# Cybercrime Judicial Monitor

Issue 7 – June 2022

*Criminal justice across borders*

# Contents

# 1. Executive Summary

Eurojust presents this seventh 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 cybercrime and cyber-enabled crime. It is produced on the basis of information provided by members of the European Judicial Cybercrime Network (EJCN). All issues of the CJM are available on the Eurojust website.

The CJM contains four main sections. The first section covers legislative developments in the area of cybercrime, cyber-enabled crime and electronic evidence in 2021.

The judicial analysis section presents brief summaries of court rulings rendered by courts in various EU Member States and non-EU countries.

The next section covers the developments within the European Union in the past year, in relation to data retention. An overview of recent case-law of the European Court of Justice is provided, along with some national developments.

The topic of interest in this issue of the CJM provides information on ransomware investigations, from the perspective of law enforcement and judicial authorities. This section gives an overview of the applicable national legal provisions in Europe for investigating ransomware attacks. The different national approaches to such investigations are touched upon, followed by a presentation of case experiences, including challenges and good practices. This section also elaborates on the cooperation between the public and private sector in ransomware investigations.

# 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 2021. The main sources of national information presented in this section are contributions collected through the EJCN.*

## 2.1. International level

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

On 17 November 2021, 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.

The Second Additional Protocol supplements the Cybercrime Convention and its First Protocol. The Protocol 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.

The Protocol provides a legal basis for:

- direct requests to obtain domain name registration information in other jurisdictions;
- direct cooperation with service providers in other jurisdictions to obtain subscriber information;
- more effective means to obtain subscriber information and traffic data through government-to-government co-operation;
- expedited forms of cooperation in emergency situations;
- additional tools for mutual assistance, such as videoconferencing and joint investigation teams; and
- personal data protection safeguards.

The text was opened for signature in Strasbourg on 12 May 2022.

Access the full text of the Second Additional Protocol.

## 2.2. EU level

- *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*

On 21 April 2021, the European Commission announced its proposal for a Regulation on artificial intelligence (AI). The proposed Regulation lays down a uniform legal framework for the development, marketing and use of AI. It also aims to address risks of specific uses of AI, to ensure the trustworthiness of the AI systems.

Article 5 of the proposal refers to prohibited AI practices, including the use of AI practices for law-enforcement purposes.

The Council reached a compromise text version on the proposal at the end of last year.

Access the full text of the Proposal for a Regulation.

- *Regulation (EU) 2021/1232 of the European Parliament and of the Council of 14 July 2021 on 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*

On 10 September 2020, the Commission presented a first legislative proposal to tackle child sexual abuse online. The proposal contained an interim Regulation allowing number-independent interpersonal communications services, such as webmail, messaging services and internet telephony, to derogate from the privacy rules contained in the ePrivacy Directive ([1]) to enable them to continue to detect, report and remove child sexual abuse material online on a voluntary basis. The Regulation was adopted on 14 July 2021 and entered into force on 2 August 2021. It will apply until 3 August 2024.

The Commission is now working on permanent rules, which are intended to replace the interim Regulation.

Access the full text of Regulation (EU) 2021/1232.

## 2.3. Member States

### Austria

- *Amendment Article 126c §1a Criminal Code*

The punishment for committing 'fraudulent misuse of data processing' was raised to 2 years imprisonment. This amendment was introduced by the federal law amending the Criminal Code and the Payment Services Act 2018 to implement the Directive on combating fraud and counterfeiting of non-cash means of payment.

- *Amendment Article 107c Criminal Code*

The legal provision on 'continuing harassment by means of a telecommunications or computer system' was amended. The wording of Article 107c of the Austrian Criminal Code was changed. Previously, the offender had to have acted for a longer period of time. With the amended provision, it is sufficient that the offence is ongoing. Therefore, the article could now also be applicable if the offender for instance publishes (once) a pornographic picture of a person without their consent on the internet that is retrievable for a longer a period of time. In paragraph 2 of Article 107c of the Austrian Criminal Code, the punishment of imprisonment for up to 3 years was introduced for cases where the offence was ongoing for more than 1 year.

- *Amendment Article 76a Code of Criminal Procedure*

Article 76a of the Code of Criminal Procedure concerns the obligation for (communication) service providers to provide information on subscriber and access data of a user at the request of judicial or investigative authorities. This article was amended and now includes 'other service providers' so that, for instance, over-the-top services are also included.

([1]) Articles 5(1) and 6(1) of Directive 2002/58/EC.

## Finland

- *Section 12 (597/2021) Criminal Code*

The Finnish Criminal Code was amended in view of transposing Directive (EU) 2019/713 of the European Parliament and of the Council of 17 April 2019 on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA ([2]). The amendment introduced a new section on 'means of payment offences' into the Criminal Code.

## France

- *Law No 2021-478 protecting minors from sexual offences and incest – Articles 227-22-2 and 227-23-1 Criminal Code*

The new Law No 2021-478 of 21 April 2021 protecting minors from sexual offences and incest created new offences to protect minors. It establishes Article 227-23-1 Criminal Code, which criminalises the soliciting by an adult of a minor, including on the internet, to distribute or transmit pornographic images, videos or representations of the minor. The law also introduces Article 227-22-2 Criminal Code, which criminalises inciting, by an adult, a minor to have sexual practices on the internet ('sextortion').

- *Law No 2021-1109 reinforcing respect for the principles of the Republic – Article 223-1-1 Criminal Code*

The new Law No 2021-1109 of 24 August 2021 reinforcing respect for the principles of the Republic aims to combat community withdrawal and the development of radical Islamism. It introduced Article 223-1-1 Penal Code, which criminalises the endangerment of others by communicating, including on the internet, information about a person that exposes them or members of their family to a direct risk of harm to the person or property.

