Cybercrime Judicial Monitor

Issue 6 – May 2021

Criminal justice across borders

Contents

1. Executive summary

The European Union Agency for Criminal Justice Cooperation (Eurojust) presents this sixth 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.

Like previous issues of the CJM, this issue contains four main sections. The first section covers legislative developments in the area of cybercrime, cyber-enabled crime and electronic evidence, or e-evidence, in 2020.

The judicial analysis section presents legal analyses of rulings rendered by courts in Member States and non-EU countries and by European courts. The courts ruled on various cyber-related matters, such as repeal of new provisions on the monitoring of encrypted messages (Austria); access to encrypted data by law enforcement authorities and the *nemo tenetur* principle (Belgium); money laundering via a cryptocurrency-exchange platform of proceeds of the Locky ransomware (France); and the search and seizure of a mobile phone containing communications pertaining to legal professional privilege (LPP) (the European Court of Human Rights). Several other national court rulings are also briefly summarised.

The next section covers developments in the European Union during the past year in relation to data retention. An overview is provided of recent national legislative and case-law developments.

Given the landmark rulings of the Court of Justice of the European Union (CJEU) of October 2020 and the seemingly increasing calls from many Member States for a harmonised legal framework at EU level on data retention, the topic of interest in this issue of the CJM provides an overview of all the main CJEU rulings so far in relation to data retention for the purpose of criminal investigations and prosecutions. Each of the six rulings is presented, including the questions referred to the CJEU for a preliminary ruling and the court's decision.

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 2020. The main sources of national information presented in this section are contributions collected through the European Judicial Cybercrime Network.

2.1. EU level

- *EU Security Union Strategy*

On 24 July 2020, the European Commission issued the EU Security Union Strategy. This Strategy covers 2020–2025 and sets out a whole-of-society approach to security that can effectively respond to a rapidly changing threat landscape in a coordinated manner. It defines strategic priorities and the corresponding actions to address digital and physical risks in an integrated manner across the EU. The tackling of evolving threats is one of these strategic priorities. This priority covers the areas of cybercrime, modern law enforcement and countering illegal content online.

Cybercrime. As cybercrime continues to rise, the Commission underlines the need to have good strategic communication across the EU, to alert Member States to risks and advise on preventive measures. The Commission will explore the feasibility of an EU cybercrime-related rapid alert system for this purpose. Alongside this, effective international cooperation is necessary. In this context, the EU supports the Council of Europe's Budapest Convention on Cybercrime, which can help in identifying ways for countries to work effectively together. Furthermore, data misuse and identity theft are major concerns. The Commission will explore possible practical measures to protect victims against all forms of identity theft. New technological developments, such as artificial intelligence, that are being exploited by criminals will also be followed closely, in order to be able to tackle cybercrime effectively.

Modern law enforcement. Technological developments and emerging threats also require law enforcement authorities to have access to new tools, acquire new skills and develop alternative investigative techniques. Law enforcement authorities need to be able to identify, secure and read the data needed to investigate crimes and to use those data as evidence in court. The Commission will therefore explore measures to enhance law enforcement capacity in digital investigations, including new tools and training for both law enforcement authorities and the judiciary. The importance of cross-border access to e-evidence is also highlighted. In this regard, the Strategy underlines that swift adoption of the e-evidence proposals is key to provide practitioners with an efficient tool. Establishing compatible rules at international level, through international negotiations, is also essential in this respect. Access to digital evidence also depends on the availability of information. The Commission will therefore assess the way forward on data retention and access to internet domain name registration information (WHOIS data). Furthermore, the Commission will explore and support balanced technical, operational and legal solutions to the challenges posed by encryption and promote an approach that both maintains the effectiveness of encryption in protecting privacy and security of communications and provides an effective response to crime and terrorism.

Countering illegal content online. Concrete actions are needed to counter illegal content online, including content relating to child sexual abuse. The Commission has issued a specific new Strategy to step up the fight against child sexual abuse online (see below).

Access the full text of the Security Union Strategy.

➢ *EU Strategy for a more effective fight against child sexual abuse*

Child sexual abuse is a particularly serious crime. Unfortunately, there are indications that the coronavirus disease 2019 (COVID-19) pandemic has worsened the problem. The fight against child sexual abuse is a priority for the EU.

On 24 July 2020, alongside the EU Security Union Strategy, the Commission issued the EU Strategy for a more effective fight against child sexual abuse. This Strategy includes eight initiatives to implement and develop a strong legal framework for the protection of children, strengthen law enforcement response and facilitate a coordinated approach across the many actors involved in protecting and supporting children.

The eight initiatives aim to:

- ensure complete implementation of the current rules (particularly Directive 2011/93/EU on combating sexual abuse and exploitation of children);
- ensure that EU laws enable an effective response;
- identify legislative gaps, best practices and priority actions;
- strengthen law enforcement efforts at national and EU levels;
- enable EU countries to better protect children through prevention;
- establish a European centre to prevent and counter child sexual abuse;
- galvanise industry efforts to ensure the protection of children in their products;
- improve protection of children globally through multistakeholder cooperation.

The Commission will propose new legislation where needed, particularly to clarify the role that online service providers can play in protecting children. In 2020, the Commission proposed an interim regulation to ensure that providers of online communications services can continue their voluntary practices to detect and report child sexual abuse online and remove child sexual abuse material.

The roles of the European Union Agency for Law Enforcement Cooperation (Europol) and Eurojust are underlined several times in the Strategy, given that child sexual abuse cases, often involving digital materials, are rarely limited to one Member State and require a coordinated approach.

Access the full text of the EU Strategy for a more effective fight against child sexual abuse.

➢ *Council Resolution on Encryption – Security through encryption and security despite encryption*

On 24 November 2020, the Council of the European Union adopted a Resolution on encryption, highlighting the need for strong encryption technology, protecting fundamental rights and digital security, while at the same time ensuring that competent authorities can exercise their powers to protect societies and citizens.

The Council acknowledges that encryption nowadays is increasingly used in all areas of public and private life, and that all parties benefit from the technology. At the same time, criminals are also misusing encryption for their illegal activities. Consequently, it has become more and more difficult for law enforcement and judicial authorities to access electronic evidence to investigate and prosecute serious crimes. The Council therefore finds it essential to preserve the powers of competent authorities through lawful access to such evidence. In doing so, the right balance needs to be struck between the fundamental rights protected by strong encryption and the rule of law. To this end, the Council emphasises that the European Union should strive to establish an active discussion with the technology industry, bringing in research and academia.

In its Resolution, the Council also mentions that the need for a regulatory framework on encryption across the EU could be further assessed. Potential technical solutions should be developed and the operational and technical skills and expertise of competent authorities continually improved.

Finally, the Council also states that it is of paramount importance to improve coordination at EU level, with the aim of combining the efforts of Member States and EU institutions and bodies, defining and establishing innovative approaches in view of new technologies, analysing technical and operational solutions, and providing tailored training. Technical and operational solutions anchored in a regulatory framework should be developed in close consultation with private industry, relevant stakeholders and competent authorities.

Access the full text of the Council Resolution on encryption.

2.2. Member States

Bulgaria

- *Amendments to the cybercrime chapter of the Criminal Code*

A proposal for amendments and supplements to the cybercrime chapter of the Bulgarian Criminal Code has been drafted. It envisages an overall increase in imprisonment sanctions for cybercrime and provides for full transposition of Directive 2013/40/EU on attacks against information systems. The draft bill is currently under review by the National Assembly.

Germany

- *Draft Bill on criminal liability for operating criminal trading platforms*

On 27 November 2020, the German Federal Ministry of Justice launched a draft bill to amend the provision on the offence of criminal liability for operating criminal trading platforms in the German Criminal Code. The exchange of goods and services has been greatly simplified by the internet. Narcotics, weapons, child pornography, counterfeit money, forged ID cards, stolen credit cards: almost anything can be bought online. So far, law enforcement authorities in Germany have not had the opportunity to counter this phenomenon effectively and consistently in all criminal areas, although there are special legal prohibitions on the sale of certain goods (especially drugs and weapons), and anyone who helps another person with such trafficking can be prosecuted. However, if a platform is operated fully automatically, prosecution is not always possible. Therefore, the German Federal Ministry of Justice saw a need to supplement criminal law regulations.

