the intention of obtaining a large-scale benefit for himself or for another.

Denmark

- *Law no. 722 of 20 June 2025*

Law no. 722 of 20 June 2025 strengthened the effort against sexually offensive material online, among others, in the following ways:

- expansion of the Danish Criminal Code's sections regarding sexual material involving persons under 18 years of age, so that the sections also include posing photos and videos (i.e. photos and videos where a person, even though not naked, etc., is being exposed in a sexualising manner);

- expansion of the Danish Criminal Code's sections regarding sexual material involving persons under 18 years of age, so that the sections also include computer-generated sexual material, including material created using AI;
- clarification that sharing everyday pictures of persons under 18 years of age in a sexualised context can be punished under the Danish Criminal Code's section regarding sexual harassment;
- expansion of the Danish Criminal Code's section regarding identity abuse, so that the section also includes the fabrication of manipulated sexual material with real persons (so-called deepfake pornographic material); and
- introduction of a new subsection to Section 754a of the Danish Act on Administration of Justice, making it possible for the police to share faux sexual material depicting persons under 18 years of age as part of the investigation of an offence.

Estonia

➢ *§ 216¹ of the Estonian Criminal Code*

As of 1 January 2026, the scope of the offence of preparation of computer-related crimes under § 216¹ of the Estonian Criminal Code has been expanded. The provision now also covers the acquisition, manufacture, possession, distribution of or making otherwise available a device or computer programme which is designed or adapted in particular for the commission of unauthorised surveillance (§ 137 of the Estonian Criminal Code), in addition to interference with computer crime, hindering of functioning of computer systems, computer-related fraud, and illegally obtaining access to computer systems.

The provision reads as follows:

§ 216¹. Preparation of computer-related crime

(1) Acquisition, manufacture, possession, distribution of or making otherwise available a device or computer programme which is designed or adapted in particular for the commission of the criminal offences provided in §§ 137, 206, 207, 213 or 217 of this Code, or a protective device by means of which it is possible to gain access to a computer system with the intention of committing themselves or enabling a third party to commit a criminal offence provided in §§ 137, 206, 207, 213 or 217 of this Code – is punishable by a pecuniary punishment or up to two years' imprisonment.

France

➢ *Law No 2025-532 of 13 June 2025 introducing Article 706-74-2 of the French Code of Criminal Procedure and Article 323-3-2 of the French Criminal Code*

Law No 2025-532 of 13 June 2025 introduced Article 706-74-2 of the French Code of Criminal Procedure, which provides that the public prosecutor for organised crime exercises concurrent national jurisdiction for offences of attacks on automated data processing systems committed by organised gangs, in cases that are or appear to be highly complex due to, in particular, the seriousness or diversity of the offences committed, the large number of perpetrators, accomplices, or victims, or the geographical area over which they extend.

The specialised cybercrime section of the Paris Public Prosecutor's Office (Section J3) retains its concurrent national jurisdiction for offences against automated data processing systems, except in cases falling within the scope of Article 706-74-2. A mechanism for joint jurisdiction remains possible between the National Prosecutor's Office for Organised Crime and the prosecutors of the Specialised

Interregional Courts (JIRS), including, where relevant, Section J3 of the Paris Public Prosecutor's Office for cybercrime proceedings brought before the JIRS of Paris.

In addition, the law also amended Article 323-3-2 of the French Criminal Code concerning the provision of an illegal online platform. The amendment extended the scope of the offence to platforms that do not comply with the obligations mentioned in Articles 15, 16, and 18 of Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act), notably obligations relating to transparency reporting for providers of intermediary services, notice-and-action mechanisms against illegal content, and notifications of suspicions of criminal offences.

Greece

➢ *Law 5172/2025 implementing Directive (EU) 2024/1385*

Law 5172/2025, implementing Directive (EU) 2024/1385 of the European Parliament and of the Council of 14 May 2024 on combating violence against women and domestic violence, introduced several provisions addressing cybercrime and the misuse of information and communications technologies. Relevant provisions include the following:

- Articles 7 and 8 – cyberstalking: the law introduces cyberstalking as a means of committing the offence of threat (*Anyone who monitors another person, continuously or repeatedly, using information and communications technology, for the purpose of tracking or monitoring their movements and activities, causing them fear or anxiety, shall be punished with imprisonment of up to two (2) years*) and sexual assault (*Anyone who communicates or sends to another person, without their consent, in any way or using information and communications technology, a real or simulated image or visual or audiovisual material recorded on an electronic or other medium, depicting genital organs in a manner that may cause fear, anxiety, or serious psychological harm to the person receiving such material, shall be punished with imprisonment of up to three (3) years. If the offense referred to in the previous paragraph was committed against a minor or a person who is a public representative, journalist, or human rights defender, or if the perpetrator is in a hierarchical or dependent relationship with the victim, this constitutes a particularly aggravating circumstance.*).
- Article 12 – orders for removal or blocking of illegal online content: *By means of a fully and specifically reasoned order issued by the competent public prosecutor, it may be ordered, on the basis of the principle of proportionality and in accordance with Article 12 of Law 5099/2024 on orders to take action against illegal content, the removal by the website administrator or content hosting provider of content that falls under the criminal offences of paragraph 2A of Article 184, the second subparagraph of paragraph 1 and paragraph 1A of Article 333, paragraph 5 of Article 337, and Article 346 of the Penal Code (Law 4619/2019), as well as paragraph 1 of Article 1 of Law 927/1979, when it concerns the deliberate incitement of violence or hatred against a group of persons or a member of such a group defined on the basis of gender, provided that the details of the administrator or hosting provider can be identified. The order is notified by the competent prosecutor to the administrator or hosting provider, who must comply within twenty-four (24) hours and send a statement of compliance with the order. Upon notification of the order, the competent prosecutor shall inform the website administrator or the hosting provider of the website content that, in the event of non-compliance within twenty-four (24) hours, access to the Internet Protocol (IP) address and/or domain name will be blocked by Internet service providers (ISPs). If*

the administrator or hosting provider of the website is unknown or does not comply with the above provision, the competent prosecutor shall issue a new order to block access to the domain name and/or IP address by ISPs. The order shall expressly mention the domain names and/or IP addresses to which access must be suspended and shall specify its period of validity. The order is communicated by the competent prosecutor to the Hellenic Telecommunications and Post Commission (EETT), in accordance with Decision No 1114/2/3.6.2024 'Regulation establishing a standby system for personnel employed in the Telecommunications Directorate and the Digital Governance Directorate of the Hellenic Telecommunications and Post Commission (EETT)', as applicable. The EETT shall notify ISPs of the provision and request its immediate implementation. Within twenty-four (24) hours of receiving the provision, ISPs shall send EETT statements of compliance with the provision, indicating the implementation of the measure and the time of access interruption. ISPs are defined as all those registered in the Register of Electronic Communications Network and Service Providers, maintained by EETT, in accordance with Article 120 of Law 4727/2020.

- Article 30 – inducing or enticing a minor to watch sexual acts through the use of information and communications technology: *Anyone who induces or entices a minor under the age of fifteen (15) to watch, through the use of information and communications technology, or to be present at a sexual act between others, without participating in it, shall be punished with imprisonment of at least two (2) years and a fine if the minor is under fourteen (14) years of age, and with imprisonment of up to three (3) years or a fine if the minor has reached the age of fourteen (14th) year of age.*

Hungary

➢ *Amendments to the Hungarian Criminal Code and Code of Criminal Procedure*

As of 1 March 2025, new measures were introduced into Hungarian legislation, aimed at enabling authorities to suspend or terminate user accounts used for fraudulent purposes on online marketplaces, social media platforms and similar interfaces.

Section 78/A of the Hungarian Criminal Code reads as follows:

(1) The court may order the termination of hosting services provided to the perpetrator, that the perpetrator used or intended to use for committing the criminal offense.

(2) The termination of hosting services may be ordered even if the perpetrator cannot be prosecuted for reason of minority or insanity, or due to other grounds for exemption from criminal liability, or if the perpetrator had been reprimanded.

Section 338/A of the Hungarian Code of Criminal Procedure reads as follows:

(1) The court, the public prosecutor's office or the investigating authority may order the suspension of hosting services if the proceedings are conducted for a criminal offense subject to public prosecution, in connection with which the hosting service should be terminated, and there are serious grounds for believing that another criminal offense subject to public prosecution would be committed by using the service.

(2) The court, the public prosecutor's office or the investigating authority shall, by a decision ordering the suspension of the service, order the natural person, legal person or other organization providing the hosting service (for the purposes of this Chapter hereinafter referred to collectively as 'service provider') to suspend the rights of the holder of pecuniary interest (user or subscriber) stemming from the service during the suspension of the service, and may also prohibit the service provider to conclude a new service contract with him or her during the suspension of the service.

(3) The service provider shall execute the decision within one working day from the time of delivery of the decision. In the event of non-compliance with that obligation in due time a disciplinary fine may be imposed.

(4) The decision ordering the suspension of the service may be appealed by the service provider and the holder of pecuniary interest.

(5) The court, the public prosecutor's office or the investigating authority shall terminate the suspension of the hosting service if:

a) the grounds therefor cease to exist; or

b) the proceedings have been terminated or suspended, except if the hosting service has to be terminated pursuant to Section 78/A of the Criminal Code, and for this purpose the procedure under Chapter CVI is opened.