## Germany

- *Telecommunications Modernization Act*

On 1 December 2021, the Telecommunications Modernization Act (TkMoG) came into force, making significant changes to the existing laws (Telecommunications Act / Telemedia Act) and supplementing them with the Telecommunications and Telemedia Data Protection Act.

The TkMoG significantly expands the range of service providers subject to the Telecommunications Act (TKG). Whereas previously only 'traditional' telecommunications services such as telephone and internet access services were indisputably covered by the TKG, this was unclear for other services such as email and messenger services (e.g. WhatsApp, Signal, Threema, Telegram). According to the prevailing opinion, these and other over-the-top services (OTT1 services) were subject to the Telemedia Act, which meant that, although it was possible to conduct searches of inventory and usage data pursuant to the Code of Criminal Procedure, the applicability of interception measures of the Code of Criminal Procedure to these services was highly controversial.

([2]) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.123.01.0018.01.ENG

The TKMoG now focuses the definitions more on the mode of operation and less on technical aspects. Telecommunications services are now 'services normally provided for remuneration via telecommunications networks which – with the exception of services that offer content via telecommunications networks and services or exercise editorial control over them – comprise the following services:

(a) internet access services;

(b) interpersonal telecommunications services; and

(c) services which consist wholly or mainly of the transmission of signals, such as transmission services used for machine-to-machine communications and for broadcasting.'

The term 'interpersonal telecommunications service' is newly introduced as 'a service usually provided for remuneration which enables a direct interpersonal and interactive exchange of information via telecommunications networks between a finite number of persons, the recipients being determined by the persons who initiate or are involved in the telecommunications; this does not include services which enable interpersonal and interactive telecommunications merely as a subordinate ancillary function inextricably linked to another service.'

This definition includes, in particular, conventional voice telephony, internet telephony, e-mails, messenger services and group chats. However, services in which telecommunications are only a 'secondary function' (such as chat functions in online games or messenger services in social networks) are excluded.

Social networks such as Facebook, Instagram, Twitter and YouTube that do not meet the above definitions continue to be telemedia services.

Number-based interpersonal telecommunications services are still obliged to store inventory data. This includes, in particular, the telephone number, name, address and date of birth of the subscriber together with the address of the connection, the date the telephone number was assigned or the start of the contract, and the device number of any mobile communications terminal provided.

Number-independent interpersonal telecommunications services must store inventory data only if they collect this data at all. This obligation does not cover inventory data such as payment data and users' account details or the time of the last use of the service and the IP address used. However, these inventory data are regularly collected and stored voluntarily by the telecommunications services, so that there is also an obligation to provide information in this respect.

There is still no obligation to disclose inventory data – with the exception of the name, address and date of birth of users of prepaid mobile communications services.

Telemedia services are not obliged to collect and store certain inventory and usage data for information requests from security authorities, nor is there any verification obligation.

## Greece

- *Article 265 Code of Criminal Procedure*

A new provision was enacted in the Code of Criminal Procedure concerning the possibility and the means of gathering cybercrime-related e-evidence such as computer data, data in the cloud or data on USB sticks. A special unit was established in the cybercrime department of the Hellenic Police, with the task of collecting and analysing the e-evidence gathered in this context and subsequently drafting a detailed report for the public prosecutor.

## Ireland

- *Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2021*

Ireland has passed a new money laundering Act, which provides that a virtual currency provider is considered a financial institution and is obliged to register with the Irish Central Bank regulator. The Act also incorporates definitions within the domestic law for virtual currency wallets, etc.

## Portugal

- *Law No 79/2021 of 24 November 2021 amending the Cybercrime Law*

An amendment was introduced in the Portuguese Cybercrime Law (Law nº 109/2009 of 15 September 2009) for the purpose of transposing the provisions of the Directive (EU) 2019/713 of the European Parliament and of the Council of 17 April 2019 on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA.

In practical terms, this revision of the Cybercrime Law (operated by Law No 79/2021 of 24 November 2021) adjusted the entire system of punishment of the criminal use of payment cards, the respective data and other payment systems.

## Slovak Republic

- *Act No 312/2020 Coll. – Sections 83a §1, 131 §6 and 7, 219 and 247 Criminal Code and Sections 96d and 91 §6 Code of Criminal Procedure*

New legal provisions were adopted by the Act No 312/2020 Coll. of 21 October 2020 on the execution of the decisions on seizure and the management of seized property and on amendments to certain acts. The legislation came into effect on 1 January 2021 (some provisions on 1 August 2021).

This Act introduced the definition of 'virtual currency' into the Criminal Code (Section 131 §6). Virtual currency was also added to the definition of 'means of payment' (Section 131 §7). Also, Section 83a on 'confiscation of a part of the property' was introduced into the Criminal Code. Several legal provisions were amended by adding the words 'by a more serious course of action' to the provisions on 'illegal access to a computer system' (Section 247), 'unlawful intervention into a computer system' (Section 247a), 'unlawful interference with computer data' (Section 247b) and 'production and possession of access devices, passwords to computer systems or other data' (Section 247d). Likewise, these additions were made to the criminal offence of 'unauthorised manufacture and use of a means of payment' (Section 219).

The Act also introduced the new provision of Section 96d of the Code of Criminal Procedure, which contains procedural rules concerning the seizure of virtual currency. A prosecutor or judge may issue an order to seize virtual currencies when established facts imply that the virtual currencies are the instruments or proceeds of crime. The order imposes the virtual currency to be provided, including the password, access code or similar data allowing it to be disposed of.

The former Section 90 of the Code of Criminal Procedure ('preservation and disclosure of computer data') is now Section 91, to which a new paragraph 6 has been added as well.

➢ *Act No 236/2021 Coll. – Section 360b Criminal Code*

Act No 236/2021 Coll. introduced the criminal offence of 'dangerous electronic harassments' into the Criminal Code. The legal provision reads as follows.