The draft bill provides for a new criminal offence of operating a criminal trading platform on the internet to be added to the German Criminal Code. Only platforms that are especially designed to promote the commission of certain criminal offences are subject to the new provision. The offence will be punishable by imprisonment for up to 5 years or a fine, or, in the case of commercial activity, by imprisonment for between 6 months and 10 years. The draft Bill also provides for effective investigative measures to investigate these crimes. The catalogue of criminal offences in those sections of the German Code of Criminal Procedure that rule on interception measures should therefore be updated to cover the operation of criminal trading platforms in a commercial manner.

The legislative process on this matter is ongoing.

Ireland

➢ *Harassment, Harmful Communications and Related Offences Act 2020*

The Harassment, Harmful Communications and Related Offences Act 2020 makes it a crime for intimate images to be published on the internet without consent.

Distributing, publishing or threatening to distribute or publish an intimate image of another person, without that other person's consent, and with intent to cause harm to, or recklessness as to whether or not harm is caused to, the other person, is an offence. The maximum penalty is 7 years of imprisonment.

The definition of 'intimate image', in relation to a person means any visual representation (including any accompanying sound or document) made by any means including any photographic, film, video or digital representation:

(a) of what is, or purports to be the person's genitals, buttocks or anal region and, in the case of a female, her breasts;

(b) of the underwear covering the person's genitals, buttocks or anal region and, in the case of a female, her breasts;

(c) in which the person is nude; or

(d) in which the person is engaged in sexual activity.

Access the full text of the Act.

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

Ireland has passed a new money-laundering Act, which states that a virtual currency provider is considered a financial institution and is obliged to register with the Central Bank of Ireland's Financial Regulator. The Act also incorporates definitions in domestic law of 'virtual currency wallets', etc.

Italy

➢ *Law No 7/2020, amending provisions on interception of conversations and communications*

Law No 7/2020, of 28 February 2020, provides for urgent modifications to provisions on interceptions of conversations and communications in the Italian Criminal Procedure Code. The Law provides that the use of Trojan software to carry out interceptions of communications between persons present is always permitted, not only in relation to the offences referred to in Article 51, paragraph 3bis and 3quater, of the Criminal Procedure Code but also in relation to crimes committed by public officials and public service officers against the public administration, for which the same maximum penalty of imprisonment for at least 5 years is imposed. This provision applies only to investigations initiated after 30 April 2020.

Law No 7/2020 clearly states that evidence resulting from wiretapping using Trojan software may not be used in proceedings other than those for which they have been ordered. The only exception is if the evidence is relevant and indispensable for the investigation of crimes for which an arrest in flagrante delicto is compulsory or for crimes referred to in Article 266, paragraph 1, of the Criminal Procedure Code.

Access the full text of Law No 7/2020 in the Gazzetta Ufficiale.

Poland

- *Higher maximum penalty for identity theft*

In 2020 in Poland, the maximum penalty for the crime of stalking and identity theft was raised from 3 years' imprisonment to 8 years' imprisonment.

Article 190a of the Polish Criminal Code now stipulates that anyone who, through the persistent harassment of another person or another person's next of kin, creates a justified sense of danger or significantly violates the person's privacy is subject to imprisonment for between 6 months and 8 years. Anyone who pretends to be another person and uses his or her image or other personal data, or other data by which he or she can be publicly identified, in order to cause property or personal damage is liable to the same penalty.

Slovakia

- *Additional criminal provisions on (seizure of) virtual currency*

Legislative changes have been adopted in both the Criminal Code and the Code of Criminal Procedure in order to implement, among other provisions, those of 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.

The changes include minor additions to the substantive legal provisions dealing with cybercrime. A definition of 'virtual currencies' was introduced, as well as a specific provision on seizure of virtual currency.

Sweden

- *Law on secret data reading*

On 1 April 2020, a new law regarding secret data reading entered into force in Sweden. A court can authorise secret data reading, which means that data intended for automated processing is secretly, and with a technical aid, read by or recorded in a readable information system.

Secret data reading can be used only in investigations regarding serious crime and under certain safeguards specified in the law. The law is valid for 5 years and will then be reviewed.

Access the full text of the Law in Swedish.

2.3. Non-EU countries

Switzerland

- *Revision of the Ordinance on Internet Domains*

On 18 November 2020, the Federal Council adopted a revision of the Ordinance on Internet Domains (OID), which entered into force on 1 January 2021. The OID is the legal basis for the distribution and management of domain names ending in .ch and .swiss. The revision offers greater protection of personal data and helps to more effectively combat cybercrime.

The revised OID no longer requires that personal data and information on domain holders and domain names be published (through the WHOIS service). The Swiss registry handling the administration of domain names that end in .ch (SWITCH) can be requested to provide information on such personal data

in justified cases. Moreover, the registry will now also provide access to the zone file. The zone file includes a list of all .ch domain names, with information about the relevant name server that can be actively used on the internet for websites and emails. The zone file is updated hourly and can be valuable in enabling law enforcement authorities to fight cybercrime faster and more effectively.

More information can be found on the SWITCH website.

Access the full text of the OID in different languages.

3. Judicial analysis

The objective of this analytical chapter is to provide insights into cybercrime judgments rendered in the EU and at international level. It is intended 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 the issues and arguments addressed by the courts.

This chapter constitutes the main portion of the CJM, as it has been created to meet demand from practitioners for a regular overview of court rulings in other countries, so that courts' motivations and justifications regarding the evidence trail could also possibly be used in other countries in cybercrime cases. The judgments analysed have been selected from the court decisions sent to Eurojust on a voluntary basis by practitioners in the Member States and non-EU countries.

3.1. Selected court rulings

Procedure: Constitutional Court, G 72/2019 (72-74/2019-48, G 181-182/2019-18), Austria

Date: 11 December 2019

Keywords: new provisions introducing measure to monitor encrypted messages repealed

Introduction

On 11 December 2019, the Austrian Constitutional Court repealed new provisions that would have introduced a new investigative measure for the monitoring of encrypted messages into the Austrian Code of Criminal Procedure. The provisions on this new investigative measure would have come into force on 1 April 2020, but they were repealed before this date.

The Constitutional Court argued that the provisions were incompatible with Article 8 of the European Convention on Human Rights (ECHR). The court considered that the planned investigative measure constituted serious interference with Article 8 of the ECHR, given the range of computer systems and the amount of personal data available on them. In particular, the scope of the measure played a role, as in the opinion of the Constitutional Court it was significantly broader than in the case of previous secret measures. The measure would make it possible to draw comprehensive conclusions about a person's private life. According to the Constitutional Court, such a serious encroachment on the private sphere, protected under Article 8 of the ECHR, would require serious public interest to justify it and could be permitted only within extremely narrow limits for the protection of correspondingly serious legal interests.

Main considerations of the Constitutional Court

1. The requirements under which the investigative measure would be allowed were too low (namely in cases relating to § 135a, paragraph 1, subparagraphs 2 and 3, in the Austrian Code of Criminal Procedure). For instance, the mere suspicion of an intentional act punishable with imprisonment of more than 6 months, and one communication partner consenting to the surveillance, would have sufficed. Consent by one communication partner, however, cannot justify the intrusion into the privacy of the communication partner who has not consented. Furthermore, in cases in which the measure would be applied as a preventive measure, even mere qualified property offences would have fallen within the scope of the measure.

2. Furthermore, the protection of the private sphere (Article 8 of the ECHR) of other affected persons was not sufficiently ensured. The requirement that the measure be ordered by the public prosecutor's office and approved by a court did not constitute sufficient control. Nor was the planned additional supervision by the judicial commissioner for legal protection sufficient. Owing to the seriousness of the encroachment on fundamental rights, the Constitutional Court stated that effective independent supervision (by a court or a body with an equivalent guarantee of independence) of the ongoing implementation of the investigative measure would be a necessary requirement for it to be in conformity with the Constitution.