Italy

- *Law No 90 of 28 June 2024 (Cybersecurity Law)* ([2])

Law No 90 of 28 June 2024 strengthened Italy's cybersecurity framework and introduced amendments to the Italian Criminal Code concerning cybercrime. The law introduced new criminal offences, including cyber extortion, and increased the maximum penalties applicable to several cybercrime offences, including unauthorised access to computer systems (Article 615-ter of the Italian Criminal Code), with aggravating circumstances where the perpetrators acted in their capacity as public servants or abused their powers, computer fraud (Article 640-ter of the Italian Criminal Code) and offences involving the damaging, disruption or cancellation of digital data or computer systems.

The law also introduced strict governance, cybersecurity and incident-reporting requirements for public and private sector entities, including operators of critical infrastructure. Public administrations, particularly in the fields of justice, healthcare, transport and finance, must comply with strict and rigorous protocols. Cyberattacks must be reported to the National Agency for Cybersecurity within 24 hours, and all public administrations are required to appoint a cybersecurity manager. The agency plays a central role in supervising and coordinating cyberattack prevention activities and strengthening national cyber defence capabilities.

- *Decree of the President of the Council of Ministers of 2 October 2025*

The Decree of the President of the Council of Ministers of 2 October 2025 implements the requirements of the NIS2 Directive in Italy, introducing cybersecurity obligations for strategic operators and public administrations.

Portugal

- *Decree-Law No 125/2025 of 4 December 2025*

Decree-Law No 125/2025 of 4 December 2025 establishes a comprehensive national legal framework on cybersecurity, including provisions relevant to cybercrime and cooperation with law enforcement. The decree reviews the regulatory framework relating to national and international security in the functioning of the state and economic actors and transposes Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of

([2]) While adopted in 2024, this legislation was not included in previous editions of this report.

cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) into Portuguese law.

The decree sets out cybersecurity obligations for public and private entities, including incident reporting requirements, governance rules for cybersecurity, and institutional cooperation mechanisms between the Portuguese National Cybersecurity Centre (CNCS) and criminal justice authorities, such as the public prosecutor's office and the judicial police, in cases involving cybercrime-related incidents. While Portugal's Criminal Code already contained substantive cybercrime offences, the 2025 legislative act modernises and expands the legal framework on cybersecurity and cooperation with law enforcement in response to cyber incidents.

The decree also introduced Article 8-A into the Cybercrime Law (Law No 109/2009 of 15 September). This provision establishes that acts which could otherwise constitute the offences of illegal access or illegal interception are not punishable when certain conditions are met for reasons of public interest in cybersecurity. The rule therefore provides a limited exemption from criminal liability for 'white hat' or ethical hackers. The purpose of this provision is to allow security experts to identify vulnerabilities in information systems and disclose them. The exemption applies only under strict conditions: the activity must be carried out solely to identify security vulnerabilities, must not cause harm (such as service disruption or theft of personal data) and must not be motivated by financial gain beyond normal professional remuneration. Researchers must also promptly report the identified vulnerabilities to the system owner, the data protection authority and the CNCS.

The decree entered into force 120 days after its publication, becoming legally effective in 2026.

Switzerland

- *Amendment to the Information Security Act*

An amendment to the Information Security Act of 29 September 2023 (ISA) entered into force on 1 April 2025.

The act introduces a legal obligation on operators and certain public authorities to report cyberattacks affecting critical infrastructure. Entities subject to this obligation include, among others, energy and drinking water suppliers, transport companies, and cantonal and communal administrations. These entities must report cyberattacks to the Switzerland's National Cyber Security Centre within 24 hours of discovery.

Examples of when a cyberattack must be reported include when the attack threatens the functioning of critical infrastructure, has resulted in the manipulation or leakage of information, or involves blackmail, threats or coercion.

Critical infrastructure operators who fail to report a cyberattack may be fined.

The Federal Council also approved the Cybersecurity Ordinance, which also entered into force on 1 April 2025. The ordinance contains the implementing provisions for the reporting obligation and regulates the exceptions provided for under Article 74c of the ISA.

2.2. e-Evidence gathering

2.2.1. EU level

- *Commission Implementing Regulation (EU) 2025/1550 on the decentralised IT system for e-evidence*

In 2025, the European Commission adopted Implementing Regulation (EU) 2025/1550 of 28 July 2025, laying down the technical specifications and requirements for the decentralised IT system to be set up

for the functioning of the EU e-Evidence package (Regulation (EU) 2023/1543 and Directive (EU) 2023/1544).

The Regulation specifies how the system will operate in practice, including interoperability requirements, secure communication channels, encryption standards and the use of e-CODEX access points to connect national systems and EU agencies and bodies. It also sets technical parameters for the transmission of e-evidence and establishes minimum requirements for availability, security and data protection.

The Regulation is a key step towards the operationalisation of the EU e-Evidence package, ensuring that European Production Orders and European Preservation Orders can be exchanged efficiently and securely across borders once the system becomes fully operational.

➢ *Commission Roadmap for effective and lawful access to data for law enforcement*

While it does not constitute a legislative development as such, it is of relevance to note that, following the work of the High-Level Group (HLG) on access to data for effective law enforcement (more information on the HLG can be found in the previous edition of this report), the European Commission has taken forward the identified priorities through a policy roadmap. In this context, on 24 June 2025, the Commission presented a Roadmap for lawful and effective access to data for law enforcement, setting out a structured approach for future EU action in this area.

The roadmap builds on the HLG recommendations and identifies key challenges faced by authorities, including the fragmentation of national data retention regimes, the increasing use of end-to-end encryption, difficulties in accessing cross-border e-evidence, and insufficient digital forensic capacities. It confirms that these issues significantly affect the effectiveness of criminal investigations in the digital environment.

To address these challenges, the roadmap outlines a combination of legislative and non-legislative measures. In particular, the Commission announced an impact assessment on data retention in May 2025 (see also Chapter 4 below), with a view to possible future legislative action, including harmonisation of rules across EU Member States. It also envisages further work on improving cross-border cooperation mechanisms for access to e-evidence and strengthening cooperation with service providers, including non-traditional communications services.

With regard to encryption, the roadmap confirms the development of a technology roadmap (expected in 2026) to explore lawful access solutions that preserve cybersecurity and fundamental rights. It also highlights the need to enhance digital forensic capabilities through investment, training and improved coordination between law enforcement and judicial authorities.

2.2.2. National level

Austria

➢ *Amendments to the Austrian Code of Criminal Procedure*

The Austrian Criminal Procedure Amendment Act 2024, which entered into force on 1 January 2025, introduces new regulations for the seizure of data and data storage devices, establishing a standalone legal basis for the securing of digital evidence. This reform replaces the previous practice of 'evidentiary seizure', which the Austrian Constitutional Court had deemed insufficient.

The core amendments are anchored in § 109(2a–2e) and § 115 et seq. of the Austrian Code of Criminal Procedure (StPO). These provisions specify the conditions under which data storage devices and data may be seized. A key requirement is that judicial approval is now mandatory for the seizure of data and data storage devices. The judicial order must precisely describe which categories of data are to be

evaluated and the relevant time period, and a comprehensive justification for the seizure is required. Before analysis, the seized data must be prepared by creating an original backup and a working copy. Only data falling within the approved categories and timeframe may be filtered out, and only this reduced dataset may be used for subsequent evaluation.

Czechia

- *Amendments to the Czech Code of Criminal Procedure*

Czechia has regulated the possibility of issuing and seizing data in electronic form (Articles 78 and 79 of the Czech Code of Criminal Procedure), allowing for the issuance or seizure of data instead of the entire device.

A new provision on searching the contents of a device was also introduced in the Czech Code of Criminal Procedure (Article 113a). It establishes the obligation to obtain a court order before searching the contents of an electronic mobile device enabling two-way communication. An exception is possible if the user consents to the search, if the device was seized during a house search, and in several other cases.

France

- *Law No 2025-532 of 13 June 2025 introducing Article L232-9 of the Domestic Security Code and amending Articles 706-95-20 and 230-22 of the French Code of Criminal Procedure*

Article 14 of Law No 2025-532 of 13 June 2025 introduced Article L232-9 of the Domestic Security Code, which provides that, for the prevention and repression of terrorism, and to facilitate the detection of offences linked with organised crime, the port authority or the authority invested with port police powers must collect data enabling the identification of recreational vessels with a home port outside the port concerned, along with information concerning their owners, the persons on board and their itinerary. This data may be transmitted to the authorities responsible for prosecuting these offences in France.

In addition, Article 41 of the same law amended Article 706-95-20 of the French Code of Criminal Procedure, allowing investigators, upon prior authorisation by the public prosecutor, the liberty and detention judge, or the investigating judge, to install or remove a technical device such as an IMSI catcher in a private location, including outside the legal hours provided for by the law. In such cases, the operation is carried out under the supervision of the liberty and detention judge and cannot be used for any other purpose other than the installation of the technical device. The use of this device is intended to facilitate the collection of connection data enabling the identification of a terminal device or the subscription number of its user, along with data relating to the location of a terminal device in use. It constitutes a special investigation technique that can only be used in proceedings related to organised crime and delinquency.

Moreover, Article 50 of the law introduced a derogation to the maximum retention period for personal data in the context of ongoing criminal investigations, stored in judicial matching software, as provided for in Article 230-22 of the French Code of Criminal Procedure. The derogation applies exclusively to investigations concerning offences covered by Articles 706-73 to 706-74 of the French Code of Criminal Procedure, which relate to organised crime and delinquency. Under the new provision, the relevant data may be retained until the investigation or inquiry is closed, subject to authorisation granted every two years by the judge in charge of the investigation.