'(1) A person who intentionally substantially worsens the quality of life of another individual through an electronic communication service, a computer system, and/or a computer network by:

a) long-lasting humiliation, intimidation, unauthorised acting in his/her name, or other harassment; and/or

b) unauthorised publication or disclosure to a third party of a visual, audio or audiovisual recording of his/her personal expression(s) obtained with his/her consent, if the publication/disclosure is capable of causing a significant threat to his/her reputation or another serious loss of his/her rights;

shall be sentenced to imprisonment for up to 3 years. […]'

### Sweden

➢ *Chapter 27 §§ 16 and 16 a. Code of Judicial Procedure*

Legal provisions have been introduced in Sweden allowing an order to preserve data to be issued. These legal provisions made it possible to ratify the Budapest Convention. Sweden became a Party to the Convention on 1 August 2021.

Chapter 27 §§ 16 and 16a of the Swedish Code of Judicial Procedure stipulates that a person who holds stored information, which can reasonably be assumed to be relevant to an investigation if a crime is committed, may be ordered to retain the information. An order to preserve data can be issued for 90 days and it may be prolonged yet another 90 days. It may not be issued against a suspect. A prosecutor or a police officer in charge of an investigation can issue an order.

## 2.4. Non-EU countries

### Switzerland

➢ *Article 46 on Provision of data of the Ordinance on Internet Domains (OID)*

For reasons of data protection, Article 46 of the OID related to the data that can be published by the registry in the RDDS database (WHOIS) was amended. So far, anyone could check anonymously the identity of the holder of a '.ch' domain in the RDDS database. Through the change in Article 46(3), the person requesting access to the personal data of the holder of a concerned domain name now needs to have an 'overriding legitimate interest' for it. It is no longer possible to obtain access to the data anonymously.

# 3. Judicial analysis

*The objective of this analytical chapter is to provide insight into cybercrime judgements rendered within the European Union and at international level. It is intended to help practitioners and offer relevant case studies and/or comparative analyses. The analyses focus on the most interesting aspects of the cases, rather than covering all issues and arguments addressed by the courts.*

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

## 3.1. Court rulings in brief

- **Constitutional Council, decision No. 2021-933 QPC, France**

  Date: 30 September 2021

This ruling is a constitutional validation of the new provisions of the Criminal Code on invasion of privacy. The Constitutional Council found Article 226-2-1 of the Criminal Code consistent with the Constitution. The provision criminalises the act of deliberately violating the privacy of another person by disseminating, without consent, any recording or document pertaining to words or images of a sexual nature, obtained with the express or presumed consent of the person or by the person himself or herself.

- **Court of Appeal, [2021] IECA 45, Ireland**

  Date: 18 February 2021

The appellant in this case had been convicted for conspiracy to possess firearms, ammunition and explosives by the Circuit Criminal Court. He appealed the decision on several grounds, one of them being that the document that was produced as evidence, recording the exchanges on the Dark Web between a user and an undercover Federal Bureau of Investigation officer, did not accord with the established case-law on agent provocateur.

At the time, the undercover agent had received an unsolicited message from a user, enquiring about the purchase of products (weapons and ammunition) which the undercover agent had indicated that he had available for purchase. The purchase was concluded and the products were delivered to the given address.

The Court of Appeal assessed the question of entrapment. The Court started by saying that there was never any suggestion or any contact between the undercover agent and the appellant. Therefore, the agent was not the reason for the appellant to become involved in the offence. The Court points out that there is a difference between the inevitable use of techniques to spy on criminal activity, which is legitimate, and the use of agent provocateur who go beyond mere solicitation and encouragement and initiate a criminal design for the purpose of entrapping a person in order to prosecute the person so

caught. A defence of entrapment cannot sensibly arise simply because an opportunity was provided to a person to commit a crime to which there was already a predisposition. Entrapment as a defence can arise only where a person who is not intending to commit a crime is inveigled into that disposition and later commits an offence because of persuasion by agents of the State ([3]). In this case, although the undercover agent offered his products for sale on the Dark Web, it was the user who launched the transaction by contacting the undercover agent.

The Court accordingly concluded that this ground failed.

- **Supreme Court, STS No 395/2021, Spain**

  Date: 6 May 2021

Up to now, the established doctrine of the Spanish Supreme Court considered that 'continuity' was not applicable in offences involving the production of child pornography when the perpetrator carries out several acts of producing pornographic material, even distanced in time, involving the same minor. This doctrine was based on the wording of the definition of the crime, as 'pornographic material' was referring to a plurality of components.

The judgment of the Supreme Court of 6 May focuses more on the protected right, namely the sexual indemnity of minors. The Court considers that there can be a 'continuity' of crime when the repetition of the action against the same child presents an autonomous and clearly differentiated act, insofar as it impacts the educational process of the minor, by potentially shaping the child's future behaviour profoundly and significantly more than previous practices would have done.

- **District Court of Oslo, Norway**

  Date: 2 November 2021

The District Court of Oslo decided on 2 November 2021 that evidence connected to a Norwegian criminal case using data from Encrochat could be presented to the court. This decision was appealed to the Borgarting appeals court and is still pending before court.

Further information on the court ruling will be provided in the next CJM.

- **Federal Supreme Court, A-5373/2020, Switzerland**

  Date: 11 February 2021

The Federal Supreme Court determined that Protonmail was not a provider of telecommunication services but a provider of derived communication services as per Article 2 of the Federal Act on the Surveillance of Post and Telecommunications (SPTA).

The Federal Supreme Court motivated its decision as follows:

The appellant describes its Mail service as a secure email service with built-in end-to-end encryption and state-of-the-art security features. Messages are stored on servers in an encrypted format. They are also transmitted in an encrypted format between the servers and the user's devices. Messages between Mail users are also transmitted in encrypted form across the network. Mail's 'zero access' architecture

([3]) See paragraph 19.02 of Criminal Law and Evidence, Bloomsbury Professional, 2020.

means that the data is encrypted in such a way as to make it inaccessible to the appellant. The data is encrypted on the client side using an encryption key to which she does not have access. The lower instance court does not claim that the appellant provides access to the internet or that it assumes any responsibility towards its customers for the transmission of information via the internet. Mail's customers must therefore use a third-party telecommunications service provider in order to have the internet access (fixed or mobile) necessary to transport information. In this situation, the Mail service is an over-the-top service, i.e. a service provided via the internet, but which does not itself constitute an internet access service.