3. Finally, authorisation for the measure under § 135a, paragraph 3, of the Code of Criminal Procedure, in accordance with which secret intrusion into apartments and other places would have been permitted for the installation of software, was found to violate Article 9 of the Constitution in conjunction with the law on the protection of the sanctity of the home (Hausrechtsgesetz 1862). Hausrechtsgesetz 1862 requires notification within 24 hours after a search has been completed. This notification would not be given, however, as it would be incompatible with the purpose of the secret investigation measure.

Court decision

§ 134 Z3a and § 135a of the Code of Criminal Procedure as amended by Federal Law No 27/2018 were repealed as unconstitutional.

Procedure: Court of Cassation, No P.19.1086.N, Belgium

Date: 4 February 2020

Keywords: order to provide access code for mobile phone, *nemo tenetur* principle

Introduction

On 15 October 2019, the Court of Appeal of Ghent acquitted a person who refused to comply with the order of the investigating judge to provide the access codes for the mobile phones in his possession. The court reasoned that such an obligation was irreconcilable with the right to remain silent and the prohibition of forced self-incrimination.

The appeal in cassation was directed against the judgment of the Court of Appeal of Ghent. The Court of Cassation considered the elements below.

Reasoning of the court

Article 88*quater*, § 1, of the Belgian Criminal Procedure Code stipulates that the investigating judge may order any person whom he or she suspects to have special knowledge of an information system to provide information on its operation and on how to access it, or to gain access in an intelligible form to the data stored, processed or transmitted through it. Punishment is specified in § 3 for any person who does not cooperate.

The court stated that Article 6.2 of the ECHR, Article 14.2 (presumption of innocence) and Article 14.3 (no self-incrimination) of the International Covenant on Civil and Political Rights, and Articles 6 and 7 of Directive (EU) 2016/343 and its recitals 24–29 did not exclude the criminalisation and punishment of a suspect on the basis of Article 88*quater* § 1 and § 3.

In making this assessment, the court took into account, among others, the following reasons.

- The right not to incriminate oneself and the presumption of innocence are not absolute and need to be considered against other rights, such as the right to freedom and security (Article 5 of the ECHR) and the prohibition of abuse of law (Article 17 of the ECHR).
- The right not to incriminate oneself primarily aims to safeguard the right to a fair trial by excluding false statements made under pressure.
- The access code for a computer system exists independently of the will of the person who has knowledge of that code. The code remains unchanged regardless of its communication and can be checked immediately. There is no risk of unreliable evidence.
- The access code is neutral information and can be distinguished from any possible incriminating data that might be found on the computer system.
- The current state of technology makes it very difficult, if not impossible, to gain access to a computer system protected by an encryption application, and such applications are widely available. Consequently, the information requested is necessary for the purpose of determining the truth.
- Following the abovementioned reasoning, the court concluded that the Court of Appeal of Ghent's judgment had not justified its decision as a matter of law.

Court decision

The Court of Cassation annulled the appeal judgment and referred the case to the Court of Appeal of Antwerp.

Procedure: Constitutional Court, No 28/2020, Belgium

Date: 20 February 2020

Keywords: encryption, obligation to provide information and request to cooperate, *nemo tenetur*

Introduction

On 11 January 2018, the Court of First Instance of Antwerp acquitted a person of a violation of Article 88*quater*, § 1 and § 3, of the Code of Criminal Procedure. The public prosecutor appealed the decision. The defendant alleged infringement of several legal norms, including the principle of *nemo tenetur*, the principle of non-incrimination and the presumption of innocence. In December 2018, the Court of Appeal subsequently referred a question for a preliminary ruling to the Constitutional Court:

Does Article 88quater, §1 and §3, of the Code of Criminal Procedure violate Articles 10, 11 and 22 of the Constitution, read in conjunction with Articles 6 and 8 of the ECHR, by providing for criminal penalties for the ***obligation to provide information****, as laid down in Article 88quater, §1, of the Code of Criminal Procedure, also with regard to the defendant, whereas the same defendant cannot be penalised if he does not provide the* ***requested cooperation*** *in the search of an information system as referred to in Article 88quater, §2, of the Code of Criminal Procedure?*

Reasoning of the court

The court took into account a memorandum submitted by the Council of Ministers. According to the Council of Ministers, the provision aims to effectively respond to technological developments relating to computer systems. Without legal instruments that allow access to computer systems and the involvement of third-party experts in examining those computer systems, it is impossible for the police to take adequate and effective action against persons who commit crimes by means of, or with the help of, computer systems. Furthermore, the Council of Ministers argued, the existence and the presence of digital evidence are independent of whether the accused could incriminate himself. There is no obligation on the accused to actively disclose where the relevant information is located. The provision is also considered proportionate, given the international awareness of the pressing need to update provisions in this regard in criminal law.

The court made the following assessment.

- Indeed, judicial authorities need to be equipped with adequate legal instruments to fight crimes committed through the use of computer systems. Article 88*quater* includes some exceptional cooperation obligations, without which it could become impossible to conduct effective investigations. In view of their enforceability, non-compliance or hindering the investigation has been made punishable.
- In Article 88*quater*, § 1, the accused is asked to **provide information** allowing access to a certain computer system, insofar as this information exists independently of his will, so that the right not to collaborate in his own accusation does not apply, whereas in Article 88*quater*, § 2, he is asked to actively **participate in the operations** carried out on the computer system, that is, to actively participate in the collection of evidence of the crime, which could lead him to collaborate in his own accusation. This is a clear difference, and therefore the difference in treatment is reasonable.

The court concluded that the preliminary question must be answered negatively.

Court decision

The court pronounced that Article 88*quater*, § 1 and § 3, of the Code of Criminal Procedure did not infringe Articles 10, 11 and 22 of the Belgian Constitution read in conjunction with Articles 6 and 8 of the ECHR.

Procedure: Correctional Court of Paris, France

Date: 7 December 2020

Keywords: Locky ransomware, aggravated money laundering via cryptocurrency exchange platform

Introduction and background

At the beginning of 2016, a massive cyberattack carried out with the help of a malicious program, the ransomware Locky, took place throughout France against both private and legal persons, and public institutions. The malware, which was installed without the victims' knowledge when they opened an attachment sent to their email inboxes, proceeded to encrypt their data through the encryption of their personal and professional documents. The computer system was paralysed, and the victims were asked to pay a ransom in cryptocurrency in exchange for the restoration of their data using a personal decryption key.

The technical investigations carried out by the French investigators, into the payment of ransoms and the tracing of bitcoins paid by the various victims, made it possible to identify the Russian cryptocurrency exchange platform BTC-e.com as an apparently pivotal element in the laundering of ransoms. Created in 2011, this platform had been used by some 700 000 customers and the sums having passed through it were estimated at 9.4 million bitcoins. More than 200 French victims of the Locky malware were counted. Bitcoin blockchain analysis made it possible to identify 5 700 victims, at the international level, of the Locky ransomware.

At the same time, it appeared that an indictment had been issued in January 2017 by a court in San Francisco against BTC-e and a defendant who was identified as the co-founder and one of the administrators of the BTC-e.com platform, possessing several administrator accounts on the platform. The US Federal Bureau of Investigation closed down the BTC-e site and seized the servers. Present on Greek territory, the defendant was arrested by the Greek authorities on 25 July 2017 at the request of the US authorities, on suspicion of laundering income from illegal activities through BTC-e. The defendant denied the charges. Numerous requests for international assistance were made by different countries, and arrest warrants were issued by the United States and Russia. The defendant was handed over to the French authorities in January 2020.

Charges

The defendant was prosecuted for organised money laundering and criminal association, as well as computer-related offences against individuals and legal entities and against the state, in the latter case with the aggravating circumstance of participation in organised crime. He was also prosecuted for extortion offences, the proceeds of which had allegedly been introduced into an organised money-laundering scheme.