Luxembourg

➢ *Amendment to Article 88-2 of the Luxembourg Code of Criminal Procedure*

Law of 19 December 2025 amended Article 88-2 of the Luxembourg Code of Criminal Procedure, expanding the scope of application of the special technical surveillance measures listed in that article (surveillance of telecommunications and correspondence, audio-video surveillance of certain places and vehicles, surveillance of IT systems).

Previously, the use of these techniques was limited to investigations relating to terrorism or offences affecting state security. The amendment extends their application to a broader range of offences, including organised crime, kidnapping, human trafficking and child sexual abuse material.

Norway

➢ *Electronic Communications Act and Regulation*

A new Electronic Communications Act and accompanying Regulation entered into force on 1 January 2025, replacing the previous Electronic Communications Act.

The new legislation is based on the previous Electronic Communication Act, with relevant additions. Notably, the scope of the legislation has been expanded to include number-independent person-to-person services. Providers of such services are now subject to obligations to facilitate access to information concerning end users and electronic communications, and they must disclose subscriber information to the police upon request.

In addition, the new legislation introduces specific provisions concerning data centres.

2.3. Crypto-assets

2.3.1. National level

Bulgaria

➢ *Law on Crypto-Asset Markets*

The Law on Crypto-Asset Markets (published in the *State Gazette*, No 54 of 4 July 2025, as amended and supplemented by No 67 of 15 August 2025 and No 25 of 10 March 2026) introduces into Bulgarian legislation the requirements of the Markets in Crypto-Assets (MiCa) Regulation (Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937).

Austria

➢ *Amendment to the Austrian Code of Criminal Procedure*

Under the Austrian Criminal Procedure Amendment Act 2024, which entered into force on 1 January 2025, Austrian law now explicitly stipulates that crypto-assets are classified as 'assets' within the meaning of § 109(1a) of the StPO. Furthermore, seized crypto-assets must be transferred to an official authority wallet, as provided for in § 114(1a) of the StPO. Additionally, the process for disbursing assets during criminal investigations has been simplified.

Czechia

➢ *Act No 31/2025 Coll. (Digital Finance Market Act)*

Act No 31/2025 Coll. (Digital Finance Market Act) sets the national framework mainly for Czech National Bank supervision, supervisory powers, remedial measures, and administrative offences/penalties in the area of 'crypto-asset markets'. It also includes rules on the protection of entrusted assets and a transitional provision allowing continuation of business if an application is filed in time (see, e.g., §§ 2-17 and 20-26).

➢ *Act No 32/2025 Coll.*

Act No 32/2025 Coll. amends a broad range of laws in connection with crypto-assets and related services, including:

- private law (Czech Civil Code – expanding the scope of regulation to contracts relating to the acquisition of crypto-assets and crypto-asset services);
- financial-market regulation (banks, credit unions, financial arbiter, capital markets, administrative fees); and
- anti-money-laundering (AML): addition of a new 'Chapter VI' introducing a licensing regime for services connected with virtual assets (licensed by the Financial Analytical Office), including an administrative offence for the unlicensed provision of such services.

➢ *Act No 218/2025 Coll.*

Act No 218/2025 Coll. includes, among other things:

- an explicit inclusion of crypto-assets within the definition of 'property' for the purposes of international sanctions; and
- rules on tax enforcement (tax execution) relating to a 'virtual asset' (a newly introduced procedure under the Czech Tax Code).

France

➢ *Law No 2025-532 of June 2025*

Article 11 of Law No 2025-532 of 13 June 2025 introduced Article L. 561-14-1 A of the Monetary and Financial Code, which prohibits the holding of any type of account or the offering of any type of service that allows for the anonymisation or increased opacity of crypto-asset transactions, including crypto-asset mixers.

In addition, Article 7 of the same law amended Article 324-1-1 of the Criminal Code, extending the presumption of money laundering to any transaction carried out using a crypto-asset with an integrated anonymisation function or any means allowing the opacity or anonymisation of crypto-asset transactions (such as mixers).

Greece

➢ *Articles 97-115 of Law 5193/2025*

Articles 97-115 of Law 5193/2025 regulate crypto-asset services in accordance with the MiCA Regulation. Most importantly, providing crypto-asset services without a license is now a criminal offence:

Anyone who intentionally provides crypto-asset services on a professional basis without the license required by Regulation (EU) 2023/1114 on markets in crypto-assets and amending Regulations (EU) 1093/2010 and (EU) 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937, shall be punished with imprisonment of at least one (1) year. If the services referred to in the previous paragraph are provided by legal persons, the penalty shall be imposed on anyone who exercises the management or administration of that legal person.

Iceland

➢ *Applicability of MiCA Regulation*

Crypto-assets became subject to a comprehensive regulatory framework in Iceland through the incorporation of the MiCA Regulation into the European Economic Area (EEA) Agreement by a decision of the EEA Joint Committee.

The decision amended Annex IX ('Financial Services') of the EEA Agreement, thereby extending the EU crypto-asset regulatory regime to the EEA European Free Trade Association states, including Iceland. As a result, the MiCA Regulation forms part of the legal framework applicable in Iceland once the decision entered into force in accordance with EEA procedures.

Lithuania

➢ *Amendments to the Law on Crypto-Asset Markets of the Republic of Lithuania (Law No. XIV-2879 of 11 July 2024)*

Several amendments to the Law on Crypto-Asset Markets of the Republic of Lithuania (Law No. XIV-2879 of 11 July 2024) were adopted, further aligning the national framework with the EU legislation in the area.

➢ *Law No. XV-185 of 8 May 2025*

Law No. XV-185 of 8 May 2025 establishes transitional provisions to ensure the transition from the previous national regulatory framework to the one set out under the MiCA Regulation. The law clarifies the legal status of virtual currency exchange operators and depository virtual currency wallet operators currently registered in the Register of Legal Entities. As of 1 January 2026, such entities may continue operating only if they obtain a licence in accordance with the MiCA Regulation and the national Law on Crypto-Asset Markets.

➢ *Law No. XV-308 of 19 June 2025*

Law No. XV-308 of 19 June 2025 further refines the Lithuanian regulatory framework for crypto-assets and aligns national legislation with the 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). Key changes include the following:

- Expanded compliance obligations (Article 3): issuers of asset-referenced tokens and crypto-asset service providers (CASPs) must comply not only with the MiCA Regulation and the national Law on Crypto-Asset Markets, but also with other legal acts within the competence of the supervisory authority (the Bank of Lithuania).
- Strengthened supervisory powers (Articles 10 and 12): the supervisory authority is formally tasked with monitoring compliance with the MiCA Regulation, national law and related

implementing acts. It is also authorised to investigate complaints regarding potential violations. When supervising traditional financial institutions (such as banks, credit unions, e-money institutions, and investment firms) regarding their crypto-asset activities, the authority retains all powers granted by the specific laws governing those entities. The authority can issue mandatory instructions to issuers and service providers if it suspects violations, identifies operational deficiencies, or perceives a threat to market stability or the interests of consumers/holders. The authority is empowered to organise and carry out inspections to ensure all relevant regulations are being followed.

- Integration of DORA (Articles 13 and 15): violations of DORA requirements are now officially listed as grounds for the supervisory authority to take action. The supervisory authority is authorised to impose fines for violations of DORA, alongside violations of the MiCA Regulation and national law.
- Sanctions and enforcement (Article 14): the supervisory authority may publicly announce violations and the identity of responsible persons or entities, issue warnings and order the cessation of infringements within a specified timeframe.
- Update of the annex to the law: the annex now expressly lists the EU legal acts implemented by the law, including the MiCA Regulation and DORA.

Portugal

Portugal enacted significant legislative provisions concerning crypto-assets, primarily to implement the MiCA Regulation and associated fund-transfer rules into national law.

➢ *Law No 69/2025 of 22 December 2025*

Law No 69/2025 of 22 December 2025, which entered into force on 27 December 2025, implements the MiCA Regulation into national law, clarifying the rights and obligations of issuers and CASPs, such as exchanges and wallet providers.

The law establishes rules concerning the classification of crypto-assets, the conditions for issuance and admission to trading, and the authorisation and supervision of CASPs. The law designates the Bank of Portugal and the Comissão do Mercado de Valores Mobiliários as the competent supervisory authorities responsible for monitoring compliance. It also establishes cooperation mechanisms between these national authorities and European regulators.

The law also includes a sanctioning regime for non-compliance, including administrative fines which, in serious cases, may reach up to EUR 5 million or up to 15 % of the annual turnover for serious infringements.

➢ *Law No 70/2025 of 22 December 2025*

Law No 70/2025 of 22 December 2025 implements Article 38 of 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 and amending Directive (EU) 2015/849, thereby strengthening AML and counter-terrorist financing (CFT) requirements for crypto-asset transactions. Most operational provisions of the law are expected to apply from 2026. The law transposes provisions of Regulation (EU) 2023/1113 that require that transfers of crypto-assets be accompanied by accurate information on the originator and the beneficiary, thereby aligning Portuguese legislation with international AML/CFT standards for crypto-asset transfers

2.4. Artificial intelligence

2.4.1. EU level

➢ *Regulation (EU) 2024/1689 (AI 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 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) entered into force on 1 August 2024 and will apply fully as of 2 August 2026, with phased implementation.

The AI Act sets out a uniform legal framework for the development, marketing and use of AI within the EU. It established a risk-based framework (minimal, limited, high and unacceptable risk), prohibiting certain harmful AI practices and imposing stricter obligations on high-risk systems to ensure safety, transparency and fundamental rights protection.

