Cybercrime Judicial Monitor

Issue 9 – July 2024

Criminal justice across borders

EUROJUST

European Union Agency for Criminal Justice Cooperation

EUROPEAN JUDICIAL CYBERCRIME NETWORK

Contents

Executive summary

Eurojust presents the ninth 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.

In the last year, up to May 2024, several significant legislative developments at the EU and national levels were noticed. The e-evidence regulation and directive were adopted, along with the markets in crypto-assets regulation. The Council of Europe adopted an international treaty on artificial intelligence in May 2024, while the EU legislative procedure on the Artificial Intelligence Act continued in 2023 and was finalised in May 2024. Some EU Member States reported amendments to existing legislation or the introduction of new cybercrime-related offences in their legislation.

The Court of Justice of the European Union (CJEU) rendered a ruling in April 2024, clarifying the conditions for the transmission and use of evidence in criminal cases with a cross-border dimension. Several Member States reported on court rulings about cryptocurrency crimes, unauthorised access to computer systems, admissibility of evidence gathered from encrypted communication platforms and remote computer searches.

In the past year, the CJEU further provided additional guidance concerning data retention rules in Member States. Some Member States reported new pieces of national legislation in the area of data retention, whereas others provided information about their domestic court rulings in 2022 related to, and/or in line with, (earlier) CJEU rulings about data retention.

The topic of interest in this ninth issue of the CJM provides information on cooperation with crypto-asset service providers (CASPs) in the context of criminal investigations and prosecutions. The section first takes a closer look at cryptocurrency investigations in general, touching upon challenges encountered and best practices used. It then continues to elaborate on the cooperation of law enforcement and judicial authorities with CASPs in the context of such investigations, highlighting recurring obstacles in obtaining information from CASPs or cooperation in relation to the seizure of crypto-assets. Finally, it covers some aspects of international cooperation.

1. Introduction

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

The CJM is produced on the basis of information provided by members of the European Judicial Cybercrime Network (EJCN). Out of the 29 members, 22 replied to this year's questionnaire. All issues of the CJM are available on the Eurojust website.

As in previous editions, the CJM consists of three main sections, followed by a topic of interest section. For this ninth issue of the CJM, Eurojust selected 'cooperation with crypto-asset service providers' as the subject of this section.

2. Legislation

The objective of this section is to provide information on developments in international, EU and national legal instruments in relation to cybercrime and e-evidence in 2023 and 2024. The main information on national legislative developments presented in Section 2.3. is collected through the EJCN.

2.1. International level

- *Framework Convention on Artificial Intelligence and Human Rights, Democracy, and the Rule of Law*.

On 17 May 2024, the Council of Europe adopted the Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law. The treaty sets out a legal framework for artificial intelligence (AI) systems and addresses the risks they may pose, while promoting responsible innovation. It applies to the use of AI systems in the public and private sectors, with exceptions for AI systems related to the protection of national security interests and research and development activities. Similar to the EU's Artificial Intelligence Act (AI Act) (see section 2.2.), the convention adopts a risk-based approach to the design, development, use and decommissioning of AI systems. It establishes transparency and oversight requirements, and parties to the convention will have to ensure accountability and responsibility for the adverse impact of AI systems. The convention also requires that each party establish an independent oversight mechanism to oversee compliance with the convention.

The framework convention will be open for signature on 5 September 2024.

2.2. EU level

e-Evidence

- *Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings (e-evidence* regulation).
- *Directive (EU) 2023/1544 of the European Parliament and of the Council of 12 July 2023 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings (e-evidence directive).*

On 27 June 2023, the Council of the European Union approved the European Parliament's first reading position of the e-evidence regulation and e-evidence directive, thereby adopting the legislative acts. The regulation and directive were signed by the Council and the Parliament on 12 July 2023 and entered into force on 18 August 2023. The regulation will apply from 18 August 2026. EU Member States have 30 months from the date of entry into force of the directive to transpose it into national law.

More information about the regulation (full text of the regulation) and directive (full text of the directive) can be read in Section 5 of the previous edition of this report.

Crypto-assets

- *Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets.*
- *Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets (MiCA regulation)*.

In 2020, the European Commission presented the digital finance strategy, which sets out general guidelines on how to support the digital transformation of finance in the EU while regulating its risks. As part of this strategy, a comprehensive legislative framework was proposed, regulating the issuing of crypto-assets and the services provided in relation to crypto-assets.

Two particular legislative acts, adopted in May 2023, can be highlighted in this context.

Regulation (EU) 2023/1113 on information accompanying the transfers of funds and certain crypto-assets lays down rules for crypto-asset service providers (CASPs) to collect and make available information about the sender and beneficiary of transfers of crypto-assets for the purposes of preventing, detecting and investigating money laundering and terrorist financing. Under this regulation, CASPs will be required to collect and make available information about the sender and beneficiary of transfers of crypto-assets, regardless of the amount of crypto-assets transacted. The new regulation will apply from 30 December 2024.

The regulation on the markets in crypto-assets lays down rules relating to the issuance of crypto-assets and the admission to trading platforms of crypto-assets, along with rules for CASPs on authorisation, supervision, operation and governance. At the same time, the MiCA regulation establishes requirements for the protection of holders of crypto-assets and clients of CASPs and provides for measures to ensure the integrity of markets in crypto-assets. This regulation will apply from 30 December 2024, with the exception of some articles that will apply earlier.

Artificial intelligence

- *Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (Procedure 2021/0106/COD* – legislative procedure).

The legislative procedure related to the AI Act continued in 2023. In December 2023, the Parliament and the Council reached a political agreement on the AI Act.

On 13 March 2024, the Parliament endorsed the AI Act. The endorsed text reflects what had been previously agreed between the institutions. On 21 May, the Council also approved the AI Act. After being signed by the presidents of the Parliament and of the Council, the legislative act will be published in the EU's Official Journal and enter into force 20 days later. The new regulation will apply 2 years after its entry into force, with some exceptions for specific provisions.

The AI Act lays down a uniform legal framework for developing, marketing and using AI. It also aims to address the risks of specific uses of AI to ensure the trustworthiness of AI systems.

2.3. EU Member States and non-EU countries

Member State	Summary of the legal provision(s)
France Decree No 2023-1083 of 23 November 2023	The Anti-cybercrime Office (OFAC) was created as part of a reorganisation of the various national services dealing with cybercrime. Among other tasks, the OFAC is responsible for: — leading and coordinating, at the national and operational levels, the fight against crimes related to information and communication technologies; — conducting judicial investigations into cybercrime; — carrying out investigative acts and technical investigations; — providing assistance to the national police and other authorities.
France Act 2023-22 of 24 January 2023	This act introduced new provisions into the Criminal Code (CC) and the Criminal Procedure Code (CPC) aimed at strengthening the fight against cybercrime. In addition, the act: — facilitates the seizure of digital assets (Article 706-154 CPC); — increases the penalties for fraudulent access to or remaining in an automated data processing system, resulting in the deletion or alteration of data in the system or impairing the functioning of the system, including when the system is operated by the state (Article 323-1 CC); — broadens the scope of the aggravating circumstance applicable when the offences are committed by an organised gang; — adds a new aggravating circumstance when the abovementioned offences cause an immediate risk of death or injury to another person, likely to result in permanent mutilation or invalidity, or of hindering assistance intended to save a person from imminent danger or to combat a disaster presenting a danger to the safety of persons (Article 323-4-2 CC); — introduces two new offences, namely (1) administering an online platform enabling the sale of products, content or services whose sale, offer, acquisition or possession are manifestly illegal; and (2) providing intermediation or escrow services, the sole or main purpose of this being to implement, conceal or facilitate the transactions referred to above (Article 323-3-2 CC).
Luxembourg Law of 29 July 2023	The law modified several provisions of the national CPC and the CC, introducing: — a possibility for the investigating judge to notify, including via email, the persons or service providers targeted by several e-

