Cybercrime Judicial Monitor

Issue 8 – June 2023

Criminal justice across borders

EUROJUST

European Union Agency for Criminal Justice Cooperation

EUROPEAN JUDICIAL CYBERCRIME NETWORK

Executive Summary

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

Last year, several legislative developments at the EU and national levels were noticed. Some procedures are ongoing in the EU (e.g. the Artificial Intelligence Act, the regulation on preventing and combating child sexual abuse, the digitalisation of the EU justice system), but others have already been completed and will have to be complied with (e.g. Digital Services Act), or incorporated into national law (e.g. the network and information security directive). Some EU Member States reported the introduction of certain changes to existing legislation, mainly in the area of (extended) search capabilities in information systems.

Several European countries reported 2022 court rulings on the culpability of persons operating darknet marketplaces and on the use of captured encrypted communication data. Up to now, the majority of rulings appear favourable for prosecuting authorities. Some countries also reported upcoming legislation or recent rulings on freezing cryptocurrency assets.

In the past year, the Court of Justice of the European Union (CJEU) concluded three preliminary rulings, providing additional guidance concerning the implementation of (supranational) data retention rules in European countries. Some EU Member States reported new pieces of national legislation in the area of data retention, whereas others reported 2022 domestic court rulings related to, and/or in line with, (earlier) CJEU rulings about data retention. Only in cases when national security is at stake, there appears to be room for retaining and requesting/collecting electronic (meta)data.

The 'topic of interest' section of this eighth issue of the CJM provides information on e-evidence, focusing on recent legislative developments such as an EU regulation and directive. The key components of the legislative package, the European production order and the European preservation order, are explained in detail. It can be concluded that the adoption of this legislation concerning e-evidence is a significant step forward concerning access to digital information in cross-border criminal investigations and prosecutions, mainly by expediting and simplifying related processes.

Table of Contents

1. Introduction

Eurojust presents the eighth issue of the *Cybercrime Judicial Monitor* (CJM). The CJM is published once a year and distributed to judicial and law enforcement authorities active in the field of preventing and combating cyber-dependent and cyber-enabled crime.

The CJM is produced on the basis of information provided by members of the European Judicial Cybercrime Network. About 60% of the members replied to this year's questionnaire. All issues of the CJM are available on the Eurojust website.

Same as in previous editions, the CJM consists of three main sections, followed by a section on a 'topic of interest'. For this eighth issue of the CJM, Eurojust selected 'e-evidence' as the topic of interest, with a focus on recent legislative developments in this area.

2. Legislation

The objective of this chapter is to provide information on developments in international, EU and national legal instruments in relation to cybercrime in 2022. The main sources of national information presented in Sections 2.3 and 2.4 are contributions collected through the European Judicial Cybercrime Network. In contrast with previous editions of the CJM, a table has been added to Section 2.3, allowing for a better overview of legislative developments and their anticipated effect in several EU Member States.

2.1. International level

- *Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence (Budapest Convention)*

As reported in the seventh issue of the CJM, the Committee of Ministers of the Council of Europe adopted the Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence on 17 November 2021. This Second Additional Protocol supplements the Convention on Cybercrime and its First Protocol. It aims to further enhance the ability of criminal justice authorities to obtain electronic evidence from another jurisdiction, for the purpose of specific criminal investigations or proceedings. Details of the protocol can be found on the website of the Council of Europe ([1]).

On 12 May 2022, the Second Additional Protocol was opened for signature. On 14 February 2023, the Council of the European Union adopted a decision authorising EU Member States to ratify the Second Additional Protocol ([2]).

2.2. EU level

- *Procedure 2021/0106/COD (Artificial Intelligence Act - legislative procedure)*

On 21 April 2021, the European Commission announced the proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (AI) – the **Artificial Intelligence Act** – and amending certain Union legislative acts ([3]). The proposed regulation lays down a uniform legal framework for the development, marketing and use of AI. It also aims to address the risks of specific uses of AI to ensure the trustworthiness of AI systems.

On 3 May 2022, the European Parliament adopted the resolution on artificial intelligence in the digital age (2020/2266(INI)) ([4]).

On 28 September 2022, the European Commission announced its proposal for a directive on AI ([5]). The objective of the proposed directive is to promote the rollout of trustworthy AI to harvest its full benefits for the internal market, by ensuring that victims of damage caused by AI obtain equivalent protection to victims of damage caused by products in general. It also reduces legal uncertainty for businesses developing or using AI regarding their possible exposure to liability and prevents fragmented AI-specific adaptations of national civil liability rules.

([1]) Full text of the Second Additional Protocol.
([2]) Press release of the Council of the European Union.
([3]) Full text of the proposal for a regulation.
([4]) Full text of the resolution on artificial intelligence in a digital age.
([5]) Full text of the proposal.

On 6 December 2022, following multiple amendments and discussions, the Council of the European Union approved a compromise version of the proposed regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (the Artificial Intelligence Act) and amending certain Union legislative acts ([6]).

The current draft version of the proposed Artificial Intelligence Act will have to be adopted by the European Parliament (expected mid-June 2023). Following this vote, discussions between EU Member States, the European Parliament and the European Commission could commence, and adoption of the final Artificial Intelligence Act could be envisaged by the end of 2023.

- *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)*

In December 2020 the European Commission presented the **Digital Services Act package**, consisting of the Digital Services Act (DSA) and the Digital Markets Act. These new rules govern the digital space and digital services, including social media platforms. The DSA focuses on creating a safer online environment for users and companies and on protecting fundamental rights in the digital space. It lays down a set of responsibilities and a clear accountability and transparency framework for providers of intermediary services (e.g. online marketplaces and content-sharing platforms), regardless of the location of these providers, within or outside the EU.

On 4 October 2022, the Council of the European Union adopted the Digital Services Act. On 19 October 2022, Regulation (EU) 2022/2065 was adopted ([7]). The DSA was published on 27 October 2022 and came into force on 16 November 2022. The DSA will be directly applicable across the EU; Article 93 of the regulation stipulates that the new rules shall apply from 17 February 2024 onwards.

The Intellectual Property Crime Project hosted at Eurojust published a factsheet about the DSA.

- *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 directive)*

The **network and information security directive** (NIS 2) introduces new rules to ensure a high common level of cybersecurity across the EU, both for companies and countries. It also strengthens cybersecurity requirements for medium-sized and large entities that operate and provide services in key sectors. It concerns an update of the 2016 NIS directive, and aims to improve clarity and implementation and to address fast-paced developments in the area of cybersecurity.

After the approval of the European Parliament and the Council of the European Union in November 2022, Directive (EU) 2022/2555 was adopted on 14 December 2022 ([8]). EU Member States have 21 months from the entry into force (on the 20th day following publication) to incorporate the provisions into their national law.

([6]) Compromise version of the proposal for a regulation (pdf).
([7]) Full text of Regulation (EU) 2022/2065.
([8]) Full text of Directive (EU) 2022/2555.

- *Proposal for a regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse*

On 10 September 2020, the European Commission presented a first legislative proposal containing an interim regulation allowing certain interpersonal communication services to derogate from established privacy rules to enable them to continue detecting and reporting child sexual abuse material online on a voluntary basis. Regulation (EU) 2021/1232 of the European Parliament and of the Council of 14 July 2021, which concerned a temporary derogation from certain provisions of Directive 2002/58/EC as regards the use of technologies by providers of number-independent interpersonal communications services for the processing of personal and other data for the purpose of combating online child sexual abuse, was adopted on 14 July 2021 and entered into force on 2 August 2021 ([9]). It will no longer be valid on 3 August 2024.