Notably, as of 2025, the following provisions apply:

- as of 2 February 2025: the prohibitions on unacceptable-risk AI systems and the general provisions (including AI literacy obligations);
- as of 2 May 2025: codes of practice for general-purpose AI (GPAI) should be available; and
- as of 2 August 2025: governance rules, obligations for GPAI models, and provisions on notified bodies and penalties apply.

All remaining rules will apply later, mainly as of 2 August 2026 (and high-risk AI requirements as of 2027).

More information about the AI Act can be found in Section 2.2 of the previous issue of this report.

➢ *Commission Guidelines on prohibited AI practices*

To ensure the consistent, effective and uniform application of the AI Act across the EU, on 4 February 2025, the Commission issued non-binding Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act). The guidelines specifically address practices such as harmful manipulation, social scoring, and certain uses of real-time remote biometric identification in public spaces. While they offer valuable insights into the Commission's interpretation of the prohibitions, they are non-binding, with authoritative interpretations reserved for the Court of Justice of the European Union (CJEU).

➢ *Commission Guidelines for providers of GPAI models*

In line with the implementation timeline for the AI Act, the Commission has issued Guidelines on the scope of the obligations for providers of general-purpose AI models established by Regulation (EU) 2024/1689 (AI Act). The guidelines are aimed at helping actors in the AI ecosystem determine whether the AI Act obligations apply to them and what those obligations entail. While non-binding, they provide the Commission's interpretation of key concepts in the AI Act and are complemented by the Code of Practice for General-Purpose AI Models, a voluntary tool offering practical guidance on compliance.

Among other things, the guidelines:

- introduce straightforward technical criteria, for instance for when an AI model is considered 'general-purpose', to help developers understand if they need to comply with the obligations under the AI Act;
- clarify that only those making significant modifications to AI models need to comply with the obligations for providers of GPAI models, not those making minor changes; and
- specify under what conditions providers of open-source AI models are exempt from certain obligations, to promote transparency and innovation.

➢ *Digital Justice @2030 Strategy*

In addition to the developments outlined above, it is of note that, in November 2025, the European Commission adopted the Digital Justice @2030 Strategy, a communication setting out a roadmap aimed at accelerating the digitalisation of national justice systems across the EU. The strategy aims to enhance the efficiency, modernisation and resilience of justice systems, increasing growth and competitiveness and easing the strained budgets for national justice systems.

The strategy sets out a set of actions to support EU Member States, including, among other things, the creation of an IT toolbox for justice, supporting Members States on the uptake of AI in justice and elaborating on the use of high-risk AI systems in justice, the creation of a European Legal Data Space to improve access to legislation and case-law, the promotion of voluntary technical standards for cross-border remote proceedings, and an assessment of the feasibility of fully digitalising cross-border proceedings in civil and commercial matters.

2.4.2. National level

Czechia

➢ *Article 181 of the Czech Criminal Code*

Czechia has adopted a new criminal offence concerning the unlawful use of another person's likeness or personal expression with the intention of causing serious damage to their rights. The offence is set out in Article 181, paragraph 2 of the Czech Criminal Code, which reads as follows:

Whoever, with the intention of causing serious damage to the rights of another, produces a work that unlawfully depicts, captures or otherwise uses the likeness of another or his personal expression, which appears to be genuine, although he knows that it is not genuine, or makes such a work publicly accessible, mediates, puts into circulation, sells or otherwise provides it to another, shall be punished by imprisonment for up to two years or by a ban on activity.

Italy

➢ *Law No 132 of 23 September 2025*

Law No 132 of 23 September 2025 regulates the development, use and governance of AI in Italy, in line with the AI Act. The law establishes general principles governing AI systems, including transparency, safety, non-discrimination, accountability and human oversight.

The law regulates the use of AI in several key sectors, including healthcare, public administration, justice, employment, education and sport. In the employment context, both public and private employers using AI systems are required to inform employees of their use through means capable of

producing a written record and with at least 24 hours' prior notice. The law also enshrines the principle of human oversight, ensuring that individuals retain the possibility to intervene in, review or challenge decisions produced through automated systems. In the judicial field, AI may be used only as a supporting tool and cannot replace judicial decision-making.

The law further introduces criminal law provisions addressing the misuse of AI technologies and establishes new aggravating circumstances for offences committed through the use of AI-generated or AI-manipulated content, including the unlawful dissemination of deepfakes, namely images, videos or audio recordings altered or manipulated to appear authentic with the intent to harm a person's reputation.

In addition, the law promotes funding and support measures for the development of start-ups operating in the fields of AI and cybersecurity.

Portugal

- *Implementation of the AI Act*

As part of implementing the AI Act, the Portuguese government designated several public authorities, coordinated by the National Communications Authority, to oversee compliance with the EU legislation and protect fundamental rights in relation to the deployment of AI systems, including high-risk applications.

Lithuania

- *Updated Recommendations for persons submitting cassation and other procedural documents*

While it does not constitute a legislative development as such, it is of relevance to note that, on 2 May 2025, the Supreme Court of Lithuania updated its Recommendations for persons submitting cassation and other procedural documents, which aim to ensure the proper quality, transparency and reliability of procedural submissions. Under point 6.3 thereof, when a procedural document or part thereof is prepared using generative AI tools, this fact must be disclosed at the beginning or at the end of the document. The person submitting the document must indicate that the procedural document or a part of it was prepared with the assistance of generative AI and confirm that its content has been carefully checked by the person who prepared or submitted the document.

3. Judicial analysis

This chapter provides insight into selected judgments delivered at the EU, international and national levels in 2025 and early 2026, structured around four main areas: cybercrime, e-evidence gathering, crypto-assets and AI. Given the cross-cutting nature of some cases, some judgments may be relevant to more than one area; however, for reasons of clarity, each has been included under a single heading. The analysis focuses on the most noteworthy legal aspects of each case, rather than providing an exhaustive account of all issues and arguments addressed by the courts.

This chapter responds to practitioners' need for a regular overview of judicial developments across jurisdictions, enabling them to draw on court reasoning and evidentiary approaches developed in other countries.

3.1. Cybercrime

3.1.1. National court rulings

France

Paris Judicial Court (13th Correctional Chamber) – 30 January 2025

Background

Article 323-3-2 of the French Criminal Code criminalises the act of administering an online platform that enables the sale or distribution of illegal products, services or content.

The case concerned a Telegram channel used to advertise and sell ransomware and raised the question of whether the administrator of such a channel could be held criminally liable.

Judicial Court ruling

The court held that the administrator of a Telegram channel facilitating the sale of ransomware qualifies as a co-author of the offence of administering an online platform enabling the sale of illegal products. It considered that the channels operated in practice as online stores allowing the sale of illegal products, and therefore fell within the scope of the provision.

The court further noted that this conclusion applied regardless of whether the administrator used technical features provided by the Telegram platform, given that it was widely known at the time of the events that Telegram did not respond to investigators' requests.

Greece

Supreme Court of Greece – Decisions 244/2025 and 303/2025

Background

Greek criminal law contains specific provisions on computer fraud under Article 386A of the Greek Criminal Code. Since its adoption, the provision has been amended several times.

Two recent cases before the Supreme Court concerned the application of this provision, including the principle of applying the criminal provision more favourable to the accused and offences involving the misuse of electronic systems and credentials.

Supreme Court ruling

In Decision 303/2025, the Supreme Court held that the current version of Article 386A of the Greek Criminal Code is more favourable to the defendant and therefore applicable. It noted that Article 386A(1)(d) and (e), as amended by Law 4619/2019 and subsequently by Law 4855/2021 and Law 4947/2022, contains a more restrictive list of the ways in which the offence of computer fraud may be committed, compared with the indicative list contained in the previous version of the provision. The earlier provision also provided for a longer sentence, making the current regulation more favourable to the accused.

In Decision 244/2025, the Supreme Court examined a case in which the defendant had illegally obtained the private security codes of a physician, used them to access the electronic state prescription system, and issued several electronic prescriptions appearing to have been created by the physician. The aim was to mislead employees of the insurance agency into believing that the insured persons were entitled to receive the items listed in the prescriptions and that the pharmaceutical suppliers were entitled to reimbursement from the insurance institution. The Supreme Court validated the judgment of the lower court, which had convicted the defendant of forgery.

Norway

Oslo District Court – 28 June 2024 ([3])

Background

Norwegian criminal law criminalises fraud under Sections 371 and 372 of the Norwegian Criminal Code, including fraud committed through deception carried out by electronic means. The case concerned a large-scale phishing scheme in which victims were deceived into disclosing their BankID credentials, allowing perpetrators to access their online banking accounts.

The perpetrators carried out phishing attacks by sending SMS messages impersonating the Norwegian Public Roads Administration. The messages were targeted at persons who had recently bought or sold vehicles and invited recipients to follow a link to a fake website resembling the official website of the Norwegian Public Roads Administration. Victims were then prompted to log in with their BankID, enabling the perpetrators to obtain their credentials and gain access to their online banking services.

The scheme affected at least 423 victims. The perpetrators attempted to transfer approximately NOK 10 million, resulting in actual losses of around NOK 1.7 million and significant risk of further losses.

District Court ruling

The Oslo District Court found both defendants guilty of aggravated fraud, attempted fraud and identity misuse. The court also clarified that the offence of fraud may already be considered completed once victims are deceived into disclosing their BankID credentials, since this exposes them to a real risk of financial loss, even if the subsequent transfer of funds requires additional actions by the perpetrators.

([3]) While issued in 2024, this ruling was not included in previous editions of this report.