Thus, the Mail service does indeed fall under the heading of derived communication services within the meaning of Article 2 of the SPTA, and not telecommunications services. The fact that the service is end-to-end encrypted does not change anything in this respect.

There is a difference between providers of telecommunication services and providers of derived communication services with respect to their duties of collaboration with the relevant authorities. Providers of derived communication services have less obligations than providers of telecommunication services. According to Article 27 SPTA, the providers of derived communications services '… must tolerate surveillance carried out by the Service or by persons it designates of the data that the person under surveillance transmits or stores using derived communications services. For this purpose, they must, without delay, grant access to their facilities and provide the information required for the surveillance. On request, they must supply the secondary telecommunications data of telecommunications available to them relating to the person under surveillance …'.

According to Article 26 SPTA, aside from the duties mentioned above, providers of telecommunication services have additional duties. On request, they must supply the content of the telecommunications to and from the person under surveillance to the service or to the ordering authority or the authority designated by the ordering authority. They must also remove any encryption they have applied.

Access the text of the Federal Act on the Surveillance of Post and Telecommunications.

# 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 Court of Justice of the European Union (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 EU level

### European Court of Justice

❖ **Judgment 'Prokuratuur' – Case C-746/18**

Date: 2 March 2021

Judgment rendered by the Grand Chamber of the Court – Rapporteur: Thomas von Danwitz

Reference for a preliminary ruling by: Supreme Court of Estonia

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 EU Charter.

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

1. Must Article 15(1) of Directive 2002/58/EC be interpreted as meaning that in criminal proceedings the access of state authorities to data, making it possible to establish the source and destination, date, time duration and type of communication, the (location of the) terminal used from a means of electronic communication of a suspect, constitutes such a serious interference with the suspect's fundamental rights that that access, in the area of prevention, investigation, detection and prosecution of criminal offences must be restricted to the fight against serious crime, regardless of the length of the period in respect of which access to those data is sought and the quantity and the nature of the data available in respect of such a period?

2. Must Article 15(1) of Directive 2002/58/EC be interpreted as precluding national legislation that confers upon the public prosecutor's office, whose task is to direct the criminal pre-trial procedure, acting independently and ascertaining both the incriminating and exonerating circumstances for the accused, and to bring, where appropriate, the public prosecution in subsequent proceedings, the power to authorise access of a public authority to traffic and location data for the purposes of a criminal investigation?

Court ruling:

- Article 15(1) of Directive 2002/58/EC must be interpreted as precluding national legislation that permits public authorities to have **access** to a set of traffic or location data, that are liable to provide information regarding the communications made by a user of a means of electronic

communication or regarding the location of the terminal equipment which he or she uses and to allow precise **conclusions to be drawn concerning his or her private life**, for the purposes of the prevention, investigation, detection and prosecution of criminal offences, without such access being confined to procedures and proceedings to combat **serious crime** or prevent serious threats to public security, and that is so **regardless of the length** of the period in respect of which **access** to those data is sought **and the quantity or nature of the data** available in respect of such a period.

- Article 15(1) of Directive 2002/58/EC must be interpreted as precluding national legislation that confers upon the **public prosecutor**'s office, whose task is to direct the criminal pre-trial procedure and to bring, where appropriate, the public prosecution in subsequent proceedings, the power to **authorise access** of a public authority to traffic and location data for the purposes of a criminal investigation.

Access the judgment of the CJEU.

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

Date: 5 April 2022

Judgment rendered by the Grand Chamber of the Court – Rapporteur: Thomas von Danwitz

Reference for a preliminary ruling by: 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 EU Charter.

*Que*stions referred for a preliminary ruling and considered by the court:

1. Is a general/universal data retention regime – even subject to stringent restrictions on retention and access – per se contrary to the provisions of Article 15 of Directive 2002/58/EC, interpreted in the light of the Charter?

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 assessing, in the context of determining the compatibility with EU law and in particular with Charter 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 Court of Justice 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, is it entitled to limit the temporal effect of any such declaration, if 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 TFEU 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 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 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 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 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;

  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.

Access the judgment of the CJEU.

## 4.2. Developments at national level

### France

The Law No. 2021-998 of 30 July 2021 relating to the prevention of acts of terrorism and intelligence, has modified the framework for the retention of connection data by electronic communications operators, internet service providers (ISPs) and hosting companies.

Connection data is now required to be kept as follows:

– For the purposes of criminal proceedings, the prevention of threats to public security and the safeguarding of national security: information relating to the civil identity of the user (up to 5 years) and information provided by the user when subscribing to a contract or creating an account, along with information relating to payment (up to 1 year).

– To fight against crime and serious delinquency, to prevent serious threats to public security and safeguarding national security: technical data enabling the identification of connection sources or data relating to the terminal equipment used (up to 1 year).

– For reasons relating to the safeguarding of national security, when a serious, current or foreseeable threat is observed: the Prime Minister may, by decree, order electronic communications operators to retain certain categories of traffic and location data specified by decree in the Council of State (up to 1 year).

**Judgment Council of State, *French Data Network*, 21 April 2021**

In its judgment of 21 April 2021, the Council of State examined the compliance of French rules on the retention of connection data with European Union law. The Council of State ruled that the generalised retention of data by telecommunications operators is today justified in view of the existing threat to national security. The Council noted that the possibility of accessing this data for the fight against serious crime makes it possible, to date, to guarantee the constitutional requirements of prevention of attacks on public order and the search for the authors of criminal offences. However, it ordered the government to conduct a 'periodic review of the existence of such a threat' to justify this generalised data retention. The Council of State also asked the government to make the use of this data by the intelligence services subject to the authorisation of an independent authority.