On 11 May 2022, the European Commission aimed to replace the interim regulation by proposing the **regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse** ([10]). Compared to the interim rules, the proposed regulation includes mandatory measures to detect and report child sexual abuse material.

On 29 July 2022, the European Data Protection Board and the European Data Protection Supervisor adopted a Joint Opinion on the proposed regulation, considering risks posed by it. Several EU Member States have provided their opinions on the proposal to the Presidency of the Council of the European Union. On 12 October 2022, the Czech Presidency of the Council of the European Union presented a new compromise text on the proposed regulation. The legislative procedure is ongoing.

- *Procedure 2021/0394/COD and Procedure 2021/0395/COD (Digitalisation of EU Justice System)*

In December 2021 the European Commission proposed two pieces of legislation concerning the **digitalisation of the EU justice system**, in reaction to the COVID-19 pandemic ([11]). The proposed regulation aims to ensure access to justice in cross-border cases in the EU, and to make sure EU Member States' judicial cooperation is maintained in the event of *force majeure*. The related directive ([12]) should reflect the changes introduced by the regulation on the use of digital technology to other legal acts to ensure legal certainty. The package seeks to reduce disparities in digitalisation between EU Member States to ensure that all EU citizens can benefit from effective access to justice.

On 1 March 2023, in a joint vote, the European Parliament Committee on Legal Affairs (JURI) and Committee on Civil Liberties, Justice and Home Affairs (LIBE) backed a legislative package on the digitalisation of judicial cooperation in the EU ([13]). The legislative procedure is ongoing.

- *Procedure 2018/0107/COD and Procedure 2018/0108/COD (e-evidence)*

On 25 January 2023, the Swedish Presidency of the Council of the European Union confirmed that an agreement was reached with the European Parliament on new rules to improve **cross-border access to e-evidence** ([14]).

([9]) Full text of Regulation (EU) 2021/1232.
([10]) Full text of the proposal for a regulation.
([11]) Full text of the proposal for a regulation.
([12]) Full text of the proposal for a directive.
([13]) Press release of the European Parliament of 1 March 2023.
([14]) Electronic evidence: Council confirms agreement with the European Parliament on new rules to improve cross-border access to e-evidence - Consilium (europa.eu).

More information about the (draft) regulation and directive and about ongoing legislative developments (e.g. proposal for a regulation of the European Parliament and of the Council on European production and preservation orders for electronic evidence in criminal matters) can be read in the fifth chapter of this report. A link to the compromise text is included there.

2.3. EU Member States and non-EU countries

EU Member States		
Country	**New law/amendment**	**Effect/summary**
France	Article L111-7-3 of the Code de la consommation *Entry into force on 1 October 2023*	**Compelling** online platform operators to carry out a cybersecurity audit and to make the results available to users of these platforms.
	Article 323-4-2 of the Code penal *Entered into force on 26 January 2023*	**Criminalising** and punishing deliberate endangerment of life in case of a cyberattack.
Latvia	Section 219 of the Law on Criminal Procedure supplemented with part 2. *Entered into force on 3 November 2022*	**Allowing** access to data stored in an information system located outside the jurisdiction of any country that can be accessed by authorised persons through investigations the system mentioned in the judge's decision. A new decision is not necessary, and if the jurisdiction of the information system is clarified during the criminal proceedings, the person in charge of the process contacts the state under whose jurisdictions the information is located, in accordance with the procedures specified in Chapters 83 and 83.1 of the Criminal Procedure Law.
Netherlands	Article 556 of the Criminal Procedure Code *Entered into force on 1 October 2022, for a period of 2 years*	**Allowing** to view or store data that arrives after a device was seized; approval by the supervisory judge is required.
	Article 557 of the Criminal Procedure Code *Entered into force on 1 October 2022, for a period of 2 years*	**Creating** the possibility to search remotely in a different automated system linked to a seized device; approval by the supervisory judge is required.

	Article 558 of the Criminal Procedure Code *Entered into force on 1 October 2022, for a period of 2 years*	**Creating** the possibility to use proportionate coercion to have a suspect unlock a seized device; no approval supervisory judge required.
Sweden	28 kap 10 a – e § of the Code of Judicial Procedure (extended search provisions) *Entered into force on 1 June 2022*	**Creating** the possibility to search through a different readable information system remotely; competences differ based on the severity of the crime and the object of the search.

3. Judicial analysis

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

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

3.1. Selected court rulings

EU Member States		
Country	**Court level and case**	**Ruling**
Denmark	Copenhagen City Court, NSK SØK-10177-00165-22 *14 July 2022*	This ruling concerned a request for **asset freezing** against a person provisionally charged with money laundering. The Court ruled in favour regarding the purpose of the freezing and the fulfilment of the conditions for asset freezing under Danish law, **approving the transfer of any deposits to different financial accounts**.
	Copenhagen City Court, Prosecution Division SØK-10177-00182-22 *27 September 2022*	The Court **ordered the handing over** of all account information and other written material – including account-opening documents, transaction lists, account statements in electronic format, underlying transaction documentation, IP addresses and port numbers – regarding accounts and **crypto wallets** owned by or having been at the disposal of a suspect, when **such information may serve as evidence in the case** and there are **no circumstances that may prevent disclosure of information.**
	Court of Aarhus, 6-10403/2022 *22 December 2022*	This case concerned a request to **freeze any balances stored on a cryptocurrency platform** belonging to a person suspected of drug smuggling, as part of the financial investigation, based on the grounds that assets should be confiscated as proceeds of crime, in order to secure the state's claim for coverage of the costs of the case, claims for confiscation of assets and any fines imposed. Based on the fact that large quantities of drugs had been traded, that the estimated proceeds of the crime

		could not be identified in the suspect's bank accounts and that the suspect held an account with a cryptocurrency platform, the Court ruled that the **requirements for issuing a freezing order under Danish law were fulfilled**, and that any balance in the cryptocurrency platform belonging to the suspect could be frozen.
Germany	German Federal Court of Justice, Case No. 5 StR 457/21, 'EncroChat' *2 March 2022*	The Federal Court of Justice dismissed the appeal lodged following a judgment passed by the Hamburg Regional Court on 15 July 2021 (sentence for offences of drug trafficking). The Court ruled that **the 'EncroChat' data forwarded by France could be used as evidence if they served the purpose of investigating serious criminal offences**.
	German Federal Court of Justice, Case No. 2 StR 12/22, 'Wall Street Market' *2 June 2022*	The Federal Court of Justice was asked for the first time to decide whether the operation of a darknet marketplace, which neither requires or facilitates a connection between platform operators and sellers or physical proximity to the sales transactions, also constitutes a drug trafficking offence. On 2 July 2021, the Regional Court of Frankfurt am Main sentenced three German administrators of the darknet marketplace 'Wall Street Market' to several years of imprisonment for drug trafficking. The Federal Court of Justice confirmed this conviction, stating that **the provision of a virtual sales and communication platform, exclusively for the purpose of trading in narcotics, and the contributions made to regularly maintain the technical and content-related forum structure constitute criminal drug trafficking, provided that the operators do not act solely out of disinterested motives**. The fact that the three administrators did not have physical control over the narcotics sold nor specify the type, quantity and price of the drugs traded of their place of delivery, would not force the assumption that they were merely assisting in the commission of an unlawful act. According to the established case law, trafficking within the meaning of Section 29 (1) sentence 1 no. 1 of the German Narcotics Act is **any self-interested activity aimed at the turnover of narcotics**.