	evidence gathering measures, such as the seizure of data from an IT system (Article 66 CPC), the localisation of telecommunication (Article 67-1 CPC), the interception of telecommunication and the surveillance of IT systems (Article 88-1 CPC); — amendments to cybercrime provisions, broadening the scope of IT systems from 'systems for the automatic processing or transmission of data' to now also include systems of non-automatic processing of data, thereby covering other types of illegal access to personal data; — the offence of processing personal data in an IT system for which authorisation was not given, in addition to already existing provisions of illegal access to IT systems (Article 509-1(1) CC) and data interference (Article 509-1(2) and Article 509-3 CC).
Hungary Amendment of the Criminal Code Entry into force on 1 January 2023	Amendments were made to the CC, introducing new offences, both punishable by imprisonment of up to 2 years: — the recording of data stored on electronic payment instruments or related security features, using technical means (Section 392(1)c CC); — producing, obtaining, possessing, placing on the market, bringing in or out of the country or transferring through its territory any material, device, appliance or computer program necessary for recording, by technical means, data or connected security elements stored on an electronic non-cash payment instrument (Section 394(1) CC).
Malta Act No VI of 2024	The act introduced amendments to the provisions in the Proceeds of Crime Act relating to confiscation orders (Chapter 621). Particularly, Article 48(5) now stipulates that 'in determining whether the Government has met its burden of establishing that the property is subject to confiscation, the Court may consider any evidence relevant to that determination submitted by the intervener'. Electronic evidence is also covered by this provision.
Austria Amendment of existing legal provisions related to cybercrime offences	Certain cybercrime offences are punishable with a higher penalty.
Romania Law No 217/2023	A new paragraph on child pornography was added to Article 374, paragraph 3^2 of the Criminal Code: 'The act of an adult requesting a minor to record, produce, distribute, display or transmit by any means, including through electronic communications or social networks, images, videos or other pornographic

	materials featuring the minor having explicit sexual behaviour is punishable by imprisonment of 6 months to 3 years'.
Sweden Amendment of legislation related to the tracing of electronic communications Entry into force on 1 October 2023	The law related to the tracing of electronic communications was amended to include covert surveillance of electronic communications, even when there is no suspect (Chapter 27, Article 19b§). This will now make it possible to monitor ransomware servers to identify perpetrators.

3. Judicial analysis

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

This section 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 Member States and non-EU countries.

3.1. Court of Justice of the European Union

On 30 April 2024, the Court of Justice of the European Union (CJEU) issued its judgment in case C-670/22 – *M.N. (EncroChat)*, following questions referred to the CJEU by the German court (Landgericht Berlin). The questions mainly related to the lawfulness of the European Investigation Orders (EIOs) that were issued by the German public prosecutor's office to France with a view to obtaining EncroChat data gathered by France and using it in criminal proceedings in Germany.

In its ruling, the CJEU interpreted several Articles 1(1), 2(c), 6, 14(7) and 31 of Directive 2014/41/EU regarding the EIO in criminal matters. The CJEU did not rule on the dispute itself (i.e. the national criminal case against the accused), which was the sole competence of the national courts.

Firstly, the Court took a closer look at the authority competent to issue the EIO. The issuance of an order to transmit evidence that has already been gathered is subject to the same conditions that apply in a domestic situation. In Germany, contrary to an order to intercept data (requiring issuance by a judge), an order for the transmission of already gathered data can be issued by a public prosecutor. The Court, therefore, replied that a **public prosecutor could issue an EIO to request the transmission of (EncroChat) data that had already been gathered by the executing state** (in this case, the French authorities).

Secondly, concerning the substantive conditions for issuing an EIO for the transmission of evidence, the CJEU stated that the **same conditions apply as for the transmission of similar evidence in a purely domestic situation**. It does not need to satisfy the same substantive conditions as those that apply to the collection of evidence. However, the CJEU clarified that a court before which an action against an EIO is brought must be able to **review compliance with the fundamental rights** of the persons concerned.

The Court further clarified that '**interception of telecommunications**', within the meaning of Article 31 of Directive 2014/41, covers a measure entailing the infiltration of terminal devices for the purpose of gathering traffic, location and communication data from an internet-based communication service. This is, in fact, the interception measure which was performed by the French authorities on German territory in the EncroChat case. When carried out, such a measure should be notified, in good time, to the authority designated for that purpose by the Member State (or to any other authority if this specific one is not known) on whose territory the subject of the interception is located (i.e. Germany). In the event that the measure would not be allowed in a similar domestic case, this **notification** enables the competent authority of the notified state to indicate that the interception may not be carried out or needs to be terminated or, where appropriate, that any material already intercepted may not be used, or may only

be used under conditions which it is to specify. This not only guarantees respect for the sovereignty of the notified Member State, but also protects the rights of the persons affected by the interception.

Finally, the Court stated that the need to disregard information and evidence obtained in breach of the requirements of EU law exists only if a court comes to the conclusion that an EIO has been unlawful. In any case, the Court reiterated that, in principle, the **rules relating to admissibility of evidence and assessment of information and evidence in criminal proceedings is a matter of national law**, but also that the rights of the defence and the right to a fair trial should be guaranteed: **if a defendant cannot review or comment on important information or evidence obtained through the EIO, and such information and evidence are likely to have a preponderant influence on the findings of fact, these should be excluded** from the criminal proceedings by the national criminal courts.

3.2. National court rulings

❖ Belgium

Court of Cassation – 31 October 2023 – P.23.0998.N

Background

This appeal in cassation was directed against the judgment of the Court of Appeal of Antwerp of 14 June 2023, in which the evidence obtained from Sky ECC communications was found admissible, and the defendants were sentenced to 10 years imprisonment.

Court ruling

The applicant put forward three pleas in law. The first plea in law alleged infringement of Article 6 of the European Convention on Human Rights (ECHR) and disregard for the **right to a fair trial**, asserting that the investigating judge had exceeded his scope of competence. According to the applicant, **not all documents of the mother file had been added to the case file**, impacting the assessment of his guilt and his right of defence. The court, however, stated that even if there were any overruns of the scope of competence of the investigating judge, which there were not, that exceedance had not been sanctioned on sanction of nullity, whereas there was no question of the unreliability of the data communication obtained or of a disregard of the right to a fair trial. Moreover, it is necessary for the defence to **provide some plausibility to the existence of the irregularity alleged** and its importance in assessing its case. Mere speculation is not sufficient. Such plausible evidence was not given, and there was sufficient information available in the case file to ensure that the investigating judge did not exceed his scope of competence.

The second plea alleged infringement of Article 90ter of the CPC, asserting that a separate decision under this article was needed to decrypt the communications. The Court of Cassation, however, agreed with the Appeal Court, ruling that **no additional authorisation is required for the decryption of communication data that has been lawfully intercepted and seized abroad** and subsequently transferred on the basis of an international legal assistance instrument.

The third plea alleged infringement of Article 6 of the ECHR, Article 149 of the Belgian Constitution and the general principle of law relating to the obligation to state reasons. According to the applicant, the appeal judgment did not respond to the defence that no tap decisions were submitted for the virtual servers, which have a separate email address, but only results were used from the tap on the particular server located in France. The Court of Cassation concluded that Article 6 of the ECHR is alien to the plea, alleging only a lack of a response to the claimant's defence. The court also stated that there was no need

to go into detail about the defence, as the judgment excluded interception of separate internet protocol (IP) addresses of virtual servers and responded to the defendant's defence.

Therefore, none of the pleas were upheld.

❖ Czechia

Supreme Court – 31 May 2023 (ruling in Czech language)

Background

Under Czech criminal law, the preparation of a particularly serious offence is punishable in certain cases. Preparation of an offence entails 'a conduct that consists in intentional creation of conditions for the commission of a particularly serious felony' (Section 14(3) CC). However, the criminal **liability for the preparation of such an offence will disappear** if the offender voluntarily stops further conduct aimed at the commission of the offence and **removes the threat** to an interest protected by the CC which occurred due to the preparation committed.

Supreme Court ruling

In this case, the accused was preparing to commit fraud via the internet by misleading persons through a website in order to extort money from them for the purchase of non-existent bonds, which would cause damage on a large scale. The accused voluntarily disabled access to the website.

The Supreme Court did **not consider the voluntary temporary disabling of access to the website by the accused a 'removal of the threat'**, as he could have made the website available again at any time in the future with a single mouse click.

❖ Germany

Federal Court – 'Cyberbunker Trial'

Background

The defendants operated a bulletproof hosting service in a former bunker in the German federal state of Rhineland-Palatinate. The defendants were aware that the services they provided were mainly used for criminal purposes.