## Norway (non-EU)

In 2021, the Norwegian Parliament approved amendments to the Electronic Communications Act and introduced new provisions (§ 2-8a and § 2-8b) requiring ISPs to retain IP-addresses and related information for a period of 12 months. The ISPs are required to have technical systems in place by 1 January 2023 at the latest.

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, as well for some specific types of crimes, including crimes against computer systems such as illegal access, illegal use of identity, computer system break-in, violation of private communication. Crimes as described in Articles 2 to 8 of the Budapest Convention would therefore also be covered.

Access the Norwegian text of the Electronic Communications Act.

# 5. Topic of interest

## Ransomware investigations: national legal frameworks in Europe, case experiences and cooperation with the private sector

### Introduction

Ransomware has become a global threat and problem. The scale, sophistication and impact of ransomware attacks has increased significantly over the past years, in part due to the pandemic. As a result, the success of criminal investigations and prosecutions depends ever more on close cooperation and coordination, mostly cross-border, between the involved stakeholders: the reporting of ransomware attacks by victims, the preservation and possible analysis of digital evidence by private companies and investigation and prosecution by public authorities. Actions by each of these stakeholders play an essential role in the mitigation of damages, disruption of an attack and identification of the perpetrators and their prosecution.

This chapter presents different aspects related to ransomware investigations, from the perspective of law enforcement and judicial authorities. First, the national legal contexts in Europe for investigating ransomware are presented. Next, an insight is given into national and international approaches to ransomware investigations, along with practical experiences in cases, including challenges and good practices encountered by police and judicial authorities. Furthermore, a section is devoted to cooperation between law enforcement and judicial authorities and the private sector. This section explains the different interests and priorities of public authorities and victims and private entities. The national legal contexts for public-private cooperation are briefly presented, followed by experiences in ransomware investigations in which such cooperation took place.

This chapter is based on information provided by the members of the European Judicial Cybercrime Network (EJCN). A dedicated questionnaire was sent for this purpose to the EJCN, to which 20 replies were received ([4]). Additionally, information was used from the 'map of ransomware', which was developed by the EJCN.

### Investigating ransomware attacks: Legal frameworks in Europe

All 20 respondents replied that there are no specific **substantive provisions** in place in their country that criminalise ransomware attacks. The countries apply (multiple) general penal provisions on unlawful access to, use of, interference with and/or damage to a computer system; unauthorised alteration, copying and/or transferring of data or making data inaccessible; distribution or possession of equipment or malware intended to damage or disrupt computer systems; vandalism; extortion or blackmail; and receiving proceeds from crime or a payment following an offence ([5]). In the latter case, the penalty for the perpetrator is increased. All respondents consider these penal provisions sufficient to address ransomware attacks, and do not see a need for specific legal provisions on ransomware (attacks). Such provisions might even risk becoming outdated when techniques used by criminals evolve. The technological neutrality of the general provisions therefore warrants their applicability in the future to this type of crime. Although additional substantive penal provisions are not considered useful or needed, higher sentences for certain offences or types of ransomware attacks are deemed appropriate in some countries.

([4]) 18 replies from EU Member States and two from non-EU countries.
([5]) See table on page 24 for an overview of national legal provisions.

Practically all countries have adequate procedural measures in place that allow the competent authorities to investigate and prosecute ransomware attacks. General **procedural provisions** are applied in investigations. In one country, however, some of these general rules do not allow traffic data information to be requested from service providers, so valuable e-evidence is excluded from the outset. Some countries have monitoring and reporting systems in place, or centralise and coordinate ransomware investigations at national level. In many countries, the procedural measures are found to be sufficient to investigate and prosecute ransomware attacks at national level. Several respondents however indicated that additional legal provisions would be useful or needed for more effective investigations and better and swift e-evidence gathering in ransomware cases. Examples of such additional provisions that would be useful to have (applicable) are provisions on pseudonym and undercover investigations, legal hacking and the takedown of a server. In one country, it is not allowed to monitor data traffic unless there is a suspect. At the same time, it is not possible to monitor data traffic to identify a suspect. The law therefore makes it practically impossible to investigate ransomware cases, as the suspect is usually unknown. When it comes to investigations with a cross-border or international dimension, several respondents indicated that national procedural provisions are not adequate or sufficient.

Except for the reporting requirements that follow from the NIS Directive ([6]), it is not mandatory for individuals or legal entities to **report ransomware attacks** in most countries. In some countries, victims do have a reporting obligation (to a central authority) in the event of personal data breaches. A few countries have a legal obligation in place for the public sector and public administration to report ransomware attacks. In one country, there is a legal obligation for citizens to notify 'perpetrated publicly actionable criminal offences'.

The opinions as to whether mandatory reporting of ransomware attacks would improve cybercrime investigations are divided. Most respondents agreed that mandatory reporting would be useful to get a better picture of the amount and scale of ransomware attacks. With regard to the investigation itself, the obligation to report could also have an accelerating effect, because it would allow law enforcement authorities to become aware of new forms of attacks and types of malware at an early stage. This in turn could speed up the development of IT-countermeasures. However, besides these few positive effects, respondents did not see any other benefits of a reporting obligation.

## National and international approaches to ransomware investigations and experiences

- *National reporting requirements and central points of contact*

Most countries do not have specific reporting requirements for cybercrime in general or ransomware in particular. Some countries do have specific ransomware reporting templates for the police or national guidelines for law enforcement and judicial authorities on the steps to take in the event that a ransomware incident has occurred. In a few countries, websites or platforms are used to register reported ransomware incidents. One of these countries has recently introduced an algorithm for ransomware cases that can indicate the need to coordinate investigations.