Evidence and reasoning of the court

1. The material and intentional elements of the offences of access, fraudulent maintenance, fraudulent introduction and modification of data, and interference with an automated data-processing system were sufficiently established.

The court found, however, that it did not appear from an examination of the facts and the evidence that the accused had performed positive acts in the commission of the abovementioned offences and that he belonged to a group of persons who had prepared and disseminated the Locky virus in order to gain access to, and then undermine, the computers. Neither did it even appear that he was an affiliate who, without having conceived the Locky virus, disseminated it. For these reasons, the court discharged the defendant from these counts of the prosecution's charges.

2. Technical investigations, including blockchain analysis, showed that the virus attack had been planned and carried out with the aim of extorting money from the victims.

The court found that there was no evidence against the defendant that he had coerced the victims to pay a ransom, that he had conceived and introduced the ransom demands into the infected systems or that the fraudulent cryptocurrency wallet used to receive payments belonged to him. The court accordingly acquitted the defendant of these charges.

3. The investigation had not established that the defendant belonged to a group of persons who had committed preparatory acts prior to the commission of these offences. Therefore, the court acquitted the defendant of this charge.

4. As regards the money-laundering offences, there was evidence of the extortion of 22 victims of the cyberattack who had paid bitcoins in order to obtain computer codes to restore their systems.

Blockchain analysis showed that the BTC-e platform appeared to be a pivotal element in the laundering of the proceeds of extortion. Investigation of a wallet showed that it had received numerous bitcoins for

amounts identical to those requested from the French Locky victims, suggesting, by extrapolation, that they all originated from the extortion of funds associated with this viral attack. As to the platform itself, it appeared that it generated one address per transaction, which had the effect of making transfers more opaque and anonymous. The platform worked as an exchanger that, using vouchers, converted bitcoins into cash, which then exited the blockchain without leaving a trace. The court concluded that it was clear from these findings that the BTC-e platform was a discrete money-laundering medium.

Furthermore, investigations of the accounts showed that they had been used to launder the ransoms from the Locky malware attack. The choice of cryptocurrency to conceal the fraudulent origin of the funds, the use of the BTC-e platform to create vouchers, the conversion of bitcoins into fiduciary currency, the transfer from one account to another and then the exit of the sums by means of payment cards demonstrated money-laundering activity. The evidence also pointed to the defendant's connection with certain accounts. Given the evidence on the platform's administrators, it was clear that he had had a central role in managing the accounts used for laundering. One account managed by the defendant had received 76 % of the money extorted by means of the Locky ransomware. This value, expressed as a percentage of the proceeds of the offence, although it did not demonstrate that he was the creator of the Locky ransomware and the instigator of the extortion, showed the major role he had played in the money-laundering operations. Evidence from the telephone and computer of the defendant showed that he wanted to keep a close eye on the money-laundering operations and that he could not have been unaware of the fraudulent origin of the sums he converted and hid on the BTC-e platform.

The analysis of the elements of the case led to the conclusion an organised group had been formed to commit the laundering of funds extorted from the victims of the Locky malware.

The court stated that the defendant had committed money laundering by assisting in an operation of investment, concealment and conversion that had used the BTC-e platform that he controlled to conceal the funds extorted from the victims of the Locky ransomware and by reinjecting some of the funds anonymously into the financial system.

Court decision

The court found the defendant guilty of aggravated money laundering as part of an organised group. He was sentenced to 5 years' imprisonment and a fine of EUR 100 000.

Procedure: European Court of Human Rights, *Saber v. Norway*, case 459/18

Date: 17 December 2020

Keywords: search and seizure of mobile phone, data protection, legal professional privilege, legal framework and safeguards insufficient

Introduction

The European Court of Human Rights convicted Norway of a violation of Article 8 of the ECHR arising from an insufficient legal framework and safeguards for protecting data subject to LPP, during police search and seizure of a smartphone.

Facts

The applicant was a possible victim of an alleged crime. As part of the criminal investigation, the police seized the applicant's smartphone and captured a mirror image copy of it, which they wished to search.

The phone contained correspondence between the applicant and his lawyers, meaning that some of the content was subject to LPP and therefore exempt from the search under domestic law.

Through applying domestic law provisions on search and seizure by analogy, there was initial agreement that the data on the mirror image copy had to be sifted through by the city court and any LPP data removed before the police could search the remainder of the material. However, in a subsequent decision of the Supreme Court, which did not involve the applicant, it was determined that procedures relating to surveillance data were applicable instead. In the light of that decision, the city court abandoned its filtering procedure and sent the mirror image copy back to the police, who examined the data.

Reasoning of the court

The search of the applicant's smartphone and/or the mirror image copy of it had entailed an interference with his right to respect for his correspondence (Article 8 of the ECHR). Moreover, the search had been carried out in the context of the applicant being the aggrieved party in the pertinent investigation.

While the interference had a formal basis in law, the court had to determine whether the law was 'compatible with the rule of law', namely whether it was sufficiently foreseeable. The court made three observations in this regard.

1. The proceedings relating to the filtering of LPP data in cases such as this had lacked a clear basis in the Code of Criminal Procedure right from the outset, which had rendered them liable to such disputes.

2. The actual form of the proceedings could hardly have been foreseeable to the applicant, given that they had effectively been reorganised following the decision of the Supreme Court.

3. Most importantly, subsequent to the Supreme Court's decision, no clear and specific procedural guarantees had been in place to prevent LPP data from being compromised by the search of the mirror image copy of the applicant's phone. The Supreme Court had not given any instructions on how the police were to carry out the task of filtering LPP data, apart from indicating that search words should be decided upon in consultation with counsel; even though the claim lodged for LPP in this case had been undisputedly valid, the mirror image copy had effectively just been returned to the police for examination without any practical procedural scheme in place for the purpose of filtering the data. A report by the police had described the deletion of data in the applicant's case, but it had not described any clear basis or form for the procedure.

There had indeed been procedural safeguards in place relating to searches and seizures in general; however, the court's concern was the lack of an established framework for the protection of LPP in cases such as this. In its decision, the Supreme Court had also pointed to the lack of provisions suited to situations in which LPP data formed part of breaches of digitally stored data and had indicated that it would be natural to regulate the exact issue that had arisen in this case by way of formal provisions of law. The issue that arose in this case had not as such been owing to the Supreme Court's findings; rather, it had originated from the lack of appropriate regulations.

The court had no basis to decide on whether or not LPP had actually been compromised in his case. Nor was it necessary to consider whether or under what circumstances credible claims for LPP in respect of specific data carriers entailed that they must be sent to a court or another third party independent of the police and prosecution in order to have any data covered by LPP deleted before the police and prosecution could proceed to search the data carrier. Instead, the lack of foreseeability in the this case due to the lack of clarity in the legal framework and the lack of procedural guarantees relating specifically to the protection of LPP had already fallen short of the requirements flowing from the criterion that such interference must be in accordance with the law.

Court decision

The court held that there has been a violation of Article 8 of the ECHR.

The legal summary and the full judgment can be found on the European Court of Human Rights website.

Note: as a result of this conviction, a working group has been established in Norway to draw up necessary amendments and propose new legal provisions. This work has just recently started.

3.2. Other court rulings in brief

- **District Court of Bad Kreuznach, 2 KLs 5 Js 226/17, Germany**

  Date: 4 April 2020

In March 2016, a 34-year-old person, together with others, founded the internet platform Fraudsters, accessible via changing domains and the darknet. He operated the forum as an administrator until it was shut down on 9 April 2019.

In March 2020, the District Court sentenced the accused to 6 years and 8 months of imprisonment. He was found guilty of forming a criminal organisation and aiding and abetting hundreds of crimes committed on the platform, such as illicit drug trafficking, illicit trafficking in medicines, the sale of counterfeit documents and money, money laundering and data theft. The court further concluded that the contribution of the accused had been limited to the establishment and maintenance of the 'business operation' aimed at committing these crimes.