The Regional Court of Trier sentenced eight defendants to prison sentences ranging from 1 year to 5 years and 9 months for membership of a criminal organisation. The court did not, however, convict them of aiding the users of their services to commit offences. Under German law, for an action to be considered 'aiding', the perpetrator has to have knowledge of the specific details of the offence they are aiding. The court did find, however, that the mere knowledge that their customers were committing crimes did not constitute specific knowledge in that respect.

Federal Court ruling

The Federal Court **confirmed the earlier conviction** by the Regional Court. It specifically addressed the question whether running the Cyberbunker was an action privileged by § 7 et seq. of the German Telemedia Act in connection with Directive 2000/31/EC (e-commerce directive). The court found that, as the defendants not only provided hosting services but also provided **bulletproof hosting services**, which included more than automated passive services of a technical nature (e.g. disguising the location of the stored data), they created **infrastructure aimed at avoiding law enforcement**. According to the court, neither German nor EU law intends to protect this type of behaviour.

❖ Spain

Supreme Court – 13 November 2023 – rec. 11213/2023

The Supreme Court defined unitary treatment for all data in the virtual environment (computers and mobiles) regardless of the existing 'old' rights protected. The **right to the protection of the virtual or digital environment** (*derecho al entorno digital*) is thus a new-generation right.

As a result, judicial authorisation can be granted, provided it contains the necessary requisites and justification, to limit this new generation right. Such authorisation can, for example, be given to the police for accessing data on a device. In this case, the authorisation can limit both the right to privacy (to access contact lists) but also the right to secrecy of communications (to access messages).

Supreme Court – 23 March 2023 – Resolution No 308/2023, rec. 7563/2022

In this case, the Supreme Court ruled about the **seriousness of computer damage**. The court found that the facts in this case constituted the offence of computer damage. Although the computer scientist was able to restore the access codes to all the company's relevant information, the hard disk had been largely erased, and it took the company almost 2½ months to solve the problem. Therefore, the defendant did not merely cause an inconvenience or annoyance to the company but significantly disrupted the digital functioning of the system for a prolonged period. The court pointed out that **the typical gravity is reached when it is impossible to recover the operability of the system or when its restoration is difficult to reverse without considerable technical and economic efforts**. It should be noted that the computer units or processes protected here are intangible elements that do not always have an intrinsic economic value, not even for the estimated value of an uncertain recovery.

❖ France

Court of Cassation – Criminal Division – 21 November 2023 – 23-82.028

The Court of Cassation ruled that an **order of the public prosecutor to access connection data does not satisfy the requirement of prior control by a court or an independent administrative body** laid down by EU law. Furthermore, connection data cannot be requested on the basis of a general request. Such a request must therefore be preceded by an examination of the necessity and proportionality of the requested measure in light of the interference with the private life and personal data of the accused, and must be formulated in a specific and explicit way.

Court of Cassation – First Civil Division – 28 June 2023 – 22-12.424

NB: This is not a decision in criminal matters but in contractual matters and consumer law.

In this case, an investor had received a gift in the form of cryptocurrency, XEM tokens. The tokens were used to carry out transactions on the New Economic Movement network, a decentralised platform. The customer accused the platform of failing in its duty of care.

The Court of Appeal relied on a number of **factors to classify the investor as a professional**. Firstly, he had benefited from a gift that had enabled him to place the sums in a wallet and carry out speculative transactions on the platform. Secondly, the transactions were numerous and the gains substantial. Thirdly, he had been involved with a foundation interested in the crypto economy. Finally, this seemed to be his only source of income.

For the Court of Cassation, these elements were insufficient to consider him a professional investor. The court emphasised that this concerned the management of private assets and that this type of investment, like any stock market investment, leaves room for both gains and losses. It was also irrelevant that the investor had the skills of a professional. The contract had been entered into for a purpose that could be considered unrelated to his professional activity. The investor in this case was not acting in the course of his professional activity, unless he considered that his investments were his sole source of income and that this was, therefore, de facto a professional activity.

An investor in crypto-assets may therefore have consumer status. The majority of investors in crypto-assets will thus qualify as consumers, allowing them, if they are victims, and where Regulation (EU) 1215/2012 is applicable, to sue at their place of domicile.

Correctional Tribunal of Paris – 21 June 2023 – No 21280000091

In this case, three defendants had created the arbiape.com website (under a fictitious identity) to promote, in particular via Discord, Twitter and Telegram, a **smart contract** ([1]) presented as allowing the **investment of Ether (crypto-assets) in return for an attractive return**. However, a fraudulent code was injected into this smart contract, which entailed, when the depositor sought to withdraw his crypto-assets from the platform, the immediate application of a **withdrawal fee rate of 100 %** (instead of the 2 to 10 % announced to investors, and the 2 % provided for when the smart contract was initially put online) **and the transfer of all the crypto-assets to an address used by the designers** of the smart contract. The defendants were charged with fraud and money laundering.

They also assisted in various operations involving the investment, concealment and conversion of the direct or indirect proceeds of the crime of fraud by making or allowing transfers of cryptocurrencies and conversions of those funds, along with their storage on wallets.

The court rejected the pleas of nullity based on the nullity of the expert report and on the orders of compelled appearance. The court also rejected an objection of lack of jurisdiction. All three defendants were fined.

Correctional Tribunal of Paris – 25 October 2023 – No 22109000340

In 2022, the defendant developed and supplied the **malicious HEAVEN XLS solution, enabling automated data processing systems to be compromised using Excel documents**.

The court ruled that the defendant was an accomplice in carrying out offences of extortion, fraudulent access to and continuous use of an automated data processing system, with the aggravating circumstances that this action resulted in an alteration of the system, fraudulent introduction into an automated data processing system, fraudulent modification of data in an automated data processing system and hindering the operation of an automated data processing system. The court also found the defendant guilty of the possession and sale of malicious software, criminal conspiracy and money laundering.

Correctional Tribunal of Paris – 2 November 2023 – No 19035000724

In January 2019, many victims received an email from an unknown individual informing them that they had hacked into their computer and captured one or more videos showing them in private while they

([1]) See visual on page 19.

were looking at a pornographic website. The victims were instructed to transfer a sum to a Bitcoin address, failing which the videos would be distributed to their relatives.

Two persons were charged with extortion, attempted extortion, fraudulent access to and continued use of all or part of an automated data processing system, and organised money laundering.

The defendants contested the categorisation of fraudulent access to and continued use of the system. They claimed that they had merely accessed mailboxes that did not belong to them and had used them to send extortion emails.

However, **fraudulent access to an automated data processing system is established when an unauthorised person enters such a system in the knowledge that they have no authorisation**. It was clear from the proceedings that the defendants gained access to the victims' machines by sending them emails with attachments, which, upon opening, infected the machines in question.

Fraudulent continued use of an automated data processing system is established because the defendants took remote control of the infected machines. This was done without any authorisation and with full knowledge of the facts. The court convicted both defendants.

Correctional Tribunal of Paris – 1 December 2023 – No 23052000264 – 'Platypus'

On 16 February 2023, hackers used **flash loans** (instant cryptocurrency loans with no collateral and repayable within seconds) **to withdraw cryptocurrencies** worth several million euro ([2]). The next day, the cryptocurrency exchange Binance reported it as a possible scam carried out from France, targeting the American company Platypus.

The hackers had taken out a loan of 44 million USD Coin (USDC) on the Aave blockchain and deposited it into the liquidity pool of the Platypus platform. The sum was then blocked as collateral, which enabled them to apply to Platypus for a new loan of USD 41.7 million.

The hackers used the 'emergency withdrawal operation' to withdraw approximately 9 million USD. This made it possible to convert the USDC into several stablecoins. At the same time, the attackers converted some of the USD 41.7 million into other crypto-assets. The deposited 44 million USDC was released on the Platypus platform and the initial loan was immediately paid back to the Aave blockchain, thus settling the debt. In a second phase, the funds were transferred to wallets in order to launder them.

The criminals concealed the various transactions by switching blockchains, turning USDT-TRON funds into Ethereum and then Avalanche (AVAX). Furthermore, a mixer circumvented the transparency of transactions recorded in the blockchain by mixing cryptocurrency funds in order to hide their origin.