Although there are central contact points for cybercrime in most countries at law enforcement and/or judicial level, only a few countries have a specific central contact point for ransomware.

([6]) Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union:
'**Operators of essential services** shall notify incidents having a significant impact on the continuity of the essential service they provide'; and '**digital service providers** shall notify incidents having a substantial impact on the provision of a service that they offer within the Union'.

➢ *Coordination of investigations at national and international level*

In many countries, ransomware cases are dealt with by the local or regional police and prosecution offices where the incident was reported. However, in some of these countries, depending on the severity, scale and international dimension of the attack, authorities can decide to coordinate investigations nationally. In several countries, ransomware investigations are coordinated at national level by national cybercrime units or departments. In one country, the approach to and coordination of ransomware cases has been outlined in a national (binding) guideline for prosecutors. It explains a three-stage approach ([7]) with the aim of avoiding overlap in investigations and ensuring the centralisation of all related cases. Another country is working on the creation of a national Ransomware Task Force, focusing not only on the attribution of ransomware attacks but also on the mitigation of damages, notification of victims and disruption of the criminal model in a broad sense. The task force would take a closer look at the whole chain of initial access, data exfiltration, criminal communication and the financial side. This strategy moves away from an incident-driven attribution approach and focuses on being impactful in a more efficient manner at certain stages of the ransomware kill chain.

Most ransomware cases will require coordination at international level. In a few countries, police and judicial authorities will directly liaise with foreign counterparts. Many countries will involve Interpol, Europol (including the J_CAT) and Eurojust for support. The cross-border coordination of a case at an early stage, including organising coordination meetings and the possible creation of a joint investigation team have already proven to be very effective.

➢ *Challenges and obstacles encountered in ransomware investigations*

The investigation of a ransomware case proceeds similarly to most other cybercrime investigations. Law enforcement and judicial authorities frequently encounter obstacles related to e-evidence gathering and cross-border investigations in such cases.

The loss of data and important e-evidence due to the volatility of the data poses a significant risk. This problem is exacerbated when an incident is not reported (or reported too late) and the data is lost. Sometimes, victims are unwilling to report an incident or to cooperate, due to concerns about reputational damage or the belief that cooperation would not be beneficial and require too much of their time and resources. The preservation of infected disks can also entail significant costs.

Aside from this, the correct securing and handling of the e-evidence is an important factor to ensure the successful continuation of the investigation. In some cases, the initial response to an incident, aimed at re-establishing the infrastructure for business continuity rather than evidence preservation, leads to the loss or alteration of e-evidence.

Another major obstacle in these cases is the criminal use of encryption and anonymisation techniques, which obfuscates the identification of the suspect. As mostly virtual currencies are used for ransom payments, the tracing of these transactions is also complex and difficult.

The international dimension of the crime complicates and often slows down the gathering of e-evidence. Investigations of ransomware cases usually involve multiple jurisdictions, having different legal frameworks and requiring cooperation with foreign law enforcement and judicial authorities. It is highly likely that several countries investigate the same ransomware wave and tackle the same infrastructure. If there is no coordinated approach to the case or it takes too long to start working in such a way, the success of the case will most likely be compromised.

Just as in other cross-border digital investigations, the scattered legal landscape on data retention within the European Union poses problems in ransomware investigations. The lack of a harmonised

([7]) Stage 1: reporting from local police station to district cybercrime prosecutor; stage 2: centralisation of related ransomware reports at national level and coordination between district cybercrime prosecutors; stage 3: centralisation of all ransomware reports to one district prosecutor for international coordination.

legal framework on data retention hampers swift cross-border collection of e-evidence. At the same time, short data retention periods can result in the loss of e-evidence.

Finally, available (specialised) resources and the expertise and skills of law enforcement authorities are also important elements that can influence a case.

➢ *Good practices experienced*

Despite the obstacles encountered in ransomware investigations, several good practices can also be highlighted to maximise the chances for a successful outcome of the investigation.

When a ransomware incident occurs, the creation of a technical report by the victim/affected company is very valuable. A technical report like this is usually drafted by IT experts that have knowledge on how to preserve and handle the e-evidence. The report outlines the technical details of the attack and explains how the attack took place. On the one hand, this facilitates the police's investigations, and on the other hand, it helps the victims to identify vulnerabilities in their computer systems.

The swift notification of a ransomware attack to the relevant authorities, including law enforcement, is an important first step to enable the initiation of an investigation. After that, there should be close cooperation between the victim (and/or their IT support) and the investigators on an ongoing basis.

In the context of ransomware incidents, the cooperation between law enforcement authorities and the private sector, for example, cybersecurity, threat intelligence or incident response companies, is particularly important. These private entities often have a good idea of how the attack was performed and they can secure the victim's data, which can help law enforcement authorities conduct criminal investigations. This public-private cooperation is further elaborated in the next chapter.

Very often, different (inter)national jurisdictions or districts receive reports on attacks with the same type of ransomware. In view of swiftly identifying and investigating such a 'wave' of attacks, the immediate centralisation of the reports and investigations can increase the chances of success. International cooperation and coordination and the creation of joint investigation teams has proven to be essential and has led to the successful identification, arrest and prosecution of cybercriminals. Good experiences in cases where Eurojust and Europol provided support were mentioned in this respect.

Several countries also have reporting templates, checklists, guidelines or handbooks for public authorities on how to deal with ransomware attacks. Some countries have guidelines, platforms or websites for victims where they can file complaints or find useful information on prevention and remediation following an attack, such as contact points for assistance ([8]). In France, a guide for victims includes the following steps to react in the event of a ransomware attack:

- ✓ disconnect the infected machines from the network and the internet;
- ✓ call a computer specialist or IT incident response company;
- ✓ strongly advised not to pay the ransom;
- ✓ open a logbook (technical report) on the incident and preserve the evidence – text of the ransom demand, preservation of the media or machines on which the ransomware was executed (system disk), email addresses and cryptocurrency addresses provided by the cybercriminals, etc.;
- ✓ reinstall the system on a known medium and restore the data from backups made.