Spain

Supreme Court of Spain – 16 October 2025

Background

Spanish criminal law protects the confidentiality of personal data under Article 197(2) of the Spanish Criminal Code. The case raised the question of whether the fraudulent obtaining of a computer password and the subsequent access to folders and files on a personal computer constituted an offence.

Supreme Court ruling

The Supreme Court held that any numeric or alphanumeric series that allows access to any telematic service constitutes data of an unidentified but perfectly identifiable person. These numeric/alphanumeric identifiers, capable of providing access to an automated service, replace physical identification with virtual identification, associated with that uniquely owned key.

The court found that fraudulently obtaining the computer key already constitutes in itself non-consensual access to private personal data. The key, as an identifier of its owner, grants access to all the information that may exist on the computer and therefore constitutes per se private personal data protected by Article 197(2) of the Spanish Criminal Code.

The court further held that the key of a personal computer provides access to all its contents, where ordinarily private personal information is stored. In line with its case-law recognising that an online identifier constitutes personal data deserving of protection because it enables the identification of its owner, the court confirmed that the improper acquisition of a computer key is likewise protectable and criminally punishable as soon as it gives access to the personal information stored on the device. The court added that no detailed description of the content is required, once it is established that the defendant did not merely obtain the key but accessed different folders and content, and that such generalised access to all the information on the computer satisfies the harm required by the offence.

3.2. e-Evidence gathering

3.2.1. Court of Justice of the European Union

- *Judgment of the General Court (Fifth Chamber) in Case T-1180/23, BW v Europol and Eurojust (Sky ECC I) – 25 February 2026*

Background

The case concerned the large-scale interception and processing of decrypted communications from the Sky ECC encrypted communication platform (suspected of marketing encrypted communications products and services specifically designed to facilitate the commission of criminal offences) in the context of cross-border criminal investigations. National authorities in Belgium, France and the Netherlands set up a joint investigation team (JIT) to investigate serious organised crime linked to the creation and use of the service.

French authorities used a 'man-in-the-middle' technique to intercept, record and transcribe and decrypt encrypted communications from Sky ECC servers within the framework of the JIT (whose objective included the development and implementation of the technique necessary to decrypt past communications), after which the data were shared with Belgian and Dutch authorities as part of the JIT agreement. Europol supported the analysis of the data, while Eurojust facilitated judicial cooperation and coordination among the JIT members and the transmission of those data to other countries in execution of European Investigation Orders and mutual legal assistance (MLA) requests, including with Serbia.

The applicant, a Serbian national prosecuted in both the Netherlands and Serbia, challenged the lawfulness of the collection, processing and sharing of his personal data by Eurojust and Europol. He sought the annulment of various acts as well as damages, alleging, inter alia, unlawful data processing, breaches of fair trial rights and failures of coordination leading to parallel proceedings.

Admissibility and scope of review

The General Court clarified the limits of its jurisdiction. It reiterated that it cannot review acts of national authorities, including interception measures or the transmission of data by EU Member States, nor the legality of the JIT agreement itself, which is not an EU act.

It further held that the majority of the conduct referred to by the applicant, such as participation by Europol and Eurojust in meetings, analytical activities, or exchanges of information, constituted preparatory measures that did not produce binding legal effects and could therefore not be challenged under Article 263 of the Treaty on the Functioning of the European Union. This included, in particular, Europol's analytical support in processing and organising the intercepted data, which did not in itself produce legal effects capable of judicial review.

By contrast, the Court held that it could review the legality of the transmission of the applicant's personal data by Eurojust to the Serbian authorities as an intermediary in execution of an MLA request addressed to the French authorities. As opposed to other internal or preparatory steps, that transfer represented the final stage of a distinct procedure involving the disclosure of personal data to a third country and directly affected the applicant's legal situation. The Court also emphasised that recognising the reviewability of this act was necessary to ensure effective judicial protection, particularly given the absence of alternative legal remedies.

Lawfulness of the data transfer

The General Court examined whether the transmission of the applicant's personal data to the Serbian authorities complied with EU data protection requirements.

It noted that the transfer was carried out within the mandate of Eurojust and was based on a valid legal framework, including EU law and a cooperation agreement between Eurojust and Serbia, on the basis of an MLA request from Serbia to France. The processing pursued legitimate objectives related to criminal investigations, and there was no indication that the data were processed for purposes other than the performance of Eurojust's tasks.

The Court further found that the transmission complied with the principles of necessity and proportionality, as it concerned specific data requested in the context of mutual legal assistance and was carried out via a secure system. It also noted that Eurojust did not store or further process the data.

The Court also found that the applicant failed to demonstrate any breach of data protection safeguards or of his rights of defence, in particular under Articles 47 and 48 of the Charter of Fundamental Rights of the European Union.

The Court also rejected the applicant's complaint that Europol and Eurojust failed to coordinate so as to prevent parallel prosecutions in the Netherlands and Serbia. It held that neither the JIT agreement nor the applicable EU rules impose such an obligation, since they concern only the coordination of investigations and the use of data, while decisions on prosecution remain within the competence of the national authorities and Eurojust's role is limited to assistance.

- *Judgment of the General Court (Fifth Chamber) in Case T-167/24, DG v Europol and Eurojust (Sky ECC II) – 25 February 2026*

Background

The case similarly concerned the processing of data from the Sky ECC platform in the context of cross-border criminal investigations into international drug trafficking. The applicant, who was subject to criminal proceedings in Belgium and the Netherlands and detained in one of those EU Member States, sought compensation for alleged harm resulting from those operations, alleging, inter alia, unlawful processing of personal data, breaches of his rights of defence, failures of coordination leading to parallel proceedings, and inadequate protection of his data resulting from the gathering, transmission and use of his Sky ECC chats as evidence in those proceedings.

Admissibility and scope of review

The General Court clarified the limits of its jurisdiction. It held that the applicant could seek only the liability of Europol and Eurojust for their own conduct, and, in the case of Europol, potentially also joint and several liability with EU Member States in respect of unlawful processing of personal data within the framework of the Europol Regulation (Regulation 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA).

The Court further held that it lacked jurisdiction to assess alleged breaches of fair trial rights by national criminal courts or to review evidentiary issues arising in those proceedings. It also confirmed that it could not review the lawfulness of data collection carried out by national authorities in the context of police operations, including the interception of Sky ECC communications by French and Dutch authorities.

The action against Eurojust

The General Court held that the claims against Eurojust were largely inadmissible. The applicant had failed to identify with sufficient precision any processing of his personal data carried out by Eurojust that could give rise to liability. In particular, Eurojust's role in organising coordination meetings did not establish that it had processed the applicant's data

The Court also rejected the complaint that Eurojust had failed to prevent parallel proceedings in Belgium and the Netherlands. It found that the applicant had not demonstrated that the same facts were being prosecuted in both countries and, in any event, that Eurojust is subject only to an obligation to use its best endeavours, while the decision to prosecute a person lies solely with the national authorities concerned. Accordingly, the action was dismissed insofar as it concerned Eurojust.

The action against Europol

As regards Europol, the General Court found several claims inadmissible, including those relating to alleged material damage and certain claims relating to non-material damage, on the grounds that the application did not sufficiently identify the conduct complained of or substantiate the alleged harm.

However, the Court accepted the admissibility of the claim alleging non-material damage resulting from the applicant's data having fallen or potentially fallen into the 'wrong hands'. However, on the merits, the Court found that the applicant had failed to prove the existence and extent of the alleged damage. Although the applicant relied on data derived from Sky ECC communications, he did not produce the relevant personal data or demonstrate concretely how the processing of the data had caused him harm. The Court therefore concluded that the condition relating to the existence of damage was not satisfied and the action had to be dismissed as it concerned Europol.

3.2.2. European Court of Human Rights

- *Ships Waste Oil Collector B.V. and Others v. the Netherlands*

On 1 April 2025, the European Court of Human Rights (ECtHR) (Grand Chamber) delivered its judgment in the case *Ships Waste Oil Collector B.V. and Others v. the Netherlands* (Application no. 2799/16 and 3 others), concerning the transmission and use of data obtained through the interception of telecommunications in criminal proceedings and their subsequent use in administrative (competition law) proceedings.

The case raised important issues regarding the use and further transmission of intercepted communications data as evidence, including whether such transmission constitutes a separate interference with the right to respect for private life under Article 8 of the European Convention on Human Rights (ECHR).

In its reasoning, the ECtHR recalled that legal entities are entitled to protection under Article 8 of the ECHR, including with regard to the confidentiality of their communications. It found that the interception of telephone communications of companies' employees in the framework of criminal investigations, as well as the subsequent transmission of a selection of that data for use in competition proceedings, constituted an interference with the applicant companies' right to respect for their correspondence under Article 8.

The Court further held that the transmission of intercept data to another authority for further use constitutes a separate interference under Article 8, distinct from, albeit related to, the original interception of communications.

As regards justification, the Court recalled that any interference with Article 8 rights must be in accordance with the law, pursue a legitimate aim and be necessary in a democratic society. It further noted that, although the transmission of intercept data is generally less intrusive than the original interception of communications, it nevertheless constitutes a significant interference where the data are used for a new purpose. Such interference therefore requires adequate safeguards against arbitrariness and abuse. In this regard, the Court emphasised that domestic law must provide clear and detailed rules governing the scope and application of such measures, including safeguards relating to the storage, use, access and onward transmission of the data, and effective review mechanisms. It also clarified that the transmission of intercept data beyond the original criminal context must have a legal basis in domestic law and be foreseeable to the data subject.