Fraudsters is said to have been an active exchange platform for criminal offences on the internet for several years up to spring 2019. The majority of those responsible for the platform remain unknown.

The platform Fraudsters

The purpose of this forum was, on the one hand, to offer its users a censorship-free platform for the exchange of tips on committing internet crimes. Thus, the defendant himself wrote an extensive tutorial, which contained multiple tips on how to conceal one's identity to avoid prosecution. He gave tips on how to encrypt the laptop / personal computer used; on 'safe email providers' that do not log user data such as internet protocol (IP) addresses, location, etc.; on browser settings to prevent tracking and fingerprinting; and on how to use the internet, root servers and secure messaging services.

On the other hand, the operators of the forum intended to offer sellers and buyers a platform for the sale and purchase of a wide variety of illegal goods or illegally obtained data for the commission of further criminal offences. Users who wanted to sell goods and data on the forum had to purchase a vendor licence from an administrator or moderator of the forum and be activated as a vendor. The administrators were paid a monthly fee by the vendors. In addition, buyers had to pay a percentage of the transaction value of a purchase to the administrators (via bitcoin addresses). Another source of income for the forum operators were fees for placing advertisements within the forum. The proceeds were divided among the operators.

❖ **County court, No 1-20-5862, Estonia**

Date: 14 September 2020

The defendant was convicted on the basis of § 216[1] of the Estonian Criminal Code (preparation of computer-related crime) of the intentional possession of the malware control panel Anubis. The malware enabled the perpetrator to collect, from the injected Android-based operation system devices, different types of data such as content data (typed texts) and data for authentication (e.g. usernames, passwords, credit card numbers). In addition, he was convicted under the same provision of intentionally obtaining and possessing the authentication data of bank clients from different countries across the world. The purpose of the latter crime was to commit computer fraud (§ 213 of the Criminal Code).

❖ **County court, No 1-20-2876, Estonia**

Date: 17 June 2020

Pursuant to § 216[1] of the Estonian Criminal Code, the defendant was convicted of the intentional possession of authentication data (mainly usernames, passwords and credit card numbers) from the clients of various online services providers, such as SunTrust, PayPal, Citizens Bank, Royalbank, GoBank, eBay and Amazon. Under the same provision, he pleaded guilty to the possession of Trojan-type malware that would have enabled him to collect personal and authentication data from different persons and traffic data. In addition, he possessed another item of Trojan-type malware that made it possible to illegally access ATMs to obtain cash. The purpose of these actions was to intentionally commit, himself or through a third party, unlawful interference with computer data (§ 206 of the Criminal Code), to hinder the functioning of computer systems (§ 207 of the Criminal Code) and to gain illegal access to computer systems (§ 217 of the Criminal Code). He also unlawfully sent data on different credit cards and authentication data to third parties, for the purpose of enabling them to commit computer fraud (§ 213 of the Criminal Code). The court agreed to satisfy the state's claim of EUR 12 000 against the defendant and confiscated the sum as a criminal asset.

❖ **County court, No 1-20-1205, Estonia**

Date: 20 May 2020

Several defendants pleaded guilty pursuant to § 22 (accomplice to a crime) and § 213 of the Estonian Criminal Code to aiding an unidentified group of criminals to perpetrate large-scale computer fraud. Two other defendants were convicted for aiding the unidentified group of perpetrators to commit the same computer fraud. One defendant sent his and other convicted persons' bank authentication data, bank account numbers and debit cards to the group of perpetrators. They subsequently illicitly accessed the PayPal computer system and made money transactions to those bank accounts, using the information sent by the defendant. In addition, the perpetrators opened new bank and savings accounts for the convicted persons and transferred fraudulent money to these accounts. The money was withdrawn from ATMs located in non-EU countries such as Russia and Thailand, or transferred to other bank accounts controlled by the convicted perpetrators. The defendant either transferred the money to his own bank accounts, for personal use, or sent it to Ukraine through Western Union. He therefore also pleaded guilty, pursuant to § 394 of the Criminal Code, to large-scale money laundering perpetrated in a group. The other defendants received criminal penalties for providing their bank account

authentication data and debit cards for transferring the fraudulent money. Approximately EUR 15 000 in criminal funds was confiscated.

- **Supreme Court, No 220/2020, Spain**

  Date: 22 May 2020

In its ruling of 22 May 2020, the Supreme Court established guidelines for assessing 'seriousness' as a requirement for a crime to be classified as 'computer damage'. The court considers that it is an autonomous concept that will have to be assessed not merely on a quantitative basis, but considering the functional damage that hinders the operating system. 'Seriousness' will be evident when it is impossible to recover the functionality of the system or when restoring the operation of the system would require great technical and economic efforts.

- **Supreme Court, No 158/2019 and No 322, Spain**

  Dates: 26 March and 19 June 2020

There is a growing volume of case-law on online sexual abuse in Spain. Inter alia, the Supreme Court has established in its rulings No 158/2019 of 26 March 2020 and No 322 of 19 June 2020 that sexual abuse can be committed via the internet, used as technological means to facilitate proximity between an offender and the victim of the abuse.

Note from the Spanish EJCN member: this is in line with the guidelines set out in the communication from the Commission to the European Parliament and the Committee of the Regions on the EU Strategy for a more effective fight against child sexual abuse of 24 July 2020.

4. Data retention developments in Europe

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

4.1. Developments at EU level

Court of Justice of the European Union

- **Judgment: *Privacy International* – Case C-623/17**
  See Chapter 5.

- **Judgment: *La Quadrature du Net and others* – Joined Cases C-511/18, C-512/18 and C520/18**
  See Chapter 5.

- **Request for preliminary ruling in Case C-140/20**
  On 25 March 2020, the Supreme Court of Ireland lodged a request for a preliminary ruling from the CJEU. The following questions were referred to 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, as interpreted in light of the Charter [of Fundamental Rights of the European Union]?

  (2) In considering whether to grant a declaration of inconsistency of a national measure implemented pursuant to Directive 2006/24/EC2, 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 European Union 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 the 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 para. 46)?*

(6) *May a national court invited to declare the inconsistency of national legislation with Article 15 of the Directive 2002/58/EC, and/or to disapply this legislation, and/or to declare that the application of such legislation had breached the rights of an individual, either in the context of proceedings commenced in order to facilitate an argument in respect of the admissibility of evidence in criminal proceedings or otherwise, be permitted to refuse such relief in respect of data retained pursuant to the national provision enacted pursuant to the obligation under Article 288 [of the Treaty on the Functioning of the European Union] to faithfully introduce into national law the provisions of a directive, or to limit any such declaration to the period after the declaration of invalidity of the Directive 2006/24/EC issued by the CJEU on the 8th day of April, 2014?*

A hearing in this case is scheduled on 24 June 2021.

European Council

The European Council Conclusions of 10 and 11 December 2020 recognise the need for law enforcement and judicial authorities to be able to exercise their powers effectively to combat both online and offline serious crime. In this respect, the Council stressed the need to advance the work on data retention necessary to combat serious crime, in the light of the latest case-law of the CJEU and in full respect of fundamental rights and freedoms.

Access the text of the European Council Conclusions.

European Commission

The June 2019 Council Conclusions tasked the Commission with engaging in targeted consultations with relevant stakeholders and conducting, on that basis, a comparative study on data retention, considering the various options, including a new legislative proposal.

The Commission finalised the 'Study on the retention of electronic communications non-content data for law enforcement purposes' at the end of 2020. The study, involving 10 EU Member States (Germany, Estonia, Ireland, Spain, France, Italy, Austria, Poland, Portugal and Slovenia), aimed to collect information on the legal framework and practices for retention of and access to electronic communications non-content data for law enforcement purposes. It includes needs of and challenges experienced by law enforcement authorities and electronic communications service providers.

Access the final report on the study.