The defendants were prosecuted for fraudulent access to and continued use of an automated information system, fraud and money laundering. They were **acquitted**, as the court considered that the constituent elements of the offences were not met. Rather, the court found the **actions concerning the flash loan to be 'unethical behaviour'**, taking advantage of Platypus's coding error to withdraw funds, and that a **civil debt was owed to the plaintiff** in connection with the flash loan.

([2]) See visual on page 19.

❖ Croatia

In 2023, there were three court decisions in which the evidence obtained from the **Sky ECC communications was found admissible**. The defendants can still appeal these rulings.

❖ Italy

Court of Cassation, United Criminal Sections – 29 February 2024

On 29 February 2024, the United Criminal Sections of the Italian Court of Cassation issued provisional information on the outcome of two cases. The full judgment(s), including the court's motivations, will follow in the coming months.

The court provided provisional information to the following disputed questions.

(a) Does the transfer to the Italian judicial authority, in the execution of an EIO, of the contents of communications via cryptophones, which was already acquired and decrypted by the foreign judicial authority in its own criminal proceedings, constitute the acquisition of digital documents and data within the meaning of Article 234-bis CPC or of documents within the meaning of Article 234 CPC, or is it subject to rules relating to other forms of acquisition of evidence?

The court stated that this transfer is a form of 'acquisition of acts of criminal proceedings', which, depending on their nature, alternatively finds its basis in Article 78 of the implementing provisions of the CPC or in Articles 238 or 270 CPC, and, as such, complies with Article 6 of the EIO directive.

(b) Should the above transmission be subject to prior judicial review of its lawfulness in the state issuing the EIO?

The court replied negatively, stating that the acquisition of acts of other criminal proceedings falls within the powers of the public prosecutor.

(c) Is the admissibility of the evidence referred to in (a) above subject to judicial review in the issuing state?

The court replied affirmatively, confirming that the court of the issuing state must verify that fundamental rights, including the right of defence and the guarantee of a fair trial, are respected.

❖ Lithuania

Supreme Court (cassation) – 15 February 2023 – No 2K-27-976/2023

In 2020, a former employee of a company accessed several times, from home, the company's document management system SharePoint and his (former) email account, which was not deactivated, without the consent of the company. He thereby **unlawfully accessed and monitored non-public electronic data** uploaded to the system, which contained information on the operational and strategic indicators of the company's management, budget and sales plans.

On 15 February 2023, the Supreme Court convicted the defendant under Article 198(1) CC and Article 198/1(1) CC of having unlawfully accessed an information system and unlawfully monitored non-public electronic data.

The defendant appealed against the ruling, arguing that the court should have found that the **offences were of minor relevance**. First of all, the defendant had been providing services to the company for several years, and was therefore generally aware of the content of the electronic documents uploaded to the system. Secondly, following the termination of the employment of the defendant, the company did not

delete his Microsoft account, and he did not conceal the fact that he had access to it. Finally, the company had not made any claims regarding the removal or alteration of electronic data, and no damage had been caused to it.

Based on Article 37 CC, a perpetrator of an offence may be exempted from criminal liability if the extent of the damage, the subject matter of the offence or any other specific features of the offence render the offence to be of minor relevance. Also, in accordance with case-law, in cases where an act does not substantially cause damage to social relations or other legal goods protected by criminal law, or does not give rise to a real risk of such damage, it shall be regarded as insignificant to the values protected by that law (i.e. it shall be recognised as being of minor relevance).

The court has clarified, through its case-law, that **unlawful access to an information system cannot, as a general rule, be regarded as insignificant**, especially if such access has enabled the commission of other illegal acts in the system. The fact that no civil action has been brought does not in itself diminish the gravity of the offence.

The court therefore concluded that the acts could not be considered as being of minor relevance, as the defendant had unlawfully accessed the system more than 60 times and subsequently viewed (downloaded) non-public electronic data, some of which were also altered.

❖ Netherlands

Supreme Court (cassation) – 13 June 2023 – Case No 23/00011, 23/00010

Questions for preliminary ruling

This ruling concerned requests for preliminary rulings from two courts relating to the **principle of mutual trust** when assessing the **legality and reliability of evidence obtained via investigative measures conducted by foreign authorities** (i.e. EncroChat and Sky ECC data intercepted by France and transmitted to the Netherlands) and options for the defence to investigate the **legality of how the evidence was obtained**. In relation to the latter, it was also questioned whether the **authorisation of a Dutch judge** would guarantee the legality of the (foreign) process of obtaining the evidence. One court also asked questions relating to the **use of the obtained data**.

Court ruling

As regards the meaning of the principle of mutual trust when assessing the legality and reliability of evidence obtained via investigative measures conducted by foreign authorities under their jurisdiction, the court stated that **it is not within the remit of the Dutch judge to review whether the manner in which the investigation was conducted under the responsibility of the foreign authorities is consistent with the rules of law applicable in the country in question for conducting that investigation**. The judge may assume that investigations carried out under the responsibility of foreign authorities have been conducted in such a way that the results obtained by such investigations are reliable. However, if there are concrete indications to the contrary, the judge needs to examine the reliability of the evidence obtained, with a view to its use (or not) in criminal proceedings, in order to guarantee the right to a fair trial.

The court clarified that in connection with the application of an investigative power abroad under the responsibility of a foreign authority, **authorisation by the Dutch examining judge is required only if the investigative measures, to be carried out by the foreign authority, are requested by the Dutch authorities**. This authorisation is therefore not needed when the investigative measure concerned is taking place at the initiative of the foreign authority. The other instance in which the authorisation of the examining judge would be required is **when the foreign authority notifies the Dutch authorities that**

it intends to intercept or has intercepted telecommunications while the telecommunications address of the person to be intercepted or intercepted is in use in the territory of the Netherlands. In this case, the examining judge needs to agree to the interception. Besides these instances, the public prosecutor is not required to seek authorisation from the examining magistrate. This does not detract from the fact that authorisation from the examining magistrate may be sought, in view of the manner in which the data obtained are used in Dutch criminal investigations. Requesting and being granted such an authorisation may thereby safeguard the right to privacy.

The court also clarified that data obtained by a (seconded) member of a joint investigation team may also be used, subject to certain conditions, for criminal proceedings other than that for which the joint investigation team was established.

As concerns the possibilities for the defence to examine the legality of how the evidence was obtained, having regard to the principle of equality of arms (one of the features of the wider concept of a fair trial), the court quoted the European Court of Human Rights: 'the **entitlement to disclosure of relevant evidence is not an absolute right**. In any criminal proceedings, there may be **competing interests, such as national security or the need to protect witnesses at risk of reprisals or keep secret police methods of investigation of crime, which must be weighed against the rights of the accused**.' If a request by the defence to add documents to the case file or to have insight into the case file relates to (the substantiation of) a defence on a point on which the Dutch Criminal Court has no jurisdiction, as a rule there will be no ground for granting this request. In addition, such a request must be substantiated, whereby the substantiation must relate to the importance of the joinder or insight in light of the decisions that can and must be made in the criminal case.

❖ Austria

Rulings by Higher Regional Courts

The higher regional courts ruled that the Austrian jurisdiction depends on where a crypto exchanger is located, which often leads to a lack of jurisdiction in many cases.

Furthermore, the seizing of cryptocurrency on government wallets was declared inadmissible – it is only permitted to secure the cryptocurrency through the crypto exchanger.

Constitutional Court

The seizure and analysis of mobile phones can currently be requested on the basis of a public prosecutor's order. The Constitutional Court ruled that a public prosecutor's order is an insufficient basis to request these measures. A draft law is currently being prepared to make the necessary legislative changes in this area.

❖ Slovenia

Constitutional Court – 6 July 2023 – U-I-144/19

On 6 July 2023, the Slovenian Constitutional Court annulled certain provisions of the Criminal Procedure Act, particularly Articles 149.b and 149.c relating to the acquisition of traffic data and paragraphs 5 and 6 of Article 156, which allow certain financial data to be obtained from debtors without a court order.

The Constitutional Court found that those particular provisions disproportionately interfered with the right to privacy of communications and/or the right to privacy of information.

NB: The Ministry of Justice has prepared amendments to these articles, which could potentially have a restrictive effect on the execution of a (future) European Production Order for electronic evidence. The

proposed amendments could also make it more difficult to identify unknown offenders, which is particularly important in the context of crimes committed through the internet or social media.