Applying these principles, the Court found that the domestic legal framework sufficiently defined the conditions for transmitting intercept data and met the requirement of foreseeability. It also accepted that prior notification was not required, given the need to preserve the effectiveness of ongoing investigations, provided that effective *ex post facto* remedies were available.

The Court further noted the absence of any reasoning in the transmission authorisations, which did not contain any verifiable assessment of whether the transmissions were necessary and proportionate. However, as the transmitted material was the product of lawful telephone tapping authorised by a court, it considered that this was compensated for by a *de novo* assessment of the transmissions' lawfulness and their 'necessity in a democratic society' by the courts which carried out the *ex post facto* review.

Finally, the Court held that the transmission pursued the legitimate aim of protecting the economic well-being of the country, and that the domestic authorities had provided relevant and sufficient reasons to justify the interference, taking into account the seriousness of the competition law violations and the limited scope of the data used.

The Court therefore concluded that there had been no violation of Article 8 of the ECHR.

As the Court found that the applicants had an effective remedy at their disposal for their complaints under Article 8, it further found no violation of Article 13 in conjunction with Article 8.

3.2.3. National court rulings

Estonia

Supreme Court of Estonia – 16 January 2025 (rulings in cases Nos 1-21-7384 and 1-21-7780 in Estonian language)

Background

The United States (US) Federal Bureau of Investigation (FBI) developed a mobile messaging application called ANOM, which enabled users to send encrypted messages. Without the users' knowledge, the application copied the messages the users sent and transmitted them to a designated server located in an EU Member State that has not been publicly disclosed. That state, in turn, made the ANOM device communications available to US authorities.

ANOM messages obtained from the US on the basis of requests for legal assistance were later used as evidence in Estonian criminal proceedings concerning narcotics offences. The Court of Appeal had previously acquitted the defendants, finding that the evidence had not been gathered in accordance with the principles of Estonian criminal procedure and that it had not been sufficiently demonstrated that the evidence had been collected lawfully in the foreign state.

Supreme Court ruling

The Supreme Court held that, when using evidence collected in other countries, it is presumed that the evidence was obtained in accordance with that state's law. It therefore confirmed that ANOM messages obtained from the US may be used as evidence in Estonian criminal proceedings.

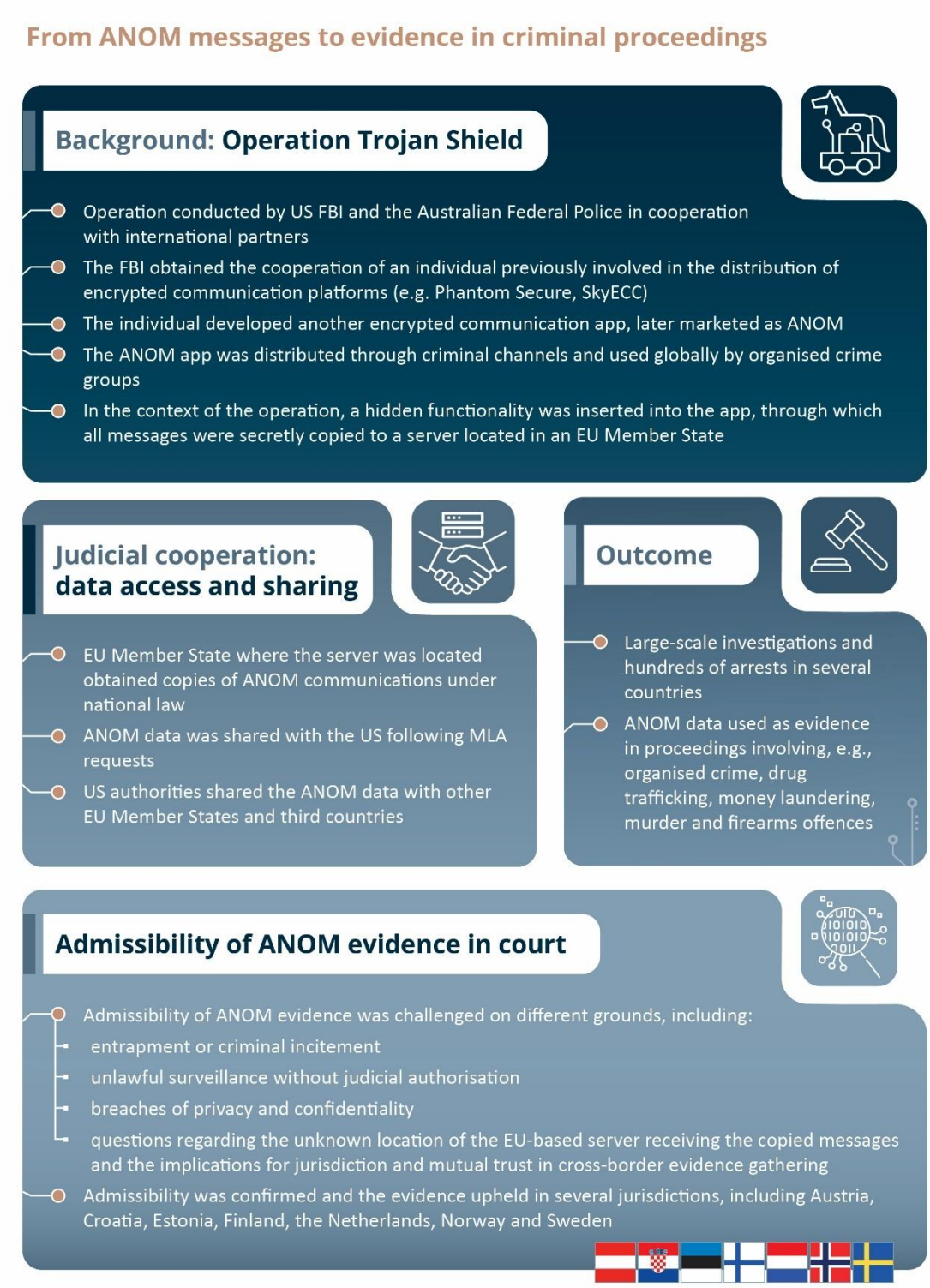
The Supreme Court explained that permitting the use of evidence collected in other countries supports the need to combat cross-border crime. The purpose of the relevant provisions of Estonian law is to open Estonian criminal proceedings to evidence originating from other legal systems. In particular, where Estonia has concluded an international agreement with a foreign state, it is presumed that the evidence was collected in accordance with that state's laws. In the case, the US had confirmed that the evidence had been obtained lawfully.

In both cases, the situation was somewhat exceptional in that not all details of the evidence-gathering process were known to the Estonian courts (for example, the specific EU Member State in which the server was located). However, according to the Supreme Court, there was no indication that the collection of evidence abroad had violated any principles underlying the functioning of Estonian criminal procedure. Such principles include the prohibition of torture, unlawful violence, degrading treatment, violations of honour and dignity, endangerment of life and health, and the privilege against self-incrimination. Nor may evidence obtained from a foreign state be used if, in collecting it, there was from the outset an intention to circumvent the rights of the person concerned or if procedural law was deliberately violated.

The Supreme Court added that the extent of information required to verify that a procedural act carried out abroad complies with the principles of Estonian criminal procedure depends on the nature of the evidence. The more easily the content of the evidence can be influenced, the more information an Estonian court may require. It is also important that, even if evidence obtained from abroad is admissible, the court hearing the case must still assess its reliability.

Proceedings before the ECtHR

A related case is currently pending before the ECtHR (*Raal and Reudolph v. Estonia*, applications Nos 14711/25 and 14712/25). The applicants allege violations of their rights under Articles 8 and 6 of the ECHR in connection with the ANOM operation and the subsequent use of the data in criminal proceedings.



France

Court of Cassation (Criminal Chamber) – 14 January 2025 (ruling in French language)

Background

French criminal procedure distinguishes between the capture of computer data (data stored on computer systems) and the interception of correspondence sent via telecommunications networks. The classification of an investigative measure determines the applicable legal regime and the type of judicial authorisation required.

The case concerned the interception of communications exchanged through telecommunications networks, in particular messages transmitted between servers used for encrypted messaging services.

Court of Cassation ruling

The court clarified the distinction between the capture of computer data and the interception of telecommunications. It held that, in the absence of any capture of data stored on servers, the interception of data exchanged via telecommunications networks does not fall under the provisions governing the capture of computer data, but rather under those governing judicial interception of correspondence sent by electronic communications.

Court of Cassation (Criminal Chamber) – 21 January 2025 (ruling in French language)

Background

French criminal procedure allows investigating judges to authorise special investigative measures, including the interception, recording and transcription of communications sent via electronic means and the installation of technical devices enabling real-time geolocation.

The case concerned the calculation of the duration and renewal of such measures, in particular whether the authorised period begins on the date of the judicial decision or on the date the technical device is actually installed, and the conditions under which the authorisation may be renewed.

Court of Cassation ruling

The court clarified the rules governing the renewal of judicial authorisations for the interception of electronic communications and the installation of real-time geolocation devices. It held that, where the investigating judge expressly authorises the implementation of the measure from the date of the decision, the authorised period cannot begin on the date on which the technical devices are installed. The court further held that the renewal of an authorisation for the interception, recording and transcription of electronic communications and for the installation of a real-time geolocation device must take place before the expiry of the previous authorisation.

Court of Cassation (Criminal Chamber) – 17 June 2025 (ruling in French language)

Background

French criminal procedure allows investigators, under judicial authorisation, to carry out measures for the capture of computer data from a terminal device in real time. In practice, such measures may involve accessing data stored on or transmitted by a device that may be located on the territory of another state.