4.2. Developments at national level

Belgium

Judgment: Court of First Instance of East Flanders (Ghent), 25 November 2020
Judgment: Court of Appeal of Antwerp, 26 November 2020
Judgment: Court of First Instance of Antwerp, 17 December 2020

Following the CJEU ruling of 6 October 2020, several courts have found evidence gathered from operators who retain traffic and location data in a general and indiscriminate way admissible in court.

Bulgaria

Owing to the COVID-19 pandemic, the Electronic Communications Act was amended to ensure that location data could be retained for the purpose of compelled compliance with mandatory isolation and hospital treatment of persons who refused or failed to comply with mandatory isolation and treatment.

The Bulgarian Constitutional Court, through its judgment of 17 November 2020, declared the abovementioned amendment to the Electronic Communications Act unconstitutional. The court ruled that the adopted legislative measure contradicted the Bulgarian Constitution and did not meet the requirements of necessity and proportionality.

Ireland

A new Bill in relation to data retention is currently being drafted in Ireland. It is intended that a revised Communications (Data Retention and Disclosure) Bill will replace the Communications (Retention of Data) Act 2011. The Bill will take into account the CJEU rulings, thereby providing the most effective crime prevention and investigative regime possible having regard to the changing legal environment.

Spain

Judgment No 217/2020, Supreme Court, 15 June 2020

In its ruling of 15 June 2020, the Supreme Court rejected the request by the defendant to refer a preliminary ruling to the CJEU. The Supreme Court maintained the arguments of previous judgments, stating that the Spanish national legislation meets the requirements set out by the CJEU. It is up to the examining judge to decide in each case, taking into account the principle of proportionality.

Note: In Spain, the domestic regulation that implemented Directive 2006/24/EC, allowing general and indiscriminate retention of traffic and location data, is still in force. A judicial authorization is required to access the retained data.

Norway (non-EU country)

In Norway, a working group has been established to take a closer look at the notions of retention of IP addresses and general data retention. So far, however, this has not resulted in any new legal provisions or amendments.

5. Topic of interest

Overview of rulings of the Court of Justice of the European Union related to data retention for the purposes of prevention and prosecution of crime

Introduction

More and more of our daily activities and communications are taking place online or via information systems and mobile devices. Criminal activity online has also increased. This means that law enforcement and judicial authorities, when investigating crime, are more and more dependent on digital information and evidence. Electronic information and evidence is needed in about 85 % of investigations into serious crimes ([1]). Having lawful access to such data is therefore important, and in some cases it is the only way to proceed with an investigation and find proof of a crime. Access to digital evidence, however, depends on the availability of information. Telecommunications service providers are often the only ones having information that can help to identify individuals behind criminal activity. Therefore, retention by service providers of non-content communications data (i.e. traffic and location data) and the possibility for law enforcement authorities to subsequently access retained data, respecting procedural and substantive safeguards, is of particular importance in order to combat serious crime effectively.

Data retention and access to data inevitably trigger discussions about balancing the right to privacy and secrecy of communications versus the need to ensure public security and effectively combat serious crime and terrorism.

In 2014, the CJEU declared the 2006 Data Retention Directive to be invalid. Subsequently, the CJEU prohibited the EU and its Member States in the Digital Rights Ireland and Tele2 Sverige cases in 2016 from laying down rules that entail general and indiscriminate retention of data, setting limits on the data retention regime and imposing conditions for access to retained data. In its La Quadrature du Net ruling, the court, on the one hand, confirmed the Tele2 Sverige decision but, on the other hand, also provided several examples of areas in which exceptions to the prohibition on general and indiscriminate data retention would be possible. Currently, several cases are still pending before the court.

Since the invalidation of the Data Retention Directive, the topic of data retention has been discussed extensively within Member States and at EU level. Member States have repeatedly emphasised at various levels that they encounter issues in criminal investigations because of the disparities in (or simply a lack of) data retention regimes in Europe, and the effects of the CJEU rulings on national data regimes. The topic was discussed at the Justice and Home Affairs Council in March 2021, where the vast majority of Member States supported a common EU legal framework on data retention, respecting the CJEU rulings and at the same time facilitating judicial cooperation with the aim of achieving a coherent response on the part of the Member States to the need to combat crime.

In order to be able to take stock of the current state of play of CJEU case-law, this chapter provides an overview of the essence of the relevant CJEU rulings on data retention until now. Where possible, the subsequent consequences at national level, following the CJEU ruling, are also mentioned.

[1] EU Security Union Strategy, p. 12.

Main CJEU Rulings related to Data Retention

8 April 2014
DIGITAL RIGHTS IRELAND
Joined Cases C-293/12 and C-594/12

Directive 2006/24/EC is invalid.

21 December 2016
TELE2 SVERIGE AND WATSON
Joined Cases C-203/15 and C-698/15

EU law does not allow general and indiscriminate **RETENTION** of traffic and location (T&L) data.

But, **targeted retention** is possible, under certain conditions.

ACCESS to retained T&L data is restricted to the objective of fighting serious crime and requires prior review.

2 October 2018
MINISTERIO FISCAL
Case C-207/16

ACCESS to retained T&L data can be justified for criminal offences in general, if it does not constitute a serious interference with privacy.

6 October 2020
PRIVACY INTERNATIONAL
Case C-623/17

General and indiscriminate transmission of (and thus **ACCESS** to) T&L data to security and intelligence services for the purpose of safeguarding national security is not allowed.

6 October 2020
LA QUADRATURE DU NET AND OTHERS
Joined Cases C-511/18, C-512/18, C-520/18

EU law does not allow general and indiscriminate **RETENTION** of traffic and location data

By contrast, some measures are allowed, for specific purposes, under certain conditions:

- General and indiscriminate retention, in case of a **serious threat to national security**;
- **Targeted retention**, limited to **categories of persons or using geographical criterion**;
- **Expedited retention** in case of serious criminal offences or attacks on national security;
- General and indiscriminate retention of **IP addresses** assigned to the source of an Internet connection;
- General and indiscriminate retention of **data relating to the civil identity of users**.

Automated analysis and real-time collection by service providers is allowed in specific situations.

EU law does not allow general and indiscriminate **RETENTION** of personal data by providers of access to online public communication services and hosting service providers.

2 March 2021
PROKURATUUR
Case C-746/18

ACCESS to a set of traffic or location data, allowing precise conclusions to be drawn concerning a person's private life, is allowed only in order to combat serious crime or prevent serious threats to public security, regardless of the duration of the access and quantity or nature of the data.

The public prosecutor's office cannot be granted the power to authorise access of a public authority to T&L data for the purpose of a criminal investigation.

❖ *Digital Rights Ireland and others* – Joined Cases C-293/12 and C-594/12

Date: 8 April 2014

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

Reference for a preliminary ruling by: High Court of Ireland and Constitutional Court of Austria.

Concerning: Validity of Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

Question referred for a preliminary ruling and considered by the court ([2])*:*

Is Directive 2006/24/EC compatible with Articles 7, 8 and 11 of the Charter of Fundamental Rights of the EU (EU Charter)?

Court ruling:

First, the **retention** is not restricted to data from a particular time period and/or a particular geographical zone and/or particular persons likely to be involved in serious crime or persons who could contribute to the prevention, detection or prosecution of serious offences. Second, the Directive does not lay down limits on **access** for competent authorities to the data, particularly concerning offences that are sufficiently serious to justify an interference with the rights enshrined in Articles 7 and 8 of the EU Charter. Furthermore, the Directive does not contain substantive and procedural conditions relating to **access**, including a prior review of access by a court or independent administrative body. Third, the Directive defines a data retention period without any distinction being made between the categories of data, and it does not set objective criteria for limiting the retention period to what is strictly necessary.

The court found that the interference of the Directive with fundamental rights was not precisely circumscribed by provisions to ensure that it would be limited to what was strictly necessary. The Directive thus exceeded the limits imposed by the principle of proportionality in the light of Articles 7, 8 and 52(1) of the EU Charter.