France	Court of Cassation, 'EncroChat' Case *11 October 2022*	The Court legitimated the provisions of Article 706-102-1 of the French Criminal Code **to authorise and execute the capture of data**. Additionally, the Court decided that the **capturing technique could be secret** for reasons of national security. The above ruling followed an earlier favourable decision by the French Constitutional Court on 8 April 2022.
Italy	Italian Supreme Court of Cassation, Criminal Section IV, Case No. 32915/22 *15 July 2022*	The Italian Supreme Court of Cassation dealt with a referral from the lower tribunal of Rome, that **denied a defendant's request to disclose information about the police methods to acquire and decrypt SkyECC data**. It was argued that since the material was acquired by Europol and foreign judicial authorities based on a European investigation order, **the information could be used without any further scrutiny based on the presumption that the interception was legally carried out**. On the contrary, the Supreme Court of Cassation ruled that the encrypted messages obtained by Europol and foreign authorities **could not be used in a pre-trial hearing unless prosecutors explained how such evidence was obtained**. It explained that the principle of cross-examination implies a procedural dialectic, not only with regard to the screening of the acquired material, but also to the manner of acquisition of said material. According to the Supreme Court, **a defendant should be able to question not only the content, but also the acquisition and investigation procedure of this material**, in order to give full rights to the defence and in order to assess the relevance, reliability and demonstrative value of the evidence. The case was sent back for a new judgment.
	Italian Supreme Court of Cassation, Case No. 6363-23 *13 October 2022*	In a similar case concerning encrypted communication data, the Italian Supreme Court of Cassation ruled that **the activity of acquiring and decrypting such data does not fall within the category of interception activities since these activities presuppose the collection of a flow of ongoing communications**. The defence appealed the decision by the lower instance tribunal that the data could be used, referring to the decision of the Italian Supreme Court of Cassation of 15 July 2023 (32195-22). The Supreme Court considered the reference by the defence to the earlier ruling irrelevant, as in this case no request was made to receive

		information about the international investigation and acquisition methods. Finally, the Supreme Court stressed that **documents transmitted following a European Investigation order are not conditional on the assessment by Italian authorities of the regularity of the acquisition activities carried out by foreign authorities**, based on the principle of mutual trust and on the presumption that these were conducted lawfully.
	Italian Supreme Court of Cassation, Case No. 6364-23 *13 October 2022*	The Supreme Court returned to address the issue of the usability of chats via encrypted communication platforms such as SkyECC and Encrochat. The court provides not only **a definition of such instruments**, but also further clarifies that **it concerns data obtained following the execution of an EIO, and not an active interception of data/communication**.
	Italian Supreme Court of Cassation, Case No. 16347-23 *5 April 2023*	This concerns another ruling by the Supreme Court of Cassation in the area of encrypted communication data, upholding the earlier ruling(s) by further specifying **that the information received had already been documented (following acquisition and decryption) in a different judicial proceeding, and does not require consent of the original data controller**.
	Italian Supreme Court of Cassation, Case No. 18514-23 *4 May 2023*	In this case all documents made available by French authorities on the acquisition of encrypted communication data were provided to the defence. Related EIOs were issued to acquire evidence already available to France, not to request interception of telecommunications. French law allows to rely on national defence secret, so modalities of data gathering do not have to be revealed. A certification of authenticity of the transferred data was provided by France. Having issued the EIOs, Italy must **presume that the evidence was gathered lawfully**, and Italian judges can **only verify if the evidence was gathered in violation of fundamental principles of Italian law**, i.e. right of access of the case file and right to a fair trial. In addition to above, in 2023 there appear to be several other rulings by the Italian Supreme Court of Cassation concerning encrypted communication platforms such as SkyECC and Encrochat, upholding the earlier positive decisions about validity and usability of acquired data in court proceedings.

Netherlands	Netherlands Supreme Court, Case no. 2022:900, 'Ennetcom' *28 June 2022*	The Netherlands Supreme Court was asked for the first time to decide on the **legality of the use of data from encrypted telephone communications**. The Court ruled that the data transferred by Canadian authorities were **legitimately used as evidence in a criminal proceeding**.
	Amsterdam District Court, Case no. 71/234728-21 *21 November 2022*	This decision concerned the hacking of the Antwerp Euroterminal in Belgium in 2020. Suspects were involved in the large-scale import and trading of cocaine. The investigation started based on intercepted messages coming from EncroChat and SkyECC. The defence contested the legitimacy of the operations regarding these encrypted communication services. The Court found that **these operations were legitimate and that they were carried out in accordance with national law**.
Sweden	Svea Court of Appeal *17 June 2022*	Following an indictment on 12 February 2020, a Swedish national was acquitted by the Stockholm District Court on 9 July 2020. The accused had been under investigation for operating a darknet marketplace, and was indicted for drug offences and money laundering, among other things. Forfeiture of assets had been demanded. On 17 June 2022 the Svea Court of Appeal **ruled that the suspect was responsible for each unique drug transfer on the marketplace**, of which there were an estimated 311 000, with the estimated criminal turnover being 49 000 BTC. The profit (a 3% fee) for the suspect amounted to 1 479 BTC in total. The suspect was convicted of drug offences and money laundering, and sentenced to 11 years and 8 months of imprisonment. **The request for forfeiture of cryptocurrency assets was upheld**. An appeal was lodged with the Swedish Supreme Court and is currently pending. The evidence in the case consisted mainly of server material and communications obtained with international legal assistance, along with information from companies that could be used to track cryptocurrency transactions from the marketplace, and other findings related to the marketplace and the accused. In the collected server material there were, among other things, databases for the marketplace's users and bitcoin management, which could be used to

		calculate how many trades had taken place and which products had been traded during the marketplace's lifetime. By analysing withdrawals from the marketplace, bitcoin transactions in complex money-laundering arrangements could be traced back to the accused. **The criminal profit was forfeited for its total value immediately after the final judgment was passed**. Some legal challenges were identified in this case: **seizing cryptocurrency is problematic by nature, as cryptocurrencies are immaterial and virtual**. Legislation in Sweden concerning the seizing and forfeiture of assets was created for traditional (fiat) money. **Presenting cryptocurrency tracing and its attribution to suspects as (digital) evidence in court is difficult**. Securing cryptocurrency assets is possible in Sweden (a custodian wallet is required for this) **if the balance in a digital wallet belonging to the suspect is within the jurisdiction or if it is located outside Swedish jurisdiction**. The latter requires a **freezing order to the country where the provider is based. When the verdict is final and no longer appealable, forfeiture can be carried out, and the digital transfer from a third party takes place.**
Non-EU countries		
Country	**Court level and case**	**Ruling**
Norway	Norway Supreme Court Case no. HR-2022-1314-A *30 June 2022*	The Supreme Court ruled in favour of an earlier decision by the Oslo District Court that **material from an encrypted communication service (i.e. EncroChat) was allowed as evidence** in a criminal case of drug trafficking. This decision was first upheld by the Norwegian Court of Appeal. The premise for the Supreme Court's conclusion was that **the evidence had been legally acquired under French law**.
	Norway Supreme Court Case no. HR-2022-2125-U *4 November 2022*	The Supreme Court's Appeals Selection Committee ruled in favour of an earlier decision by the Court of Appeal (see Case no. HR-2022-1314-A above), **having correctly dismissed the defendant's request to exclude 'EncroChat' data as evidence**. The appellants raised the issue of the exclusion of EncroChat material once more, as the French Court of

		Cassation had ruled on the EncroChat case on 11 October 2022 (see further information above).