The case concerned the lawfulness of the capture of computer data carried out while the targeted device was located abroad.

Court of Cassation ruling

The court examined the conditions under which computer data captured abroad may be used in French criminal proceedings.

The court deduced from the judgment of the Court of Justice of the European Union in case C-670/22 dated 30 April 2024 that Article 31 of Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters (EIO Directive) is applicable to measures involving the capture of computer data carried out on the territory of another EU Member State. Accordingly, where such a measure is implemented without requiring the technical assistance of the foreign state, the investigating authority must notify that EU Member State of the measure, in accordance with the notification mechanism provided for in Article 31 of the EIO Directive.

Greece

Supreme Court of Greece

Background

Greek law protects the confidentiality of communications, while allowing the interception of communications in criminal investigations under specific legal conditions. Article 5(10) of Law 2225/1994 provides that the content of correspondence or communication obtained following the lifting of confidentiality, along with any related information, may not be used as evidence in other criminal, civil, administrative or disciplinary proceedings for purposes other than those for which the measure was authorised.

Supreme Court ruling

The court held that 'another criminal trial' is understood to mean a criminal trial that is not identical to the one in which the evidence was lawfully obtained. Greek criminal proceedings begin with the initiation of criminal prosecution by the public prosecutor and retain their identity throughout their course, despite any procedural divisions that may occur. In order to fulfil the condition of regarding 'another trial', the two procedures (the one in which the evidence was legally obtained and the one in which it is used) must already be distinct at the stage of criminal prosecution or preliminary investigation; otherwise, a single criminal trial is deemed to exist, maintaining its character until its conclusion.

The court further noted that this interpretation reflects the intention of the legislator, who sought to exclude the use of completely random findings in cases with no connection, including procedural, to the original proceedings, in order to avoid unjustified infringements of the confidentiality of communications and the creation of a pool of information that could be used in unrelated cases.

However, the legislator did not intend to exclude the use of evidence lawfully obtained in cases that had already been revealed within the framework of the initial proceedings, particularly where the criminal conduct forms part of the same coherent set of events or the activities of the same criminal organisation. In such cases, the prohibition does not apply, and lawfully obtained evidence may be used to reveal additional crimes or perpetrators connected to the same criminal activity.

3.3. Crypto-assets

3.3.1. National court rulings

Estonia

Harju County Court and Tallinn District Court rulings

Background

Under Estonian law, the provision of virtual asset service provider (VASP) services requires authorisation from the Estonian Financial Intelligence Unit (FIU). Companies offering such services without a valid licence may incur criminal liability if they continue operating after the licence has expired.

The case concerned the company Garantex Europe OÜ, which previously held an FIU licence to provide virtual currency services. However, during the period 25 February 2022 to 20 April 2022, the company no longer held such a license, but the provision of services continued on the platform, with a total transaction volume exceeding USD 1.2 billion.

Harju County Court – 20 December 2024 (judgment in Estonian language)

The Harju County Court convicted two former members of the management board of Garantex Europe OÜ for conducting economic activities without the required licence for the provision of VASP services.

The evidence presented and examined in court did not support the defendants' claims that Garantex Europe OÜ lacked substantive economic activity, that the Estonian company had no connection to the platform used or the transactions carried out there, and that they were merely nominal board members without actual knowledge of, or influence over, the platform's operations or the management of the company.

The court held that although the situation may have formally appeared as if Garantex Europe OÜ had no economic activity during the relevant period, this did not mean that such activity did not in fact exist. In the court's assessment, the evidence indicated that during the relevant period Garantex Europe OÜ was connected to the provision of virtual currency services on the relevant platform.

Furthermore, the provision of services on the platform continued in the same manner as during the period when the company operated under a valid licence, and this was known to the defendants. The defendants actively performed board member duties, participated in discussions regarding the company's business model and restructuring, had access to the platform, and received remuneration and compensation for expenses.

The court further concluded that the unlicensed activity took place in Estonia, as the company was registered there, had previously operated under an FIU licence, and its management board, familiar with the business model, was located in Estonia. These connections were sufficient to establish Estonia as the place where the offence was committed.

Tallinn District Court – 22 April 2025 (judgment in Estonian language)

The Tallinn Circuit Court reviewed the appeal lodged by the defendants against the judgment of the Harju County Court. It dismissed the appeals and upheld the County Court's judgment, agreeing with the lower court's assessment of the evidence.

Harju County Court – 24 April 2025 (order in Estonian language)

Background

In the context of a money laundering investigation, Estonian authorities identified certain bitcoin addresses suspected of holding assets connected to criminal activity, the holders of which were unidentified.

Harju County Court ruling

The Harju County Court granted permission to prohibit transactions with bitcoins of an unidentified person or unidentified persons.

The court ordered the unidentified holders of the bitcoins at the specified addresses to contact the Central Criminal Police or the State Prosecutor's Office and to transfer the bitcoins that were the subject of the money laundering investigation to the deposit account of the Central Criminal Police.

The court also prohibited any future holders of the bitcoins (if they would be transferred in breach of the prohibition) from carrying out transactions with those bitcoins, and ordered them to contact the Central Criminal Police or the State Prosecutor's Office and to transfer the bitcoins suspected of money laundering to the deposit account of the Central Criminal Police.

Netherlands

District Court of Zeeland-West-Brabant – 31 January 2025 (ruling in Dutch language)

Background

The case concerned online banking fraud and the laundering of criminal proceeds through bank accounts and crypto-asset transactions. Victims were deceived into disclosing banking credentials and security information, enabling the perpetrators to gain unauthorised access to bank accounts and transfer funds. The defendant was involved both in the fraudulent schemes and in handling the proceeds obtained through those offences.

District Court ruling

The court convicted the defendant of co-perpetration of bank help-desk fraud, money laundering and forgery. It found that the defendant had knowingly participated in fraudulent online schemes and in concealing the criminal origin of the proceeds, including through crypto-asset transactions.

District Court of Northern Netherlands – 9 April 2026 (ruling in Dutch language)

Background

The case concerned a large-scale criminal organisation engaged in bank help-desk fraud, in which victims were deceived into disclosing banking credentials, verification codes and other security information. The perpetrators subsequently used this information to gain unauthorised access to victims' bank accounts, transfer funds and convert criminal proceeds into crypto-assets. The defendant played a leading and coordinating role within the organisation and was involved in laundering the criminal proceeds. The laundering operation concerned approximately EUR 6.5 million.

District Court ruling

The court found the defendant guilty of directing a criminal organisation engaged in bank help-desk fraud, as well as fraud, computer hacking and money laundering. It further found that the use of crypto-assets played an important role in concealing the origin and movement of criminal proceeds. Funds obtained through fraud were converted into crypto-assets and transferred through various

wallets and transactions in order to hinder tracing by the authorities. The defendant was sentenced to seven years of imprisonment and the court also ordered the forfeiture of crypto-assets valued at approximately EUR 2 million.

Portugal

Court of Appeal

Background

Portuguese criminal law criminalises fraud and money laundering, including the concealment and conversion of illicit proceeds. The case concerned the use of an online platform and crypto-assets to facilitate such activities.

Court of Appeal ruling

A Portuguese court of appeal held that the defendant's conduct in operating an online platform facilitating transactions in crypto-assets constituted part of criminal activity, involving the concealment and conversion of illicit proceeds through crypto-asset transfers.

The court analysed the way the defendant managed and moved crypto-asset proceeds and confirmed that the defendant knowingly facilitated transactions involving goods and services of illicit origin and used crypto-assets to conceal the nature and origin of the proceeds. The court further held that converting crypto-assets into euro in order to integrate them into the formal financial system constituted criminal conduct. The court therefore confirmed that this behaviour met the elements of fraud and money-laundering offences under the Portuguese Criminal Code.

The ruling clarified how Portuguese judicial authorities treat crypto-asset translations linked to criminal conduct (fraud and money laundering) under existing criminal law, even before the full implementation of the EU crypto-asset regulatory framework.

3.4. Artificial intelligence

3.4.1. National court rulings

Denmark

Danish Western High Court – 12 June 2025 (ruling in Danish language)

Background

Section 235 of the Danish Criminal Code criminalises, among other things, the production, possession and dissemination of sexual material depicting persons under the age of 18.

In the case, the defendant used AI tools to generate a large number of sexualised images depicting persons under 18 years of age. Approximately 36 000 such images were produced and some of them were disseminated online in exchange for payment.

Western High Court ruling

The court found the defendant guilty of violating Section 235 of the Danish Criminal Code. It held that the production, possession and dissemination of the AI-generated images constituted sexual material depicting persons under 18 years of age within the meaning of the provision.

The accused was sentenced to one year and six months' imprisonment. The court attached particular weight to the very large quantity of images produced and possessed and the fact that some of the material had been disseminated for payment.

The judgment has been appealed to the Supreme Court of Denmark, with a judgment still pending at the time when the information was provided for the purposes of drafting of this report. The offences were committed before the adoption of Law No 722 of 20 June 2025 (see Section 2.4.2 above), which subsequently strengthened the Danish legal framework concerning sexually offensive material, including AI-generated material.

Switzerland

Federal Supreme Court of Switzerland – 20 November 2025 (ruling in German language)

Background

Swiss criminal law prohibits the dissemination of pornographic material involving minors, including the sharing or making available of such material through online platforms. The prohibition applies regardless of whether the person sharing the material is the original creator of the content.

The case concerned the dissemination via Instagram of a video originally depicting two adults engaged in a sexual act, which had been altered using a de-aging filter so that the female performer appeared to be a minor.