Next to these practical tools, continuous information exchange between national cybercrime police departments and prosecutors, and between EJCN members, has proven its added value. Given the complexity of the investigations, specialised training for police and judicial authorities is also beneficial.

([8]) www.cybermalveillance.gouv.fr

## Public-private cooperation in ransomware cases

As already mentioned above, particularly in situations in which ransomware incidents have occurred, private companies (which provide cybersecurity services to victims or are victims themselves) can have a clear picture on how the ransomware attack was executed. They can analyse the affected systems and preserve the data so that the police can access and use it as evidence during the subsequent investigation. Private companies also play a role in proactive threat analysis, disruption of ransomware attacks and other types of victim support and remediation. It is therefore obvious that cooperation between these private entities and public authorities is essential and beneficial for both the investigation and the victim.

- *Victims and public authorities: different interests and priorities*

Good cooperation between victims and law enforcement authorities is not self-evident, given the different interests and priorities at stake. For the victim, the main priorities after a ransomware attack has occurred are damage control and business continuity. The victim or their IT support will aim to have the computer system(s) up-and-running again as soon as possible and regain access to the encrypted data. For these reasons, actions are performed on the computer system and data might be altered or lost. Victims want to minimise the economic and potential reputational damage caused by a ransomware attack, which will sometimes stop them from notifying the police and even bring them to paying the ransom. On the other hand, police and judicial authorities need to have quick access to the relevant data that the victim has from the ransomware attack, to be able to conduct criminal investigations and use the data as admissible evidence.

Despite this potential tension field between victims/private entities and law enforcement and judicial authorities, cooperation is possible, needed and wanted. Below, the legal context for such cooperation is touched upon, followed by a section describing some experiences of cooperation in ransomware cases.

- *National legal contexts for public-private cooperation*

Not many countries have legislation in place that regulates public-private cooperation. In several countries, criminal procedure rules determine that (certain categories of) companies, institutions or organisations are obliged to provide police and judicial authorities assistance and cooperate to facilitate interception, searches of mass data storage devices and remote searches. Companies can also be requested to provide documents, information, access to and copies of documents and data. Several countries apply provisions enabling authorities to cooperate with private entities as an expert or witness. One country referred to specific legislation on public-private cooperation with the financial sector in the fight against terrorism and money laundering. Besides these general procedural law provisions and one reference to specific legislation, there are no specific legal rules established in most countries on public-private cooperation in criminal investigations ([9]).

A few legal obstacles were mentioned in the context of public-private cooperation:

- The secrecy of the investigation limits the amount of information that law enforcement authorities can share with victims and private entities.
- Data protection issues considered by the private companies and the extent to which personal data can/will be shared with the police.
- Broad interpretation by the Data Protection Authority of 'personal data'. As a consequence, although the sharing of information in the course of a criminal investigation is still possible, it is not allowed just for analytical purposes.

([9]) For the purpose of this chapter, legislation implementing Directive (EU) 2016/1148 has not been included.

- Private entities are not authorised to take investigative steps that require a judicial authorisation.
- Data retention issues.
- The lack of a legal framework creates doubt about the legal possibilities for cooperation.

Despite these legal obstacles and the limited existence of legal rules on public-private cooperation, practitioners generally do not consider it necessary to establish specific legislation to ensure or facilitate public-private cooperation.

➢ *Public-private cooperation in ransomware cases: experiences from police and judicial authorities*

The number of cases in which there have been practical experience of public-private cooperation differs within Europe. Some countries have had no or limited experience in this respect. In the countries where such cooperation already exists, law enforcement and judicial authorities are positive about their experiences.

In the context of ransomware incidents, two different stages for cooperation between the police and private entities can be distinguished, before or after an attack takes place. In the former case, if the police is aware that victims/companies have been infected by ransomware, but the attack has not been completed yet, private entities can notify the victims and provide them technical advice and conduct analyses on the infected system. In the event that an attack has occurred, the cooperation with the private entities further entails the securing of evidence from the attack and proper system restoration. For law enforcement and judicial authorities, the swift receipt or access to data on the attack is of utmost importance.

Unfortunately, some challenges are intrinsically linked to public-private cooperation in ransomware cases, because of the different interests and priorities on both sides. According to police and judicial authorities, the following challenges or obstacles could occur:

- Law enforcement authorities are not notified or notified very late about a ransomware attack.
- Victims (individuals or smaller companies) may not have the IT-capabilities required to take immediate, proper actions and secure data.
- While attempting to restore their systems, victims may alter, delete or lose data which is proof of the attack and therefore important for the investigation and evidence collection.
- Lack of interest, time and resources from the side of the victim to cooperate with the police on a long-term basis. Aside from this, because of the secrecy of the criminal investigation, public authorities cannot share much information on the case with the victim. For these reasons, the interest and willingness of the victim to cooperate with the police decrease over time.
- Reluctance of the private sector to share (confidential) information because of commercial or intellectual property considerations or potential reputational damage.
- If the victim shares information with the police on a confidential basis, it is sometimes not possible to disrupt a ransomware attack, using special investigation techniques such as wiretapping, as these would reveal the source of the information.
- Existing prejudices on the side of the authorities regarding the incorrect handling of data by the victim or private entity. The same on the side of the victims regarding the handling of confidential information and impact of the involvement of the police. These prejudices have a negative effect on public-private cooperation.