- **Directive 2006/24/EC is invalid.**

Subsequent national court rulings and/or effects:

Austria

The Austrian regulations related to data retention were repealed by the Austrian Constitutional Court on 27 June 2014, following this CJEU ruling.

Ireland

Ireland has prepared draft legislation in this area. On 25 March 2020, the Supreme Court lodged a request for a preliminary ruling to the CJEU (see questions on page 19).

[2] For the purpose of this chapter, only the questions considered by the court are mentioned.

❖ *Tele2 Sverige AB and Watson and others* – Joined Cases C-203/15 and C-698/15

Date: 21 December 2016

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

Reference for a preliminary ruling by: Administrative Court of Appeal of Stockholm, Sweden, and Court of Appeal (England and Wales), United Kingdom

Concerning: Interpretation of Article 15(1) 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, as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, in the light of Articles 7, 8 and 52(1) of the EU Charter.

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

1. Is a general obligation to retain traffic data covering all persons, all means of electronic communication and all traffic data without any distinctions, limitations or exceptions for the purpose of combating crime compatible with Article 15(1) of Directive 2002/58/EC, taking account of Articles 7 and 8 and Article 52(1) of the Charter?

2. Must Article 15(1) of Directive 2002/58/EC be interpreted as precluding national legislation governing the protection and security of traffic and location data and the access of competent authorities to retained data, where that legislation does not restrict that access solely to the objective of fighting serious crime, where that access is not subject to prior review and where there is no requirement that the data should be retained within the EU?

3. Does the Digital Rights Ireland judgment expand the scope of Articles 7 and/or 8 of the EU Charter beyond that of Article 8 of the ECHR as established in the jurisprudence of the European Court of Human Rights? (Question found inadmissible by the court.)

Court ruling:

- Article 15(1) of Directive 2002/58/EC must be interpreted as precluding national legislation which, for the purpose of fighting crime, provides for **general and indiscriminate retention** of all traffic and location data of all subscribers and registered users relating to all means of electronic communication.
  Article 15(1) of Directive 2002/58/EC does not prevent Member States from adopting legislation permitting, as a preventive measure, the **targeted retention** of traffic and location data, for the purpose of fighting serious crime. This targeted retention of data needs to be limited, with respect to the **categories of data** to be retained, the **means of communication** affected, the **persons concerned** and the **retention period** adopted, to what is strictly necessary.

- Article 15(1) of Directive 2002/58/EC must be interpreted as precluding national legislation governing the protection and security of traffic and location data and, in particular, **access** of the competent national authorities to the retained data, where the objective pursued by that access, in the context of fighting crime, is not restricted solely to fighting **serious crime**, where access is not

subject to **prior review** by a court or an independent administrative authority, and where there is no requirement that the data concerned should be **retained within the European Union**.

Subsequent national court rulings and/or effects:

Sweden

Following this CJEU ruling, the Court of Appeal ruled that the Swedish legislation regarding data retention was incompatible with EU law and therefore repealed the order to retain data in the specific case. After the judgment, all service providers stopped retaining data and deleted all remaining data that had been previously retained. As a result of this, a new data retention law was introduced in Sweden in 2019.

United Kingdom

This CJEU ruling required the United Kingdom to limit the scope of its data retention regime. In response to the ruling, the UK government introduced the Data Retention and Acquisition Regulations 2018, amending the Regulation of Investigatory Powers Act 2000 and Parts 3 and 4 of the Investigatory Powers Act 2016, which provided for interference in privacy in the interests of national security.

❖ *Ministerio Fiscal* – Case C-207/16

Date: 2 October 2018

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

Reference for a preliminary ruling by: Provincial Court of Tarragona, Spain

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

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

1. Can the sufficient seriousness of offences be determined solely on the basis of the sentence that may be imposed in respect of the offence investigated, or is it also necessary to identify in the criminal conduct particular levels of harm to legally protected interests?

2. If the seriousness of the offence should be determined solely on the basis of the sentence imposed, what should be the minimum threshold and would it be compatible with a general provision setting a minimum threshold of 3 years' imprisonment?

Court ruling:

- Article 15(1) of Directive 2002/58/EC must be interpreted as meaning that the **access** by public authorities to data for the purpose of identifying the owners of SIM cards activated with a stolen mobile telephone, such as the surnames, forenames and, if need be, addresses of the owners, entails interference with their fundamental rights enshrined in the EU Charter. This **interference is not sufficiently serious** to entail that **access being limited**, in the area of prevention, investigation, detection and prosecution of criminal offences, to the objective of fighting **serious crime**.

Subsequent national court rulings and/or effects:

Spain

The Court of Appeal upheld the appeal made by the public prosecutor in the national case, thereby granting the judicial police access to the retained data. Following the CJEU ruling, Opinion 1/2019 of the Computer Crime Unit of the Attorney General's Office was delivered. It clarified whether information relating to the connection between a physical mobile device (identified by the International Mobile Equipment Identity) and an International Mobile Subscriber Identity (integrated into the SIM card) needed to be considered subscriber data or traffic data. This issue is of particular interest in Spain, as access to subscriber data, unlike traffic data, does not require judicial authorisation. Following this opinion, a general approach to be followed by all prosecutors was adopted.

❖ *Privacy International* – Case C-623/17

Date: 6 October 2020

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

Reference for a preliminary ruling by: Investigatory Powers Tribunal, United Kingdom

Concerning: Interpretation of Article 1(3) and Article 15(1) of Directive 2002/58/EC, read in the light of Article 4(2) of the Treaty on European Union and Articles 7, 8 and 52(1) of the EU Charter. Legality of legislation authorising the acquisition and use of bulk communications data by the security and intelligence agencies.

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

1. Does national legislation enabling a Member State authority to require service providers to forward traffic and location data to the security and intelligence agencies for the purpose of safeguarding national security fall within the scope of Directive 2002/58/EC?

2. If such national legislation falls within the scope of the Directive, do any of the requirements applicable to retained communications data as set out in the Tele2 judgment apply to it? And if so, how and to what extent do they apply?

Court ruling:

- Article 1(3), Article 3 and Article 15(1) of Directive 2002/58/EC must be interpreted as meaning that national legislation enabling a state authority to require providers of electronic communications services to forward traffic data and location data to the security and intelligence agencies for the purpose of safeguarding national security falls within the scope of that directive.

- Article 15(1) of Directive 2002/58/EC must be interpreted as precluding national legislation enabling a state authority to require providers of electronic communications services to carry out the general and indiscriminate transmission of traffic data and location data to the security and intelligence agencies for the purpose of safeguarding national security.

❖ *La Quadrature du Net and others* – Joined Cases C 511/18, C-512/18 and C-520/18

Date: 6 October 2020

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

Reference for a preliminary ruling by: Council of State, France, and Constitutional Court, Belgium

Concerning: Interpretation of Article 15(1) of Directive 2002/58/EC and of Articles 12 to 15 of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, read in the light of Articles 4, 6, 7, 8 and 11 and Article 52(1) of the EU Charter and Article 4(2) of the Treaty on European Union.

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

1. Must Article 15(1) of Directive 2002/58/EC be interpreted as precluding national legislation that imposes on providers of electronic communications services, for the purposes set out in Article 15(1), an obligation requiring the general and indiscriminate retention of traffic and location data?

2. Must Article 15(1) of Directive 2002/58/EC be interpreted as precluding national legislation that requires providers of electronic communications services to implement, on their networks, measures allowing, first, the automated analysis and real-time collection of traffic and location data and, second, real-time collection of technical data concerning the location of the terminal equipment used, but which makes no provision for the persons concerned by that processing and that collection to be notified thereof?

3. Must the provisions of Directive 2000/31/EC be interpreted as precluding national legislation that requires providers of access to online public communication services and hosting service providers to retain, generally and indiscriminately, inter alia, personal data relating to those services?