❖ Sweden

Supreme Court – 30 March 2023 – Ö 5686-22

In this ruling, the Supreme Court assessed the question whether a remote search may be ordered even when the information to be searched may be stored abroad.

Background

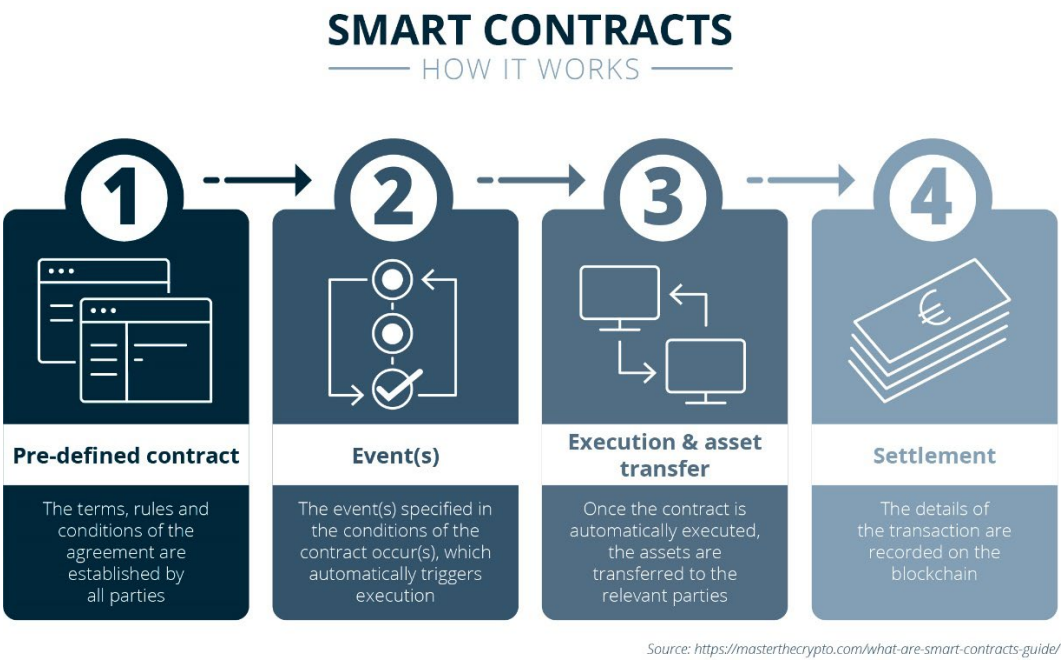
During a preliminary investigation into the facts of money laundering and accounting offences, the prosecutor requested that the district court order a remote search for documents that could be relevant to the investigation of the crimes. According to the prosecutor, the documents were stored in readable information systems, which were accessible on mobile phones and computers seized from the suspect. The prosecutor stated that it was unclear on which cloud service and where the sought-after information was stored. The District Court, concluding that the conditions for ordering a remote search were met, granted the request. The Court of Appeal upheld the decision of the District Court. The Supreme Court subsequently assessed the question whether it was possible to order a remote search, despite the fact that the search concerned information that may be stored abroad.

Court ruling

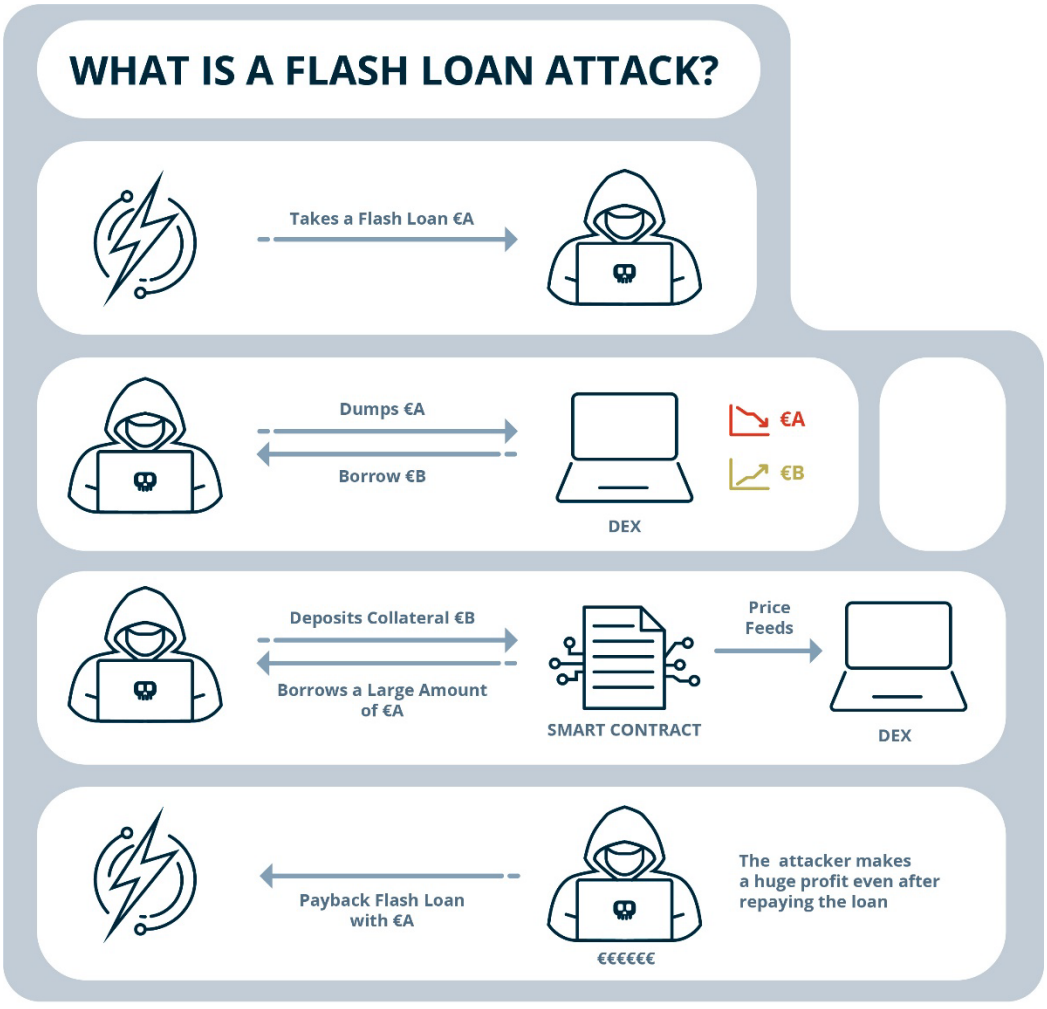
The coercive measure of remote search is regulated in Chapter 28, Sections 10 a–10 i of the Code of Judicial Procedure. When executing a remote search warrant, Swedish authorities may come across electronic documents stored abroad or in an unknown location. The question is whether this circumstance constitutes an obstacle to the measure, either in that no decision on a remote search can be taken at all or in that the decision cannot be executed.

The provisions on remote searches are, by their wording, not limited to searches of information stored in Sweden. On the contrary, it is clear that such a restriction would significantly undermine the purpose of the legislation, as Swedish authorities would then regularly have to request legal assistance from foreign authorities. The negative effects of such a restriction would be particularly evident when it is not known where the information is stored (loss of location), as Swedish authorities would then lack practical possibilities to request legal assistance. The Supreme Court continued by concluding that there is no international legislation or any international agreement binding on Sweden that precludes such an application. It is irrelevant if it is known in which country the information is stored or if the location of the storage is unknown. The Supreme Court thus explained that it was **possible to order a remote search, even though the requested search concerned information that may be stored abroad**.

The court's considerations apply under the condition that the measure is taken within the framework of a Swedish criminal investigation and thus is prompted by a suspicion of crime that falls within Swedish judicial jurisdiction.



Source: https://masterthecrypto.com/what-are-smart-contracts-guide/



Source: https://www.immunebytes.com/blog/top-10-flash-loan-attacks/

4. Data retention developments in Europe

The objective of this section is to provide an overview of the legislative and/or case-law developments within Europe in the area of data retention, following the ruling of the CJEU in 2014 invalidating the data retention directive (Directive 2006/24/EC) and the subsequent CJEU rulings in relation to data retention.