No relevant court decisions or judgments were reported or noted in **Cyprus**, but national law enforcement authorities and the Financial Intelligence Unit are **preparing guidelines on how to confiscate cryptocurrency**.

A regional court in **Germany** has requested a preliminary ruling by the CJEU on fourteen questions concerning a case involving '**EncroChat'** data. Two British detainees in the **United Kingdom** have lodged complaints with the European Court of Human Rights about the use of '**EncroChat'** data in their court cases.

No national court rulings were reported by prosecutors in 2022 in **Slovakia**. Following the decision of the CJEU in Case C-724/19, some courts **refused to issue the national warrant supporting the European investigation order received requesting to obtain traffic and location data associated with telecommunications.** No specific decisions in case of refusal were issued.

In **Sweden**, there is a pending case before the Swedish Supreme Court regarding the **new rules of extended searches** and whether or not they can be used in cases where data is stored in another country and/or in cases of loss of location, or whether such a coercive measure falls outside the jurisdiction of Swedish authorities. The decision is expected to be issued later this year.

In the canton of Basel, in **Switzerland**, a person was convicted of drug trafficking and money laundering. In this judgment, the **exploitability of SkyECC data** was discussed. The judgment has not been published yet. According to open-source reporting, the authenticity of the SkyECC communication data was questioned by the defence. The court did not agree with this, but doubted **whether the incriminating communication could be attributed to the accused**.

4. Data retention developments in Europe

The objective of this section is to provide an overview of the legislative and/or case-law developments in Europe in the area of data retention following the ruling of the CJEU in 2014 invalidating the Data Retention Directive (2006/24/EC) and the subsequent CJEU ruling in the Tele2 and Watson case of 21 December 2016.

4.1. Developments at the EU level (legislation and court rulings)

Rulings of the Court of Justice of the European Union

- **Judgment: Commissioner of An Garda Síochána – Case C-140/20**

Date: 5 April 2022

Judgment rendered by the Grand Chamber of the Court

Reference for a preliminary ruling by the Supreme Court of Ireland

Concerning: Interpretation of Article 15(1) of Directive 2002/58/EC, read in the light of Articles 7, 8, 11 and 52(1) of the Charter of Fundamental Rights of the European Union.

Questions referred for a preliminary ruling and considered by the court.

1. Is a general/universal data retention regime per se contrary to the provisions of Article 15 of Directive 2002/58/EC, interpreted in the light of the Charter, even if it is subject to stringent restrictions on retention and access?
2. In considering whether to grant a declaration of inconsistency of a national measure implemented pursuant to Directive 2006/24/EC, and making provision for a general data retention regime (subject to the necessary stringent controls on retention and/or in relation to access), and in particular in assessing the proportionality of any such regime, is a national court entitled to have regard to the fact that data may be retained lawfully by service providers for their own commercial purposes, and may be required to be retained for reasons of national security excluded from the provisions of Directive 2002/58/EC?
3. In the context of determining the compatibility with EU law and in particular with the Charter of Fundamental Rights of a national measure for access to retained data, what criteria should a national court apply in considering whether any such access regime provides the required independent prior scrutiny as determined by the CJEU in its case-law? In that context, can a national court, in making such an assessment, have any regard to the existence of *ex post* judicial or independent scrutiny?
4. In any event, is a national court obliged to declare the inconsistency of a national measure with the provisions of Article 15 of Directive 2002/58/EC, if the national measure makes provision for a general data retention regime for the purpose of combating serious crime, and where the national court has concluded, on all the evidence available, that such retention is both essential and strictly necessary to the achievement of the objective of combating serious crime?
5. If a national court is obliged to conclude that a national measure is inconsistent with the provisions of Article 15 of Directive 2002/58/EC, as interpreted in the light of the Charter of Fundamental Rights, is it entitled to limit the temporal effect of any such declaration, if it is satisfied that a failure to do so would lead to 'resultant chaos and damage to the public interest'

(in line with the approach taken, for example, in *R (National Council for Civil Liberties)* v *Secretary of State for Home Department and Secretary of State for Foreign Affairs* [2018] EWHC 975, at paragraph 46)?

6. May a national court invited to declare the inconsistency of national legislation with Article 15 of Directive 2002/58/EC, and/or to disapply this legislation, and/or to declare that the application of such legislation had breached the rights of an individual, either in the context of proceedings commenced in order to facilitate an argument in respect of the admissibility of evidence in criminal proceedings or otherwise, be permitted to refuse such relief in respect of data retained pursuant to the national provision enacted pursuant to the obligation under Article 288 of the Treaty on the Functioning of the European Union to faithfully introduce into national law the provisions of a directive, or to limit any such declaration to the period after the declaration of invalidity of Directive 2006/24/EC issued by the judgment of 8 April 2014, ***Digital Rights Ireland Ltd* v *Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*** (C-293/12 and C-594/12)?'

Court ruling:

- Article 15(1) of Directive 2002/58/EC must be interpreted as **precluding** legislative measures which, as a preventive measure for the purposes of combating serious crime and preventing serious threats to public security, provide for the general and indiscriminate retention of traffic and location data. However, Article 15(1), read in the light of Articles 7, 8, 11 and 52(1) of the Charter of Fundamental Rights, does **not preclude** legislative measures that, for the purposes of safeguarding national security, combating serious crime and preventing serious threats to public security, provide for:
  - the **targeted retention of traffic and location data which is limited**, on the basis of objective and non-discriminatory factors, according to the **categories of persons concerned or using a geographical criterion**, for a period that is **limited in time** to what is strictly necessary, but which may be extended;
  - the **general and indiscriminate retention of internet protocol (IP) addresses assigned to the source** of an internet connection for a period that is **limited in time** to what is strictly necessary;
  - the **general and indiscriminate retention of data relating to the civil identity of users of electronic communications systems**; and
  - recourse to an **instruction** requiring providers of electronic communications services, by means of a decision of the competent authority that is subject to effective judicial review, to undertake, for a **specified period of time**, the **expedited retention of traffic and location data** in the possession of those service providers.

  This is the case provided that those measures ensure, by means of clear and precise rules, that the retention of data at issue is subject to compliance with the applicable substantive and procedural conditions and that the persons concerned have **effective safeguards** against the risks of abuse.
- Article 15(1) of Directive 2002/58/EC must be interpreted as precluding national legislation pursuant to which the **centralised processing of requests for access to data**, which have been retained by providers of electronic communications services, issued by the police in the context

of the investigation or prosecution of serious criminal offences, is the responsibility of a police officer, who is assisted by a unit established within the police service which has a degree of autonomy in the exercise of its duties, and whose decisions may subsequently be subject to judicial review.

- EU law must be interpreted as **precluding a national court from limiting the temporal effects of a declaration of invalidity** which it is bound to make, under national law, with respect to **national legislation imposing on providers of electronic communications services the general and indiscriminate retention of traffic and location data**, owing to the incompatibility of that legislation with Article 15(1) of Directive 2002/58/EC. The admissibility of evidence obtained by means of such retention is, in accordance with the principle of procedural autonomy of the Member States, a matter of national law, subject to compliance, inter alia, with the principles of equivalence and effectiveness.