Federal Supreme Court ruling

The Federal Supreme Court confirmed the conviction of a person who had shared the edited video on Instagram. It held that, although the original recording depicted adults, the application of a digital de-aging filter altered the visual appearance of the female performer so that she appeared to be underage. As a result, the video qualified as prohibited pornographic material involving minors within the meaning of Swiss criminal law.

The court further clarified that criminal liability for dissemination does not depend on the person having created the material or applied the filter themselves. It was sufficient that the accused knowingly shared the content, thereby making the prohibited material accessible to others.

The judgment therefore confirmed that digitally altered sexual material portraying adults as minors may fall within the scope of child sexual abuse material offences, and that persons who redistribute such content may incur criminal liability even if they were not involved in its creation.

4. Data retention

This chapter provides an overview of legislative, policy and/or case-law developments in the EU in the area of data retention following the 2014 judgment of the CJEU, which invalidated the Data Retention Directive (Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC).

4.1. EU level

➢ *Impact Assessment on Retention of data by service providers for criminal proceedings*

The issue of data retention has regained prominence in the broader context of access to e-evidence for criminal investigations. Following the annulment of the Data Retention Directive, EU law no longer provides for general obligations requiring electronic communications service providers to retain non-content data for law enforcement purposes. In the absence of a harmonised framework, EU Member States have adopted divergent approaches, while in some cases no mandatory retention rules are in place. This situation has been identified by judicial and law enforcement authorities as creating practical difficulties, in particular where data are no longer available at the time they are requested or where cross-border cooperation is affected by differing national regimes.

Against this background, the European Commission has initiated a process to assess whether further action at the EU level is warranted. In May 2025, it launched an Impact Assessment on Retention of data by service providers for criminal proceedings, aimed at examining the obstacles arising from the current legal fragmentation and identifying possible policy responses. The assessment covers both non-regulatory and regulatory options, including the potential introduction of harmonised retention obligations accompanied by safeguards governing access by competent authorities. Particular attention is given to ensuring compliance with fundamental rights, notably the requirements of necessity and proportionality as interpreted in the case-law of the CJEU. The outcome of this process may inform future legislative initiatives at the EU level.

EUROJUST In 2024, Eurojust issued a report on The effect of Court of Justice of the European Union case-law on national data retention regimes and judicial cooperation in the EU. This report served as an input to the work of the HLG on access to data for effective law enforcement referred to in Section 2.2.1 above and to the Roadmap for lawful and effective access to data for law enforcement, which subsequently informed the launch of the European Commission's Impact Assessment on Retention of data by service providers for criminal proceedings .

4.2. National level

Czechia

➢ *Decision No 30 Cdo/2556/2025*

The Supreme Court of the Czech Republic issued Decision No 30 Cdo/2556/2025, which obliged the state to apologise to a Czech journalist for the widespread and untargeted collection of his traffic and location data in violation of EU law.

Greece

➢ *Pending decision of the Plenary Session of the Supreme Court of Greece following Decision 587/2025*

In Decision 587/2025, issued by the 6th Section of the Supreme Court, the court examined issues concerning the investigation and seizure of communication data stored on digital equipment through OTT services, and the time frame applicable to obtaining past external communication data.

Because the 6th Section intended to adopt a position contrary to that taken by the Plenary Session of the Supreme Court in previous decisions, the case was referred to the Plenary Session for the resolution of key legal questions.

In particular, the Plenary Session is called upon to determine:

- whether the confidentiality of communications also applies to communication data (content and metadata) stored on digital equipment, and therefore whether compliance with the requirements of Article 5 of Law 2225/1994 and Article 8 of Law 5002/2022 is required; and
- if such compliance is required, whether communication data must be disclosed gradually and consecutively every 2 months, for a total period of 12 months under Law 2225/1994 (10 months under Law 5002/2022), or whether such a restriction does not apply to past communications.

A decision of the Plenary Session of the Supreme Court of Greece is pending at the time of drafting of this report.

Slovenia

Constitutional Court of Slovenia – 8 January 2026 (ruling in Slovenian language)

Background

The legal basis for the retention of traffic and location data by electronic communications providers in Slovenia was set out under the Electronic Communications Act. However, parts of this legislation were later repealed following a decision of the Constitutional Court, which found the retention regime unconstitutional in light of EU law and fundamental rights standards.

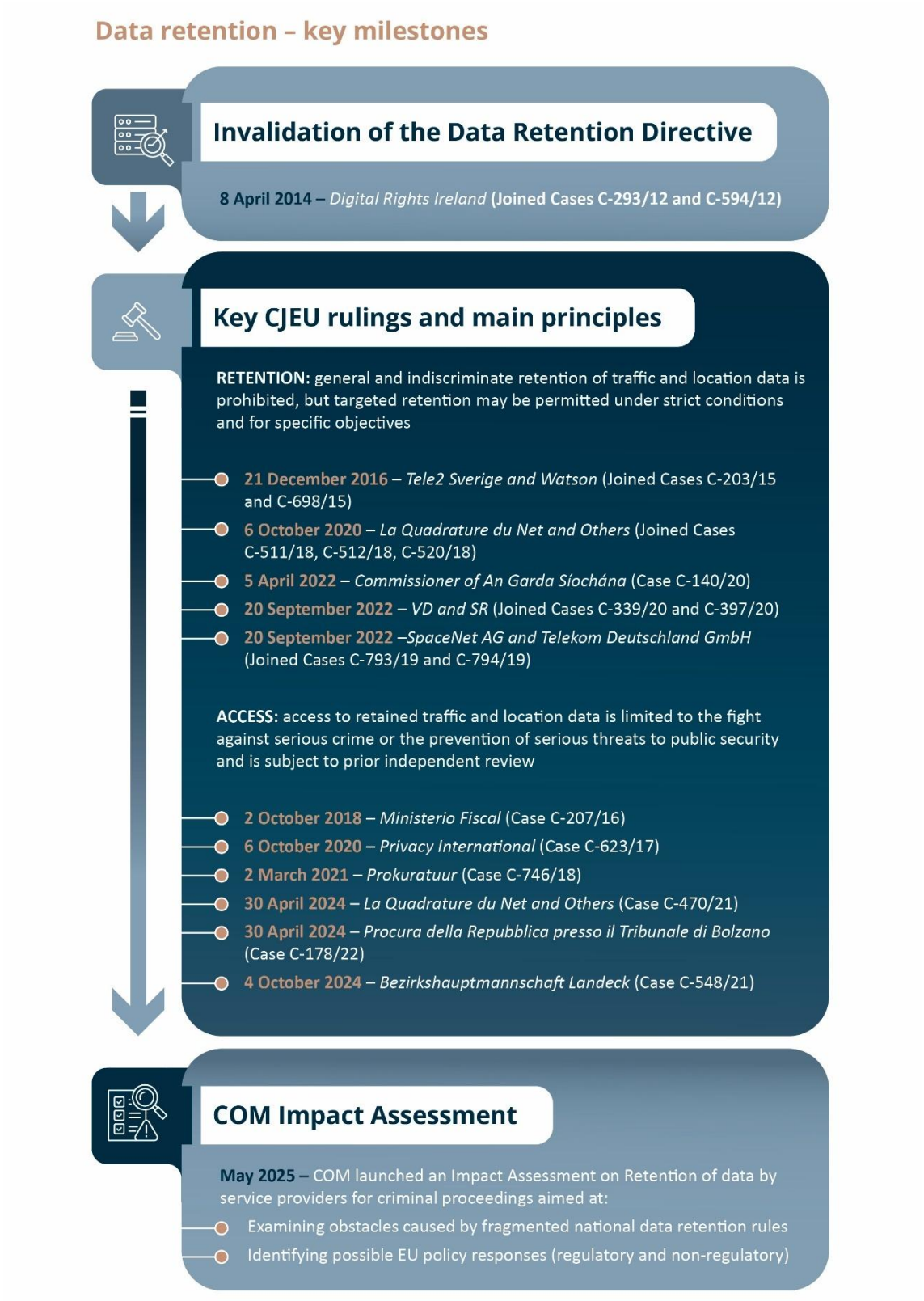
Questions subsequently arose as to whether traffic data that had already been stored under the unconstitutional legal framework could nevertheless still be used as evidence in criminal proceedings.

Constitutional Court ruling

The Constitutional Court held that if traffic data has been retained on the basis of legislation that is unconstitutional, the subsequent use of that data in criminal proceedings cannot be regarded as constitutionally compliant. In reaching this conclusion, the Court referred to the case-law of the ECtHR, in particular the judgment in the case of *Škoberne v. Slovenia* (Application No 19920/20), which addressed the use of telecommunications data obtained under an unlawful legal basis.

As a result, the decision limits the possibility of using traffic data retained under the previously repealed provisions of the Electronic Communications Act in criminal proceedings.

At the time of the decision, it remained uncertain how this ruling would influence future legislative regulation of data retention in Slovenia.



5. 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 field of combating cyber-dependent and cyber-enabled crime.

Future issues of the CJM will continue to focus on legislative and policy developments in the area of cybercrime, e-evidence gathering, crypto-assets and AI, as well as the assessment of relevant court decisions in these areas. Developments concerning data retention will remain under review for as long as they are pertinent.

The CJM is mainly based on input from practitioners, and this collaborative approach will continue in future issues. We would like to thank the experts of the EJCN for their valuable contributions to this issue.

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

PDF: Catalogue number: QP-01-26-014-EN-N • ISBN: 978-92-9404-569-0 • DOI: 10.2812/6202096

Eurojust is an agency of the European Union