4.1. Developments at the EU level

Rulings: Court of Justice of the European Union

- **Judgment:** ***Procura della Repubblica presso il Tribunale di Bolzano***

  Case C-178/22

Date: 30 April 2024

Judgment rendered by the Grand Chamber of the Court

Reference for a preliminary ruling by: judge in charge of preliminary investigations at the district court, Bolzano, Italy

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

Question referred for a preliminary ruling and considered by the Court:

> *Does Article 15(1) of Directive [2002/58] preclude a provision of national law such as that contained in Article 132[(3)] of Legislative Decree [No 196/2003], … [which] … provides:*
>
> *'3. Within the retention period laid down by law, if there is sufficient evidence of the commission of an offence for which the law prescribes the penalty of life imprisonment or a maximum term of imprisonment of at least three years, determined in accordance with Article 4 of the Code of Criminal Procedure, or of an offence of threatening and harassing or disturbing persons by means of the telephone, where the threat, harassment or disturbance is serious, the data may, if relevant to establishing the facts, be acquired with the prior authorisation of the court, by way of reasoned order, at the request of the Public Prosecutor's Office or upon an application by the legal representative of the accused, of the person under investigation, of the injured party or of any other private party'?*

Court ruling

> *Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, must be interpreted as not precluding a national provision which requires a national court, acting in the context of a prior review carried out following a reasoned request for access to a set of traffic or location data – which are liable to allow precise conclusions to be drawn concerning the private life of a user of a means of electronic communication and retained by providers of electronic communications services – submitted by a competent national authority in the context of a criminal investigation, to authorise such access if it is requested for the purposes of investigating criminal*

offences punishable under national law by a maximum term of imprisonment of at least three years, provided that there is sufficient evidence of the commission of such offences and that those data are relevant to establishing the facts, on condition, however, that that court is entitled to refuse such access if it is requested in the context of an investigation into an offence which is manifestly not a serious offence, in the light of the societal conditions prevailing in the Member State concerned.

The press release on the judgment provided the following information.

In its judgment, the Court holds that the interference with those fundamental rights caused by access to telephone records is likely to be classified as serious, and it confirms that such access can be granted only to the data of individuals suspected of being implicated in a serious offence. The Court clarifies that it is for the Member States to define 'serious offences' for the purposes of applying the directive in question.
[…]
However, the Member States cannot distort that concept of 'serious offences' and, by extension, the concept of 'serious crime', by including within it offences which are manifestly not serious offences, in the light of the societal conditions prevailing in the Member State concerned, even though the legislature of that Member State has provided for such offences to be punishable by a maximum term of imprisonment of at least three years. The Court states, in that connection, that a minimum period fixed by reference to such a term of imprisonment does not appear, in that regard, to be excessively low. Moreover, setting a minimum period above which the term of imprisonment for an offence justifies the classification of that offence as a serious offence is not necessarily contrary to the principle of proportionality.

In order to ascertain, in particular, that there is no distortion of the concept of 'serious crime', it is nonetheless essential that, where access to retained data carries the risk of a serious interference with the fundamental rights of the person concerned, that access be subject to a prior review carried out either by a court or by an independent administrative body.

Furthermore, the court or independent administrative body which carries out that prior review must be entitled to refuse or restrict that access where it finds that the interference with fundamental rights is serious, while it is clear that the offence at issue does not actually constitute serious crime in the light of the societal conditions prevailing in the Member State concerned. Indeed, it must be able to strike a fair balance between the needs of the investigation and the fundamental rights to privacy and protection of personal data ([3]).

- **Judgment: *La Quadrature du Net and Others***
  Case C-470/21

Date: 30 April 2024

Judgment rendered by the Full Court

Reference for a preliminary ruling by: La Quadrature du Net, Fédération des fournisseurs d'accès à Internet associatifs, Franciliens.net and French Data Network, on the one hand, and the Premier ministre (Prime Minister, France) and the ministre de la Culture (Minister for Culture, France), on the other hand.

([3]) https://curia.europa.eu/jcms/jcms/p1_4384676/en/.

Concerning: interpretation of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 (OJ L 337, 18.12.2009, p. 11) ('Directive 2002/58'), read in the light of the Charter of Fundamental Rights of the European Union ('the Charter') (Articles 7, 8, 11 and 52(1)).

Questions referred for a preliminary ruling and considered by the Court:

(1) Are the civil identity data corresponding to an IP address included among the traffic and location data to which, in principle, the requirement [of] prior review by a court or an independent administrative entity [whose decisions are binding] applies?

(2) If the first question is answered in the affirmative, and having regard to the fact that the data relating to the civil identity of users, including their contact details, are not particularly sensitive data, is Directive [2002/58], read in the light of the [Charter], to be interpreted as precluding national legislation which provides for the collection of those data, corresponding to the IP addresses of users, by an administrative authority, without prior review by a court or an independent administrative entity [whose decisions are binding]?

(3) If the second question is answered in the affirmative, and having regard to the fact that the data relating to civil identity are not particularly sensitive data, that only those data may be collected and they may be collected solely for the purposes of preventing failures to fulfil obligations which have been defined precisely, exhaustively and restrictively by national law, and that the systematic review of access to the data of each user by a court or a third-party administrative entity [whose decisions are binding] would be liable to jeopardise the fulfilment of the public service [mission] entrusted to the administrative authority which collects those data, which is itself independent, does [Directive 2002/58] preclude the review from being performed in an adapted fashion, for example as an automated review, as the case may be under the supervision of a department within the body which offers guarantees of independence and impartiality in relation to the officials who have the task of collecting the data?

Court ruling

The press release on the judgment provided the following information.

The Court … holds that the general and indiscriminate retention of IP addresses does not necessarily constitute a serious interference with fundamental rights. Such retention is permitted where the national legislation imposes retention arrangements that ensure a genuinely watertight separation of the different categories of personal data and thus rule out the possibility that precise conclusions could be drawn about the private life of the person concerned.

The Court also specifies that EU law does not preclude national legislation authorising the competent public authority, for the sole purpose of identifying the person suspected of having committed a criminal offence, to access the civil identity data associated with an IP address, retained separately and in a genuinely watertight manner by the internet access providers. The Member States must nevertheless ensure that that access does not allow precise conclusions to be drawn about the private life of the IP address holders concerned. That means that officials with such access must be prohibited

from disclosing information on the content of the files consulted, from tracking the clickstream on the basis of IP addresses and from using those IP addresses for any purpose other than that of identifying their holders with a view to the potential adoption of measures.

Where data relating to the civil identity of users of electronic communications is accessed for the sole purpose of identifying the user concerned, a prior review of that access by a court or by an independent administrative body is not required since the interference entailed by that access cannot be classified as serious. Such a review must be carried out, however, where the particular features of a national procedure governing such access may – through the linking of the data and information collected as that procedure progresses though [through] its different stages – allow precise conclusions to be drawn about the private life of the person concerned and, accordingly, give rise to [a] serious interference with fundamental rights. In such a case, that review by a court or an independent administrative body must take place before that linking, while preserving the effectiveness of that procedure by, in particular, allowing the identification of the cases in which there is a possible further repetition of the offending conduct in question ([4]).

Moreover, the judgment itself stated that 'the data processing system used by the public authority [should be] subject at regular intervals to a review at regular intervals, by an independent body acting as a third party in relation to that public authority, intended to verify the integrity of the system'.

4.2. Developments at the national level

❖ Spain

Judgment, Supreme Court, 54/2024 – 10779/2023, 18 January 2024

The Spanish **Supreme Court reiterated the validity of the Data Retention Law (2007)** and pointed out that the national regulation is respectful of EU law and that the judgments of the CJEU are binding but do not necessarily lead to the nullity of Spanish regulation; rather, there is an obligation to assess if the Spanish retention regime is in accordance with EU law. The court emphasised that the doctrine of the CJEU has been evolving, shifting the problem of the lawfulness of the rule to the evidential validity of the information obtained from the retained data, which, in the opinion of the Supreme Court shows that the CJEU is aware of the complexity of the situation created as a result of its own doctrine and, above all, of the absence of a regulatory framework that provides the necessary legal certainty in this complex area.