- **Judgment: VD and SR – Joined Cases C-339/20 and C-397/20**

Date: 20 September 2022

Judgment rendered by the Grand Chamber of the Court

Reference for a preliminary ruling by: Court of Cassation of France

Concerning: Interpretation of Article 12(2)(a) and (d) of Directive 2003/6/EC Article 15(1) and Article 23(2)(g) and (h) of Regulation (EU) No 596/2014, read in conjunction with Article 15(1) of Directive 2002/58/EC and in the light of Articles 7, 8 and 11 and of Article 52(1) of the Charter of Fundamental Rights of the European Union.

Questions referred for a preliminary ruling and considered by the court.

1. Do Article 12(2)(a) and (d) of Directive 2003/6/EC of the European Parliament and of the Council of 28 January 2003 on insider dealing and market manipulation, and Article 23(2)(g) and (h) of Regulation (EU) No 596/2014 of the European Parliament and of the Council of 16 April 2014 on market abuse, read in the light of recital 65 of that regulation, not imply that, account being taken of the covert nature of the information exchanged and the fact that the potential subjects of investigation are members of the general public, the national legislature must be able to require electronic communications operators to retain connection data on a temporary but general basis in order to enable the administrative authority referred to in Article 11 of the directive and Article 22 of the regulation, in the event of the emergence of grounds for suspecting certain persons of being involved in insider dealing or market manipulation, to require the operator to surrender existing records of traffic data in cases where there are reasons to suspect that the records linked to the subject matter of the investigation may prove relevant to the production of evidence of the actual commission of the breach, to the extent, in particular, that they offer a means of tracing the contacts established by the persons concerned before the suspicions emerged?
2. If the answer given by the CJEU is such as to prompt the Cour de cassation (Court of Cassation) to form the view that the French legislation on the retention of connection data is not consistent with EU law, could the effects of that legislation be temporarily maintained in order to avoid legal uncertainty and to enable data previously collected and retained to be used for one of the objectives of that legislation?

3. Can a national court temporarily maintain the effects of legislation enabling the officials of an independent administrative authority responsible for investigating market abuse to obtain access to connection data without prior review by a court or another independent administrative authority?

Court ruling:

- Article 12(2)(a) and (d) of Directive 2003/6/EC and Article 23(2)(g) and (h) of Regulation (EU) No 596/2014, read in conjunction with Article 15(1) of Directive 2002/58/EC and in the light of Articles 7, 8 and 11 and of Article 52(1) of the Charter of Fundamental Rights of the European Union must be interpreted as **precluding legislative measures which**, as a preventive measure, in order to combat market abuse offences, including insider dealing, **provide for the general and indiscriminate retention of traffic data for a year from the date on which they were recorded**.
- European Union law must be interpreted **as precluding a national court from restricting the temporal effects of a declaration of invalidity** which it is required to make, under national law, with respect to provisions of national law which, first, **require operators providing electronic communications services to retain generally and indiscriminately traffic data** and, second, **allow such data to be submitted to the competent financial authority**, **without prior authorisation from a court or independent administrative authority**, owing to the incompatibility of those provisions with Article 15(1) of Directive 2002/58, as amended by Directive 2009/136, read in the light of the Charter of Fundamental Rights. The admissibility of evidence obtained pursuant to provisions of national law that are incompatible with EU law is, in accordance with the principle of procedural autonomy of the Member States, a matter for national law, subject to compliance, inter alia, with the principles of equivalence and effectiveness.

- **Judgment:** SpaceNet AG (C-793/19) and Telekom Deutschland GmbH – Joined Cases C-793/19 and C-794/19

Date: 20 September 2022

Judgment rendered by the Grand Chamber of the Court

Reference for a preliminary ruling by the Federal Administrative Court of Germany

Concerning: Interpretation of Article 15(1) of Directive 2002/58/EC, read in the light of Articles 6 to 8 and 11 and 52(1) of the Charter of Fundamental Rights of the European Union and Article 4(2) of the Treaty on European Union.

Questions referred for a preliminary ruling and considered by the court.

1. In the light of Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights of the European Union, on the one hand, and of Article 6 of the Charter and Article 4 of the Treaty on European Union, on the other hand, is Article 15 of Directive 2002/58/EC to be interpreted as precluding national legislation which obliges providers of publicly available electronic communications services to retain traffic and location data of end users of those services where:
   - that obligation does not require a specific reason in terms of location, time or region;

- the following data are the subject of the storage obligation in the provision of publicly available telephone services – including the transmission of short messages, multimedia messages or similar messages and unanswered or unsuccessful calls:
  - the telephone number or other identifier of the calling and called parties and, in the case of call switching or forwarding, of every other line involved;
  - the date and time of the start and end of the call or – in the case of the transmission of a short message, multimedia message or similar message – the times of dispatch and receipt of the message, and an indication of the relevant time zone;
  - information regarding the service used, if different services can be used in the context of the telephone service;
  - in the case of mobile telephone services, the International Mobile Subscriber Identity of the calling and called parties and the international identifier of the calling and called terminal equipment;
  - in the case of pre-paid services, the date and time of the initial activation of the service, an indication of the relevant time zone, and the designations of the cells that were used by the calling and called parties at the beginning of the call;
  - in the case of internet telephone services, the IP addresses of the calling and the called parties and allocated user IDs;
- the following data are the subject of the storage obligation in the provision of publicly available internet access services:
  - the IP address allocated to the subscriber for internet use;
  - a unique identifier of the connection via which the internet use takes place, along with an allocated user ID;
  - the date and time of the start and end of the internet use at the allocated IP address, and an indication of the relevant time zone;
- in the case of mobile use, the designation of the cell used at the start of the internet connection, the following data must not be stored:
  - the content of the communication;
  - data regarding the internet pages accessed;
  - data from electronic mail services;
  - data underlying links to or from specific connections of persons, authorities and organisations in social or ecclesiastical spheres;
- the retention period is 4 weeks for location data (i.e. the designation of the cell used) and 10 weeks for the other data;
- effective protection of retained data against risks of misuse and against any unlawful access to that data is ensured; and
- the retained data may be used only to prosecute particularly serious criminal offences and to prevent a specific threat to a person's life or freedom or to the continued existence of the

Federal Republic or of a Federal Land, with the exception of the IP address allocated to a subscriber for internet use, the use of which data is permissible in the context of the provision of inventory data information for the prosecution of any criminal offence, maintaining public order and security and carrying out the tasks of the intelligence services?

Court ruling:

- Article 15(1) of Directive 2002/58/EC must be interpreted as **precluding national legislative measures which provide, on a preventative basis, for the purposes of combating serious crime and preventing serious threats to public security, for the general and indiscriminate retention of traffic and location data**.
- It **does not preclude legislative measures that**:
  - allow, **for the purposes of safeguarding national security**, recourse to an instruction requiring providers of electronic communications services to retain, generally and indiscriminately, traffic and location data in situations where the Member State concerned is confronted with a serious threat to national security that is shown to be genuine and present or foreseeable, where the decision imposing such an instruction is subject to effective review, either by a court or by an independent administrative body whose decision is binding, the aim of that review being to verify that one of those situations exists and that the conditions and safeguards which must be laid down are observed, and where that instruction may be given only for a period that is limited in time to what is strictly necessary, but which may be extended if that threat persists;
  - provide, for the purposes of safeguarding national security, combating serious crime and preventing serious threats to public security, for the targeted retention of traffic and location data, on the basis of objective and non-discriminatory factors, according to the categories of persons concerned or using a geographical criterion, for a period that is limited in time to what is strictly necessary, but which may be extended;
  - provide, **for the purposes of safeguarding national security**, combating serious crime and preventing serious threats to public security, for the general and indiscriminate retention of IP addresses assigned to the source of an internet connection for a period that is limited in time to what is strictly necessary;
  - provide, for the purposes of safeguarding national security, combating crime and safeguarding public security, for the general and indiscriminate retention of data relating to the civil identity of users of electronic communications systems;
  - allow, for the purposes of combating serious crime and, a fortiori, safeguarding national security, recourse to an instruction requiring providers of electronic communications services, **by means of a decision of the competent authority that is subject to effective judicial review, to undertake, for a specified period of time, the expedited retention of traffic and location data in the possession of those service providers, provided that those measures ensure, by means of clear and precise rules, that the retention of data at issue is subject to compliance with the applicable substantive and procedural conditions and that the persons concerned have effective safeguards against the risks of abuse**.