Despite the potential occurrence of these challenges, good practices yielding fruitful cooperation have also been observed. Several examples of such good practices, including points of attention, were mentioned:

- Swift notification of ransomware incidents to the police, enabling their involvement from an early stage.
- Use of specific forms to share information.
- Disconnection of the affected machines from the network and the internet.
- Creation of a technical report or logbook and preservation of the evidence of the ransomware attack, such as log files, malware samples, email addresses, communication from the perpetrators and system disks.
- Early involvement on both sides of specialised and trained IT experts and police officers.
- Continuous contact between the authorities and the victim/technical team.
- Reducing prejudices on both sides and building trust. Within the given limits, cooperation should work both ways. If private entities share information with law enforcement and judicial authorities, they may have reasonable expectations to receive possible updates on how this information is used and if it leads to any results outside the specific investigation (such as threat analysis, public statistics and the sharing of information with foreign police).

## Conclusion

Investigations into ransomware attacks are very difficult by nature. The international dimension of investigations and complexity of identifying criminals require early and close cross-border cooperation and coordination between law enforcement and judicial authorities. Aside from this, victims and private companies also play an essential role, as they can swiftly notify authorities of ransomware incidents and can preserve and provide the (digital) data and evidence that the police need to investigate the crime and identify criminals. Public-private cooperation is therefore particularly important and valuable in ransomware cases. Although most countries do not have a particular legal framework for such cooperation, experience has shown that such cooperation is much needed, and has enabled significant progress in investigations. Hence, the further strengthening of public-private cooperation is the key to confronting ransomware attacks and having successful investigations.

| COUNTRY | LEGAL PROVISIONS OF THE CRIMINAL CODE |
|---|---|
| **Austria** | §118a: unlawful use of a computer system<br>§126a: damage to electronic data<br>§126b: disrupting the operation of a computer system<br>§126c: misuse of a computer system or access data<br>§144: extortion |
| **Bulgaria** | Article 319b: unlawful interference with data in an information system |
| **Germany** | §253: extortion<br>§202a: data espionage<br>§303a: data manipulation<br>§303b: computer sabotage |
| **Denmark** | §193 Criminal Code: disruption of critical data systems<br>§263: unauthorised access to IT systems<br>§281: blackmailing<br>§291: vandalism<br>§293: utility theft |
| **Greece** | Extortion provisions<br>Art. 79: payment following an offence as aggravating circumstance |
| **Spain** | Article 264: unauthorised alteration of computer program and/or data<br>Article 264 bis: unlawful hindering the operation of a computer system |
| **Finland** | Chapter 31: robbery and extortion |
| **France** | Art. 323-1: fraudulent access to an automated data processing system<br>Art. 323-2: obstruction to the functioning of an automated data processing system<br>Art. 312-1: extortion<br>Art. 323-3-1: possession or transfer of malware |
| **Italy** | Art. 629: extortion<br>Art. 615ter: unauthorised access to a computer or telecommunication system<br>Art. 635bis: damaging a computer of telecommunication system<br>Art. 615quinquies: distribution of equipment, devices or computer programs intended to damage or disrupt a computer or telecommunication system |
| **Lithuania** | Art. 196: Unlawful Influence on Electronic Data<br>Art. 197: Unlawful Influence on an Information System<br>Art. 198: unlawful Interception and Use of Electronic Data<br>Art. 198-1: unlawful connection to an information system<br>Art. 198-2: unlawful Disposal of Installations, Software, Passwords, Login Codes and Other Data |
| **Luxembourg** | Art. 509-3: unauthorised interference with automated system<br>Art. 509-4: transfer of monetary value/payment following offence of art. 509-3 |
| **Latvia** | Section 177: fraud in an automated data processing system<br>Section 241: arbitrary accessing of automated data processing system<br>Section 243: interference in the operation of automated data processing system and illegal actions with the information included in such system<br>Section 244: illegal operations with automated data processing system resource influencing devices |

| | |
|---|---|
| **Netherlands** | Art. 138ab: computer intrusion<br>Art. 138c: copying non-public data<br>Art. 139d (2): creating, selling, spreading or possessing malware<br>Art. 350a: making data inaccessible<br>Art. 350d: possessing equipment with which data can be made inaccessible<br>Art. 317, section 2: extortion by threatening to make unusable, inaccessible or delete data stored by means of an automated work<br>Art. 318: extortion by threating to disclose a secret |
| **Portugal** | Art. 5 Cybercrime Law: computer sabotage/system interference |
| **Romania** | Art. 360: illegal access to a computer system<br>Art. 362: altering computer data integrity<br>Art. 363: disruption of the operation of computer systems<br>Art. 364: unauthorised transfer of computer data<br>Art. 365: illegal operations with devices or software<br>Art. 207: blackmail |
| **Sweden** | Chapter 4, Section 9c: unlawful access to and interference with automated information system |
| **Slovenia** | Art. 108: terrorism<br>Art. 221: attack on information systems<br>Art. 237: misuse of information systems<br>Art. 213: extortion and blackmail |
| **Slovakia** | Section 247a: unlawful intervention into a computer system<br>Section 247b: unlawful interference with computer data<br>Section 189: blackmail |
| **Norway** | Section 204: intrusion into a computer system<br>Section 205: violation of the right to private communication<br>Section 206: risk of operational disruption of a computer system<br>Section 330-331: extortion/aggravated extortion<br>Section 332-333: receiving proceeds from crime/aggravated receiving proceeds from crime<br>Section 351-352: vandalism/aggravated vandalism |
| **Switzerland** | Art. 143bis: unauthorised access to a data processing system<br>Art. 144bis: damage to data<br>Art. 156: extortion<br>Art. 143: Unauthorised obtaining of data<br>Art. 179novies: Obtaining personal data without authorisation |

# 6. Way ahead

The *Cybercrime Judicial Monitor* is produced once per year and 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 remain on legislative developments in the area of cybercrime and e-evidence and the analysis of relevant court decisions. The topic of interest will be determined based on ongoing or emerging trends.

The CJM is 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 edition of the CJM.

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

*Catalogue number:* QP-AG-22-001-EN-N • *ISBN*: 978-92-9490-770-7 • *ISSN*: 2600-0113 • *DOI*: 10.2812/81111