❖ France

Judgment, Court of Cassation, case No 22-84.370, 23 May 2023

The court ruled that the invasions of the defendant's privacy were justified by the seriousness of the facts (i.e. cross-border drug trafficking as part of organised crime). In principle, general and indiscriminate retention of traffic and location data is prohibited, with the exception that **a serious and real, current or foreseeable, threat to national security makes it possible to require operators of electronic telecommunications services to retain traffic and location data in a generalised and undifferentiated manner**. Judicial authorities are obliged to check the serious crime criterion and that storage does not go beyond what is strictly necessary (e.g. for establishing and prosecuting offences and searching for perpetrators of offences).

([4]) https://curia.europa.eu/jcms/jcms/p1_4384626/en/.

❖ Lithuania

Law XIV-2386 amending Articles 40 and 78 of the Law on Electronic Communications

On 19 December 2023, Law XIV-2386 amending Articles 40 and 78 of the Law of the Republic of Lithuania on Electronic Communications No IX-2135 was passed.

The amendments provide that **a person concluding a contract for the provision of public mobile communication services under which public mobile communication services are paid for in advance must provide the provider of such services with the data necessary to identify them as a subscriber**. A provider of public mobile communications services shall not be entitled to provide public mobile communications services under a contract referred to in this paragraph unless the identity of the subscriber has been identified (the provisions will enter into force on 1 January 2025).

Article 77(2) of the Law on Electronic Communications provides that:

> *[I]n order to ensure that data are available for the prevention, investigation, detection or prosecution of criminal offences or for the purposes of forecasting, identifying and/or addressing threats that may affect the sovereignty of the State, the inviolability and integrity of the territory, the constitutional order, the interests of the State, or its defence or economic power,* ***providers of public electronic communications networks and/or public electronic communications services shall be obliged to store the data*** *listed in Annex 1 to this Law* ***and to make available to the competent authorities the data they generate or process, in accordance with procedures established by law****.*

Article 78(5) of that law stipulates that the data referred to in Article 77(2) (with the exception of the data necessary to determine the geographic location of the network equipment corresponding to the geotagging zone defined in the telecommunication standards, which shall be kept for 2 months) **shall be kept for 6 months from the date of notification**.

❖ Luxembourg

The bill of Law No 8148 on the retention of personal data is currently under debate in parliament.

❖ Malta

Judgments of the Constitutional Court

In 2023, the Constitutional Court of Malta ruled in a case concerning transnational drug trafficking. The Malta Police Force was made aware of the offence through phone calls intercepted by the Malta Security Service. The defendant contested both the legality of the interception of the phone calls and the illegality of authorities to retain such data for years.

The court ruled **that it does not recognise the plea to remove such data on the basis that it exceeded data retention periods**, stating there was **a lack of abuse and breach of fundamental rights and that such a plea on data retention was to be made in the criminal courts following the court procedure applicable there**.

In another case handled by the Constitutional Court in 2024, related to a criminal case about a murder, the defendant raised a similar plea as in the abovementioned case on data retention, also following recent CJEU judgments on the matter.

The court ruled that this was **irrelevant to the criminal case, citing a lack of relevance and interest on the part of the plaintiff, especially after the plaintiff admitted and pleaded guilty to the charges and a jury was never set up**.

❖ Portugal

Law No 18/2024 amending Law No 32/2008

Following a judgment by the Constitutional Court in 2023, a new data retention law was introduced in January 2024. In general terms, this law keeps in force existing rules regarding the retention of data for billing purposes and extends the retention period to 1 year for data used for the investigation of serious crimes only. In such cases, obtaining the data will depend on the decision of a judge ([5]).

([5]) ::: Lei n.º 32/2008, de 17 de Julho (pgdlisboa.pt)

5. Topic of interest: cooperation with crypto-asset service providers in criminal investigations and prosecutions

Introduction

With the growing digitalisation of our world, developments in the financial system also continue to evolve at a rapid pace. People are increasingly investing and trading in crypto-assets and buying goods and services online with cryptocurrencies rather than using monetary banking systems for online transactions.

There are a number of important differences between monetary banking systems and cryptocurrency payments. Transactions with virtual currencies are more difficult to trace back to physical persons as they are anonymised and encrypted (through the so-called blockchain). The use of cryptocurrency mixers or tumblers, which mix cryptocurrencies with others so as to obfuscate the trail back to the original source of the cryptocurrency, raises the level of anonymity even more. Also, virtual currencies are not regulated in the same way as traditional monetary systems, which gives more freedom to users when making transactions. Because of these specificities, criminals often make use of cryptocurrencies to conduct their illegal business, commit crimes and launder money.

It is evident that the complexity and technicality of cryptocurrency tracing, in combination with the available legal frameworks for investigating cryptocurrency crimes, make the investigation and prosecution of these crimes quite difficult for LEAs and judicial authorities. Similar to financial investigations of bank transactions, where cooperation with financial institutions can advance investigations, LEAs cooperation with CASPs ([6]) can help investigators identify perpetrators through the tracing of cryptocurrency transactions.

The fifth issue of the CJM looked into the topic of handling cryptocurrencies in criminal investigations and proceedings, with a focus on the legal frameworks applied by LEAs and judicial authorities when conducting investigations into cryptocurrencies, along with practical experience, possibilities and challenges encountered in relation to seizures and further handling of cryptocurrency throughout investigations and prosecutions.

This section looks at the topic from a different angle, namely the cooperation of CASPs with LEAs and judicial authorities for the purpose of criminal investigation and prosecution. A general overview is given on cryptocurrency investigations, followed by more specific information related to cooperation with CASPs, particularly for the seizure of cryptocurrencies and in the context of cross-border cooperation.

([6]) Article 3 of the MiCA regulation states that:
'"crypto-asset service provider" means a legal person or other undertaking whose occupation or business is the provision of one or more crypto-asset services to clients on a professional basis, and that is allowed to provide crypto-asset services in accordance with Article 59; …
"crypto-asset service" means any of the following services and activities relating to any crypto-asset:
(a) providing custody and administration of crypto-assets on behalf of clients;
(b) operation of a trading platform for crypto-assets;
(c) exchange of crypto-assets for funds;
(d) exchange of crypto-assets for other crypto-assets;
(e) execution of orders for crypto-assets on behalf of clients;
(f) placing of crypto-assets;
(g) reception and transmission of orders for crypto-assets on behalf of clients;
(h) providing advice on crypto-assets;
(i) providing portfolio management on crypto-assets;
(j) providing transfer services for crypto-assets on behalf of clients'.

Practical experiences, challenges and best practices identified through such cooperation are highlighted. An interesting Swiss court ruling is mentioned at the end as an illustration.

The information presented in this section was gathered via a questionnaire distributed to the experts of the EJCN. In total, replies from EJCN members from 21 countries were received, including two non-EU countries (Norway and Switzerland).

Cryptocurrency investigations

Investigating cryptocurrency crimes is often very complex and time-consuming because of the characteristics of how these intangible assets are stored, transmitted and used. The **challenges** that can occur during an investigation are multiple:

- the use of anonymisation (mixer) services, decentralised platforms/cryptocurrencies, private coins/exchanges and unhosted wallets makes the tracing of the origin of the transactions and funds very difficult;
- unregistered or uncooperative platforms, hindering the tracing of cryptocurrencies;
- the use of smart contracts ([7]);
- the technical complexity of cryptocurrency tracing, requiring LEAs with specific expertise and often costly tracing tools;
- the lack of knowledge among police, prosecutors and judges, resulting in the need to explain how the blockchain works and how crypto tracing is done, in view of the correct investigative process, the reliability of crypto analysis and eventual admissibility of evidence in court;
- the lack of a (domestic) regulatory legal framework on the seizure and management of cryptocurrencies, along with difficulties in legally qualifying certain actions (e.g. smart contracts);
- international police/judicial cooperation can be cumbersome, particularly when involving non-cooperative countries or countries outside the EU where targets and/or services are hosted;
- mutual legal assistance (MLA) in the framework of international cooperation can take a long time;
- the lack of cooperation from cryptocurrency exchanges / CASPs that are located abroad or have no location / do not provide information on on their location, which hinders the eventual sending of EIO or MLA requests.

In order to **address certain of these challenges**, some countries have developed guides for the seizure of cryptocurrencies and provide training or methodologies to investigators to conduct transaction analysis or cryptocurrency tracing. Also, one country provides specific tracing tools to the police for this purpose.