4.2. Developments at the national level (legislation and court rulings)

EU Member States		
Country	**Legislation**	**Court ruling**
Denmark	Three new laws have been passed, supplementing the Act on Electronic Communications Networks and Services in relation to data retention. • The Order on the Retention of Data Subjected to Registration and Retention (Law No. 379 of 29 March 2022), requiring providers, as defined under Section 2(1)(1) of the Act on Electronic Communications Networks and Services, to store information on servers located within EU territory. When the storage period expires, providers must destroy such information in an irreversible manner, unless a valid basis exists to store the information for a longer period of time. • The Ordinance on General and Indiscriminate Registration and Retention of Information of an End-user's Access to the Internet (Law No. 380 of 29 March 2022), requiring providers to record the following information on an end-user's access to the internet, generated or processed in their networks: o the assigned user ID; o the user identity (including IP address, source port number and other identifying information) and telephone number allocated to communications forming part of a public electronic communications network;	

	○ the name and address of the subscriber/registered user; ○ the starting and ending time of access to the internet. **Such information must be recorded and stored by at least one provider, or in agreement by a third party, for 1 year**. • The Order on General and Indiscriminate Registration Up to and Including 29 March 2023 and Retention Up to and Including 29 March 2024 of Traffic Data (Law No. 381, 29 March 2022), based on sufficiently specific circumstances that give rise to the assumption that Denmark is facing a serious threat to **national security**, to store the information for a longer period of time.	
Ireland	The Communications (Retention of Data) (Amendment) Act 2022 has completed the Irish legislative process. As of the time of publication, it has not yet been commenced. This new Act will amend the previous legislation to be in compliance with the CJEU rulings on data retention, which set aside a blanket requirement to retain online subscriber and traffic data. **This new Act will allow for specific retention of such data in defined circumstances as set out in the Act**.	**Judgment, Irish Court of Appeal, *The People at The Suit of the Director of Public Prosecutions* v *Smyth & McAreavey*, 28 July 2022** The use of Cell Site analysis and extracted mobile telephone evidence was referenced during the trial.
Spain		**Judgment Supreme Court, *Decision No. 824/2022*, 19 October 2022** The Supreme Court refused the defendant's request to refer the case to the CJEU and declared the **validity of the evidence consisting of the retroactive collection of geolocation data**, based on Law 25/2007 of 18 October on the retention of electronic communications

		and public communication networks data (the Data Retention Law), to still be in force. The Supreme Court concluded that even if the Spanish Data Retention Law were to be considered unlawful – which the Court rejected on the grounds that it offers sufficient guarantees for protection of personal data against the risk of unlawful misuse – the evidence obtained would still be valid in accordance with the latest CJEU rulings about data retention, according to which the most decisive factor in criminal proceedings is to establish that the **fundamental rights of the person under investigation have not been violated**.
France		**Judgment(s), Court of Cassation, *Requests Nos. 21-83.710, 21-83.820, 21-84.096 and 20-86.652*, 12 July 2022** The Court discussed the conformity of the national provisions authorising the retention and access to traffic and location data in criminal investigations with the requirements of the CJEU. According to these judgments, any court seized of a dispute relating to access to traffic and location data will have to verify, *ex post*, that: • the facts involved and justifying the need for such an investigative measure constitute **a serious crime**; • the rapid retention of and access to traffic and location data were both strictly necessary and proportionate to the prosecution of the offences concerned. The provisions of Article L. 34, III of the Electronic Posts and Communications Code, in the version resulting from Law No 2013-1168 of 18 December 2013, were in conformity with EU law only insofar as they required operators of

		electronic telecommunications services to retain in a generalised and undifferentiated manner: • for offences, regardless of their seriousness, data relating to civil identity, account information and payments; • for serious crimes, IP addresses assigned to the source of a connection; • traffic and location data, for the purposes of the investigation, establishment and prosecution of offences detrimental to the fundamental interests of the nation and acts of terrorism, with the purpose of safeguarding national security. Data stored by operators, either for their own purposes or under the general retention obligation in **order to safeguard national security**, may therefore also be retained, at the request of the investigators, by means of requisitions, **to combat a particular serious crime**. With regard to access to data, Articles 60-1, 60-2, 77-1-1 and 77-1-2 of the Code of Criminal Procedure are contrary to EU law only insofar as they do not provide for prior review by an independent court or administrative body. On the other hand, the investigating judge is empowered to control access to connection data. As regards the penalty for that non-compliance, the court must examine whether the irregularity caused the applicant to lodge a complaint. Such damage can only be established if the applicant demonstrates unjustified interference in their privacy and the protection of their personal data, because (i) the data could not be regularly stored

		for the purpose of rapid retention; (ii) the category of data referred to, and the duration for which access to the data took place, were not limited to what was strictly justified by the requirements of the investigation.
Cyprus	Data retention is covered under Law 183(I)/2007 on the Retention of Telecommunication Data for the Investigation of Serious Offences, transposing Directive 2006/24/JHA. Although the directive was invalidated by the CJEU, the national law is still valid as it is founded on a constitutional provision and includes specific safeguards for the protection of privacy; for example, communication data are released only following a court order.	**Judgment Supreme Court, 2022** A case was recently filed before the Supreme Court of Cyprus on the impact of the annulment of the EU directive on Law 183(I)/2007. The Court decided that Law 183(I)/2007 complies with the European Court of Human Rights only for the retention of IP addresses. After this decision, Cyprus law enforcement authorities could access the telecommunication data in relation to telephony based on Law 112 (i)/2004, which binds telecommunication service providers to retain the data for a 6-month period for billing purposes.
Portugal		On 19 April 2022 (Acórdão nº 268/2022), the Portuguese Constitutional Court **declared unconstitutional a number of provisions of the Portuguese Data Retention Act** (Law 32/2008) providing for the retention of traffic data, because they were in violation of paragraphs 1 and 4 of Article 35 (use of information technology) and of paragraph 1 of Article 26 (other personal rights), in conjunction with paragraph 2 of Article 18 of the Portuguese Constitution. This Act intended to introduce into the national legal regime the provisions of the EU directive on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks (EU Directive 2006/24/EC).