4. May a national court apply a provision of national law empowering it to limit the temporal effects of a declaration of illegality that it is bound to make under that law in respect of national legislation imposing on providers of electronic communications services – with a view to, inter alia, pursuing the objectives of safeguarding national security and combating crime – an obligation requiring the general and indiscriminate retention of traffic and location data, owing to the fact that that legislation is incompatible with Article 15(1) of Directive 2002/58/EC, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter?

Court ruling:

- Article 15(1) of Directive 2002/58/EC must be interpreted as precluding legislative measures which, for the purposes laid down in Article 15(1), provide, as a preventive measure, for the **general and indiscriminate retention** of traffic and location data.
  By contrast, Article 15(1), read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, does not preclude legislative measures that:

- allow, for the purposes of safeguarding national security, recourse to an instruction requiring providers of electronic communications services to **retain, generally and indiscriminately**, traffic and location data in situations where the Member State concerned is confronted with a **serious threat to national security** that is shown to be **genuine and present or foreseeable**, where the decision imposing such an instruction is subject to **effective review**, either by a court or by an independent administrative body whose decision is binding, the aim of that review being to verify that one of those situations exists and that the conditions and safeguards which must be laid down are observed, and where that instruction may be given only for a **period that is limited in time** to what is strictly necessary, but which may be extended if that threat persists;

– provide, for the purposes of safeguarding national security, combating serious crime and preventing serious threats to public security, for the **targeted retention** of traffic and location data 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;

– provide, for the purposes of safeguarding national security, combating serious crime and preventing serious threats to public security, for the **general and indiscriminate retention of IP addresses** assigned to the source of an internet connection for a **period that is limited in time** to what is strictly necessary;

– provide, for the purposes of safeguarding national security, combating crime and safeguarding public security, for the **general and indiscriminate retention of data relating to the civil identity of users** of electronic communications systems;

– allow, for the purposes of combating serious crime and, a fortiori, safeguarding national security, recourse to an instruction requiring providers of electronic communications services, by means of a decision of the competent authority that is subject to **effective judicial review**, to undertake, for a **specified period of time**, the **expedited retention** of traffic and location data in the possession of those service providers,

provided that those measures ensure, by means of clear and precise rules, that the retention of data at issue is subject to compliance with the applicable substantive and procedural conditions and that the persons concerned have effective safeguards against the risks of abuse.

➢ Article 15(1) of Directive 2002/58/EC must be interpreted as not precluding national rules which requires providers of electronic communications services to have recourse, first, to the **automated analysis and real-time collection**, inter alia, of traffic and location data and, second, to the **real-time collection of technical data** concerning the location of the terminal equipment used, where:

– recourse to **automated analysis** is limited to situations in which a Member State is facing a serious threat to national security which is shown to be **genuine and present or foreseeable**, and where recourse to such analysis may be the subject of an **effective review**, either by a court or by an independent administrative body whose decision is binding, the aim of that review being

to verify that a situation justifying that measure exists and that the conditions and safeguards that must be laid down are observed; and where

- recourse to the **real-time collection** of traffic and location data is **limited to persons in respect of whom there is a valid reason to suspect that they are involved in one way or another in terrorist activities** and is subject to a **prior review** carried out either by a court or by an independent administrative body whose decision is binding, in order to ensure that such real-time collection is authorised only within the limits of what is strictly necessary. In cases of duly justified urgency, the review must take place within a short time.

- **Directive 2000/31** must be interpreted as **not being applicable** in the field of the protection of the confidentiality of communications and of natural persons as regards the processing of personal data in the context of information society services, such protection being governed by Directive 2002/58/EC or by Regulation 2016/679, as appropriate. **Article 23(1) of Regulation 2016/679**, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, must be interpreted as precluding national legislation which requires that **providers of access to online public communication services and hosting service providers** retain, generally and indiscriminately, inter alia, personal data relating to those services.

- A national court may **not** apply a provision of national law empowering it to **limit the temporal effects of a declaration of illegality**, which it is bound to make under that law, in respect of national legislation imposing on providers of electronic communications services – with a view to, inter alia, safeguarding national security and combating crime – an **obligation requiring the general and indiscriminate retention of traffic and location data that is incompatible with Article 15(1)** of Directive 2002/58/EC, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter. Article 15(1), interpreted in the light of the principle of effectiveness, requires **national criminal courts to disregard information and evidence obtained by means of the general and indiscriminate retention of traffic and location data in breach of EU law**, in the context of **criminal proceedings** against persons suspected of having committed criminal offences, where those **persons are not in a position to comment** effectively on that information and that evidence and they pertain to a field of which the judges have no knowledge and are likely to have a **preponderant influence on the findings of fact**.

Subsequent national court rulings and/or effects:

Belgium

On 22 April 2021, the Constitutional Court annulled the Belgian data retention law.

France

On 21 April 2021, the Council of State ruled on appeals lodged by several non-governmental organisations and a telecommunications operator. The Council of State examined the conformity with EU law of French rules on the retention of connection data. It also verified that the implementation of EU law, as interpreted by the CJEU, does not jeopardise the requirements of the French Constitution.

The Council of State ruled that the existing threat to national security currently justified the generalised retention of data. It also noted that the possibility of accessing connection data to fight serious crime allows the government, at the present time, to meet the constitutional requirements to prevent breaches of law and order and ensure the search for perpetrators of criminal offences.

However, it ordered the government to regularly reassess the threat that exists in France to justify the generalised retention of data and to make the use of these data by the intelligence services subject to an authorisation provided by an independent authority.

This and more detailed information can be found on the Council of State website.

❖ *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.

Provisions of Directive 2006/24/EC and Directive 2002/58/EC

Directive 2006/24/EC

Article 1 – Subject matter and scope

This Directive aims to harmonise Member States' provisions concerning the obligations of the providers of publicly available electronic communications services or of public communications networks with respect to the retention of certain data which are generated or processed by them, in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law.

This Directive shall apply to traffic and location data on both legal entities and natural persons and to the related data necessary to identify the subscriber or registered user. It shall not apply to the content of electronic communications, including information consulted using an electronic communications network.

Article 3 – Obligation to retain data

By way of derogation from Articles 5, 6 and 9 of Directive 2002/58/EC, Member States shall adopt measures to ensure that the data specified in Article 5 of this Directive are retained in accordance with the provisions thereof, to the extent that those data are generated or processed by providers of publicly available electronic communications services or of a public communications network within their jurisdiction in the process of supplying the communications services concerned.

[…]

Article 4 – Access to retained data

Member States shall adopt measures to ensure that data retained in accordance with this Directive are provided only to the competent national authorities in specific cases and in accordance with national law. The procedures to be followed and the conditions to be fulfilled in order to gain access to retained data in accordance with necessity and proportionality requirements shall be defined by each Member State in its national law, subject to the relevant provisions of European Union law or public international law, and in particular the ECHR as interpreted by the European Court of Human Rights.

Article 6 – Retention period

Member States shall ensure that the categories of data specified in Article 5 are retained for periods of not less than six months and not more than two years from the date of the communication.

Directive 2002/58/EC

Article 1(3) – Scope and aim

This Directive shall not apply to activities which fall outside the scope of [the Treaty on the Functioning of the European Union], such as those covered by Titles V and VI of the Treaty on European Union, and in any case to activities concerning public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the activities of the State in areas of criminal law.

Article 15 – Application of certain provisions of Directive 95/46/EC

Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph.

6. Way ahead

The CJM is produced once per year. As of this issue, the CJM is produced at the beginning of the year, reporting on information relating to the full 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.

Importantly, the content of the CJM depends on the input of practitioners. We therefore kindly encourage EJCN practitioners to send to Eurojust, throughout the year, relevant national legislative developments, court decisions, suggestions for topics of interest and other information considered useful for the purpose of producing future issues of the CJM.

We thank the experts of the European Judicial Cybercrime Network for their valuable contributions 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
Twitter & LinkedIn: @Eurojust

Catalogue number: QP-AG-21-006-EN-N • *ISBN*: 978-92-9490-605-2 • *ISSN*: 2600-0113 • *DOI*: 10.2812/406484