Two Member States have specific legal provisions in place that provide clarity on how to conduct investigations. In Lithuania, Order No I-64 of the Prosecutor General of the Republic of Lithuania of 9 March 2020 approved methodological guidelines for conducting proceedings with virtual currencies, which cover the peculiarities of the seizure of virtual currencies in the course of a search or a seizure and the peculiarities of their return or sale in the course of a pre-trial investigation. In Hungary, a new rule was introduced in the Code of Criminal Procedure on 1 March 2024, which allows LEAs to carry out a transaction for transferring crypto-assets originating from a crime to an official law enforcement wallet when the provider is uncooperative or impossible to contact.

([7]) A digital agreement that is signed and stored on a blockchain network, which is executed automatically when the contract's terms and conditions are met.

Cooperation with CASPs

- General observations

The fifth anti-money laundering directive (AML directive) imposed a **registration obligation for CASPs**. In order to be able to conduct business in a Member State, CASPs first have to register with the appropriate authorities. The number of CASPs offering services in a country and subject to that country's jurisdiction, whether domestic or foreign controlled, differs widely from country to country. Some respondents replied that there are only a few CASPs active in their territory; others reported a couple of dozen; and several mentioned over a hundred CASPs being registered. One country even mentioned almost 600. These range from numerous small CASPs to major international CASPs that are providing services worldwide.

Given the high quantity of CASPs active in Europe, it is obvious that LEAs and judicial authorities will not yet have had practical experience with each and every CASP active in their country. Moreover, experiences in **cooperation** currently differ from CASP to CASP, which might partly stem from the different ways in which the AML directive has been transposed into national law throughout the EU. The MiCA regulation, which will enter into force at the end of 2024 (see Section 1), aims to regulate the crypto industry, with new requirements for financial institutions and CASPs related to transparency, disclosure, supervision, protection of clients and prevention of market manipulation.

The **records that CASPs can provide** to authorities include registration and other account information (name, email, baking information), transaction data and IP address information (registration IP, last login IP, etc.). In some cases, customer service chats, know-your-customer data, linked accounts and devices associated with the account, pictures and credit card information can also be provided.

Although CASPs are legally obliged to respond to requests from the police or judicial authorities, half of the respondents replied that CASPs in their country cooperate on a voluntary basis as well, providing information that can be used for intelligence purposes. On the other hand, in other countries, this would not be possible, and a formal written request from the relevant authorities would be required. For requests to CASPs in another jurisdiction, an MLA request or EIO is needed. Overall, most respondents reported that cooperation with CASPs is going well, although there are differences to be observed with certain CASPs not cooperating, or cooperating depending on the type of request. Next to this, CASPs are also legally obliged, following the implementation of the fifth AML directive, to **cooperate with financial intelligence units**. This includes the reporting of suspicious transactions.

As to the **ways of cooperating with CASPs**, most countries refer to the legal provisions detailing the procedure for requesting and obtaining information from financial institutions, including CASPs, during a criminal investigation. Next to this legal framework, there are some practical tools provided by CASPs for receiving law enforcement requests, such as contact addresses of the CASPs, request forms or dedicated platforms. Several respondents indicated that they have or are in the process of creating guidelines for the police and prosecutors on crypto-assets. Also, the practical guidelines provided by Europol, the Sirius project and the EJCN were mentioned as useful tools in this respect.

- Seizure and handling of crypto-assets in criminal investigations

Since the fifth edition of the CJM, besides Hungary, France and Slovakia have also introduced specific **legal provisions** covering the seizure of cryptocurrencies. In Luxembourg, specific provisions on the management (transfer, storage and conversion) of cryptocurrencies were introduced in 2022.

The procedure for the seizing and further handling of crypto-assets was elaborated in detail in the **fifth edition of the CJM**. In relation to the cooperation with CASPs in this respect, it can be noted that several respondents mentioned that some CASPs **proactively freeze accounts** following a notification from the police or financial intelligence unit that a seizure order will follow. A few respondents stated that this voluntary cooperation by certain CASPs only happened when they were located abroad (so not domestic CASPs). For other countries, such a procedure would, however, not take place or even be possible.

A few **challenges** related to the cooperation with CASPs in the context of seizing cryptocurrencies were mentioned:

- the execution of MLA requests for seizures can be very time-consuming;
- the location of the seat of a CASP is unknown, and as a result an MLA request for seizure cannot be sent out;
- non-cooperative CASPs (usually in foreign countries);
- the inability to enforce the execution of foreign freezing certificates related to crypto platform services that were not licensed in the country.

In many countries, **manuals or guidelines** have been developed for LEAs and/or judicial authorities in relation to the handling of cryptocurrencies in criminal investigations, including the seizure and confiscation of cryptocurrencies. A few countries have developed methodological guidelines for LEAs relating to the securing and storage of cryptocurrencies. In some countries, legal guidelines for prosecutors and forensic accountants are also available.

➢ International judicial cooperation

Many respondents indicated that, in general, cooperation with CASPs that are located in another country goes well. Foreign CASPs can decide for themselves whether to respond to direct requests for information from foreign authorities and **cooperate on a voluntary basis**. Experiences in this respect differ per CASP. In case they do not want to cooperate voluntarily, authorities will have to follow the procedure for international legal assistance and send an **MLA request or EIO** to obtain the required information. Unfortunately, there are also non-EU countries that do not respond to international legal assistance requests. Also, the time-consuming nature of MLA requests is often an issue, particularly in the context of cryptocurrency investigations, as digital assets are volatile and can be moved very quickly. Therefore, freezing assets quickly is challenging without approaching the CASPs directly. In Sweden, the issue of volatility has been addressed by asking for forfeiture of the crypto-assets value in krona (SEK) on the day a verdict can no longer be appealed. Some respondents indicated as well that there are CASPs abroad that require certain procedures, authorisation from a court or the use of their own platforms before replying to a request, which is not possible under the law of the requesting country.

All respondents confirmed being able to **seize cryptocurrencies in response to EIO or MLA** requests from foreign judicial authorities, provided that the legal requirements were met. Within the EU, authorities can issue a freezing or confiscation order, in accordance with Regulation (EU) 2018/1805 on the mutual recognition of freezing orders and confiscation orders. Information related to the cryptocurrencies, such as wallet addresses, amounts to be seized, wallet holder and hash of transactions, should be included in the request.

So far, there is no abundant **case-law** on the topic of cooperation with CASPs. An interesting judgment of the Court of Appeal of the canton of Berne (Switzerland) was rendered on 4 December 2023 in relation to the blocking of a cryptocurrency exchange account, following an order from the public prosecutor that was sent directly to Binance. The court considered that, in contrast to conventional fiat currencies, cryptocurrencies are not stored locally at a specific location but are stored in a decentralised or location-

independent manner on a blockchain. In addition, the Binance cryptocurrency exchange does not have a fixed location and only appears to be accessible via the internet. Against this background, no request for MLA can be made to another state and the public prosecutor's office does not violate the principle of territoriality by contacting the cryptocurrency exchange Binance directly or without a prior request for MLA to block the account of the accused person.

Also, the higher regional courts in Austria and the French Correctional Court in Paris have rendered rulings in the past year related to cryptocurrency investigations and exchanges (see Section 3).

Conclusion

Criminal investigations into cybercrime or cyber-enabled crime usually involve cryptocurrency investigations. In this respect, LEAs and judicial authorities very often require cooperation from CASPs to obtain customer records and related information or to freeze or seize crypto-assets. Such cooperation goes well, in general, but often also depends on the willingness of the CASPs to cooperate on a voluntary basis. If this is not the case, authorities have to resort to the formal route by sending an EIO or MLA request to the country where the CASP is located. However, following this route can be challenging if the CASP cannot be located, and even when an MLA request is sent, the time it takes to receive a response can be (too) long, which, due to the volatile nature of crypto-assets, could render the whole process unsuccessful.

Within the EU, the MiCA regulation, entering into force at the end of 2024, will hopefully help to improve cooperation with CASPs.

6. Future of the *Cybercrime Judicial Monitor*

The CJM is produced once per year and mainly reports on information related to the previous year. The CJM is published on the Eurojust website and distributed to judicial and LEAs 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, 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.

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

Catalogue number: QP-AG-24-001-EN-N • ISBN: 978-92-9404-304-7 • ISSN: 2600-0113 • DOI: 10.2812/331733

Eurojust is an agency of the European Union