		The process in place allowing criminal justice authorities to access such stored traffic data for the investigation, detection and prosecution of serious crimes was declared unconstitutional as it **did not expressly provide for notification to the person involved that the retained data had been accessed by the criminal investigation authorities**, considering that such communication is not likely to compromise investigations or the life or physical integrity of third parties, and violated provisions on access to the law and effective judicial protection. **From now onwards, the criminal justice authorities no longer have access to traffic data in criminal investigations and can only have access to data that communications operators store for billing purposes (which are kept for 6 months)**.
Slovenia	The amendment of the Criminal Procedure Act (ZKP-N) from 2019 on obtaining data in electronic communication networks has been updated. These articles do not constitute a general obligation for operators, internet service providers and information service providers to store data for purposes of possible criminal investigation, but rather an obligation to disclose data they store on another legal basis for other purposes (billing, commercial) to a competent court.	
Slovakia	Act No. 452/2021 on electronic communications came into effect in 2022. This Act **does not specify a particular period of retention** for the obligation to retain data.	
Sweden	No new legal provisions have been enacted, but a proposal on data	

	retention is expected to be made during 2023.	
Non-EU countries		
Country	**Legislation**	**Court ruling**
Norway	No new legal provisions have been enacted. However, the §2-8a and §2-8b of the Electronic Communications Act ([15]) were amended in 2021 to provide for the retention of IP addresses. The law is in force; providers were given a time period to implement the technical tools and other systems required. This period of technical implementation ended on 1 January 2023, so **retention of IP addresses is functional** from this date. Public IP addresses can be retained for 12 months, but not destination information. The data in question may only be disclosed to the police/prosecutors/courts for crimes with a maximum penalty of 3 years or more and some specific types of crimes, including crimes against computer systems such as illegal access, illegal use of identity, computer system break-in and violation of private communication. Crimes as described in Articles 2 to 8 of the Budapest Convention would therefore also be covered.	

([15]) Norwegian text of the Electronic Communications Act.

5. Topic of interest: e-evidence

Introduction

In today's digital age, criminals increasingly rely on technology services and tools to plan and commit crimes, making e-evidence crucial for combating any crime, as almost all criminal investigations involve digital data. For cybercrime investigations, digital evidence is especially crucial. However, obtaining access to e-evidence can be a complex and time-consuming process for authorities, as the data is often stored in another country. Online service providers store user data on servers located in various countries, both within and outside the EU.

The *Sirius Digital Evidence Situation Report*, based on input from practitioners, has repeatedly highlighted that the main challenges faced by practitioners in obtaining e-evidence are the following:

- the mutual legal assistance processes take too long;
- the policies among online service providers regarding responses to information requests are different ([16]).

In April 2018, in response to calls from the European Council and the Council of the European Union, the European Commission proposed new rules to expedite and simplify the process for authorities to access e-evidence, regardless of data location. The Commission's proposal included two legislative proposals:

a) a regulation on European production and preservation orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings;

b) a directive laying down harmonised rules on the designation of establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings.

Following nearly 5 years of negotiations, the co-legislators agreed on the content of the legislation in early 2023, with a view to formally adopt and publish the legislation in the first half of 2023 and apply it 3 years later.

The purpose of this overview is to highlight the main elements of the legislation and the process envisaged to issue, execute and enforce the European preservation and production orders. As the proposed directive addresses the rules on designating and appointing the legal representatives and the regulation covers the main content of the legislation relevant for the practitioners, only the main elements of the regulation are discussed in this overview.

Main elements of the proposed legislation ([17])

The key components of the legislative package are the European production order and the European preservation order.

([16]) *EU Digital Evidence Situation Report 2022*, p 19.

([17]) At the time of writing this overview, an agreement has been reached between the Council Presidency and the European Parliament on the draft regulation and the draft directive, but it has not been officially adopted and has not been subject to lawyer-linguist review. Therefore the wording and numbering of the articles may change in the final text. The versions with the compromise text of the Parliament and the Council are available here: https://www.consilium.europa.eu/en/press/press-releases/2023/01/25/electronic-evidence-council-confirms-agreement-with-the-european-parliament-on-new-rules-to-improve-cross-border-access-to-e-evidence/.

The European production order enables competent authorities within the EU to directly request service providers to produce specific types of data, including subscriber, traffic and content data.

The European preservation order is a complementary instrument to the European production order which aims to preserve electronic evidence while the production order (or any other follow-up mutual legal assistance measure, such as the European investigation order) is being issued and executed. The preservation order ensures that evidence is not deleted or tampered with before it can be collected as evidence.

Issuing authorities

The issuing authority varies according to the type of order and the type of data requested.

The strictest requirement is for issuing production orders for traffic data (excluding requests for solely identifying the user) and content data, which can only be issued or validated by a judge, a court or the competent investigating judge in the case concerned. Other competent authorities can also issue the order, but in this case it must be validated by a judge, court or investigating judge.

For production orders for obtaining subscriber data and data requested for the sole purpose of identifying the user (e.g. IP addresses and the relevant source ports and timestamp (date/time), or technical equivalents of these identifiers and related information), the order may be issued or validated by a public prosecutor, in addition to courts.

Preservation orders may also be issued or validated by a judge, a court, an investigating judge or a public prosecutor.

Therefore, unlike the regulation on the European investigation order, the e-evidence regulation makes a distinction between issuing authorities according to the type of data requested, and production orders for traffic and content data can only be issued by judges.

In addition, Article 1(1a) also specifies that the issuing of both orders may also be requested by a suspected or accused person, or by a lawyer on their behalf, within the framework of applicable defence rights in accordance with national criminal procedures.

Conditions for issuing the European production and preservation orders

Articles 5 and 6 of the regulation outline the conditions for issuing production and preservation orders.

Both orders need to be necessary and proportionate to their purpose. The European production order should be necessary and proportionate for the purpose of the criminal proceedings, while the European preservation order must be necessary and proportionate to prevent the removal, deletion or alteration of data in view of a subsequent request for production of this data. Similarly to other judicial cooperation instruments, both orders should only be issued if they could have been ordered under the same conditions in a similar domestic case.

The European preservation order can be issued for any crime, as long as it could have been granted in a comparable domestic case. However, the regulation sets a minimum threshold for production orders.

For content and traffic data (excluding requests for data solely for user identification), the production order may be issued:

- if the criminal offense in the issuing state carries a maximum custodial sentence of at least 3 years;

- if the offense is part of a group specified in other EU legislation relating to cybercrime, child pornography, counterfeiting of non-cash means of payment, or terrorism, as listed in Article 5(4)(b-c); or
- for the execution of a custodial sentence of at least 4 months, which has been imposed for the crimes mentioned above.

If the issuing authority believes that the requested traffic or content data is protected by immunities and privileges under the law of the addressed Member State, or subject to rules regarding freedom of press and expression, they may seek clarification before issuing the European production order (except for data solely for user identification). This can involve consulting the competent authorities of that Member State, either directly or via Eurojust or the European Judicial Network. If it is determined that if the data is indeed protected by such immunities or rules, the issuing authority must not issue the European production order.

Notification procedure and the role of the enforcing state

While the general rule for both the production order and preservation order is that these shall be directly addressed to the designated representative of the service provider for immediate execution, an additional notification procedure is envisaged in Article 7a for the production orders issued for traffic data (excluding the traffic data requests solely for the identification of the user) and content data.

Production orders requesting this data must be simultaneously transmitted to the service provider and the competent authority of the enforcing state.

According to Article 7a(2), this notification procedure does not apply if, at the time of issuing the order, there are reasonable grounds to believe that the offense has been committed in the issuing state or if the person whose data is sought resides in the issuing state. Therefore, it is not important for the purposes of the notification obligation whether the offence has been committed and the person is residing in the enforcing state, but just that it would be any other country than the issuing state. Also, in cases where the crime has been committed and the person who committed the crime is residing in any other country, the enforcing state must still be notified.

The principle remains that it is ultimately up to the issuing state to decide if the notification procedure applies. However, recitals 35d and 35e of the regulation provide guidance that can be considered when determining whether the offense occurred within the issuing state's jurisdiction or whether the individual in question resides there.

The notification procedure has a suspensive effect on the execution of the order – either when the enforcing authority confirms to the service provider that it will not provide any grounds for refusal or when 10 days have passed, whichever is sooner.

In emergency cases, when there is an imminent threat to life or to the physical integrity or safety of a person or critical infrastructure, the notification does not suspend the execution. However, the enforcing authority can still object to using the data within 96 hours by providing grounds for refusal. If this happens, the issuing authority must either delete the received data or limit its use based on the conditions set by the enforcing authority.

Execution of the orders and grounds for refusal

Preservation order

After receiving the European preservation order certificate, the service provider must preserve the data requested without undue delay and do so for 60 days or until the issuing authority has informed the service provider that preservation is no longer necessary.

After 60 days, the issuing authority may issue either an extension request for another 30 days or a production order.

In case a preservation order is issued, the service provider has only very limited grounds for non-execution, as listed in Article 10, mostly related to situations where the execution of the request is de facto not possible or when there is not enough information. Also in these cases the service provider must inform the issuing authority and explain these reasons. Additionally, Article 10(3a) envisages that if it is evident from the request that it could interfere with immunities or privileges, or freedom of press or media, the service provider informs the competent authorities of the issuing and the enforcing state. But in this case, the information is only to be taken into account by the issuing state to decide whether to withdraw, adapt or maintain the order.

Production order

For production orders, the procedure and possible grounds for refusal are more detailed.

Firstly, after receiving the production order certificate, the service provider must promptly preserve the data. Thereafter, the process continues depending on whether the notification of the enforcing authority was needed or not.

In case the notification was not required, the addressee should transmit the required data to the issuing authority at the latest within 10 days upon receipt of the order. In case the notification procedure is required, the service provider can only send the requested data when the enforcing authority has confirmed that it will not provide grounds for refusal or when 10 days have passed. Once either of these conditions is met, the addressee must send the requested data as soon as possible, at the latest by the end of the 10 days.

Similarly to the preservation order, in the case of the production order, the addressee may consider that the execution of the order could interfere with immunities or privileges, or be related to the determination of criminal liability that relates to freedom of press or media. In these cases, the service provider should inform the competent authorities of the issuing and the enforcing state.

According to Article 10a(1), after receiving the notification from the issuing state, the enforcing state may then give one or more of the following grounds for refusing the order.

- The data is protected by immunities or privileges or by rules on criminal liability that relate to freedom of press or freedom of expression.
- In exceptional situations, there are substantial grounds to believe that the execution would entail a manifest breach of fundamental rights.
- The execution of the order would be contrary to the principle of *ne bis in idem*.
- The offence for which the order is issued is not an offense in the enforcing state, unless the offence is punishable in the issuing state by at least a 3-year custodial sentence and is listed in the list of serious crimes in Annex IIIa.

Before providing any of these grounds, the enforcing authority has the obligation under Article 10a(3) to contact the issuing authority to discuss these concerns, which might enable the issuing authority to adapt or withdraw the order.

If no solution is found in these discussions, the enforcing authority can provide one or more of these grounds of refusal and inform the addressee and the issuing authority immediately. This stops the execution of the order immediately, and no data is transferred.

Enforcement procedure

The enforcement of the request is regulated in Article 14 of the regulation and applies in cases when the addressee does not comply with a production or preservation order without valid reasons, and the enforcing authority has not invoked any grounds for refusal. The issuing authority can then request enforcement by the competent authority in the enforcing state. The issuing authority translates the order into the language accepted by the enforcing state and sends the necessary documents to the enforcing state.

The enforcing authority must recognise and enforce the order within 5 working days unless certain grounds for refusal apply. It then requires the addressee to comply or oppose the execution, informing them of the applicable sanctions for non-compliance.

Enforcement of the European production order may only be denied based on specific grounds, such as the order not being issued by a valid authority, the order not being issued for a valid offense, de facto impossibility, or data being protected by immunities or privileges. The enforcement of the European preservation order may also be denied based on similar grounds.

In case of objection by the addressee, the enforcing authority decides to enforce the production order based on information from the addressee and the issuing authority. Before deciding not to recognise or enforce the order, the enforcing authority must consult the issuing authority and request further information, if needed. The enforcing authority notifies the issuing authority and addressee of its decisions. If the addressee does not comply with a recognised order, the enforcing authority must be able to apply a pecuniary sanction, and an effective judicial remedy to this decision should be available.

Channel of requests

The regulation includes the establishment of a decentralised IT system for data exchange between competent authorities and service providers. Article 18a outlines this system, and Article 18f tasks the Commission with developing software for Member States to use for this purpose.

Member States must ensure that the service providers' designated representatives have access to the decentralised IT system through their national IT systems. Service providers must also be able to use this system.

Alternative means of communication may only be used when the decentralised IT system is unavailable due to disruption, data size, legal or forensic requirements, or exceptional circumstances. In these cases, basic transmission details must still be recorded in the decentralised IT system without undue delay.

The Commission is required to adopt implementing acts for establishing the decentralised IT system within 2 years after the regulation's entry into force. Article 18h provides a transition period for using alternative means until the decentralised IT system becomes compulsory. However, this transition period may not be necessary in practice, as the obligation to use the decentralised system will apply

from 1 year after the adoption of the implementing act, which coincides with the application of the regulation 3 years after its entry into force.

Relation to other instruments

The use of this regulation is not mandatory for the Member States and does not affect any other EU or international instruments, agreements and arrangements on the gathering of evidence. Member States are nonetheless obliged to inform the Commission by the time of the application of the regulation which existing agreements and arrangements on the gathering of evidence they will continue to apply.

In February 2023, the Council also authorised the Member States to ratify the Second Additional Protocol to the Convention on Cybercrime (Budapest Convention), which will complement the internal EU framework on access to e-evidence ([18]). As the protocol is open for signatures from all countries, parties have an opportunity to enhance direct cooperation with service providers across the world.

Conclusion

The adoption of the legislative package on e-evidence marks a significant advancement in the access to digital information in cross-border criminal investigations and prosecutions. By expediting and simplifying the process of obtaining electronic evidence from the service providers providing their services in the EU, this comprehensive legal framework aims to enhance the efficacy of law enforcement and judicial authorities in combating crime in the digital age.

([18]) https://www.consilium.europa.eu/en/press/press-releases/2023/02/14/access-to-e-evidence-council-authorises-member-states-to-ratify-international-agreement/.

6. Future of the Cybercrime Judicial Monitor

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

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

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

For this eighth edition of the CJM, a slight decrease in the number of contributions was noticed. Eurojust and the European Judicial Cybercrime Network will review whether a different reporting format should be considered.

Eurojust, Johan de Wittlaan 9, 2517 JR The Hague, The Netherlands
www.eurojust.europa.eu • info@eurojust.europa.eu • +31 70 412 5000
Twitter, LinkedIn & YouTube: @Eurojust

Catalogue number: QP-AG-23-001-EN-N • *ISBN*: 978-92-9490-914-5 • *ISSN*: 2600-0113 • *DOI*: 10.2812/063826

Eurojust is an agency of the European Union