Cybercrime Judicial Monitor

Issue 5 – December 2019

Criminal justice across borders

Table of Contents

1. Executive Summary

Eurojust presents this fifth 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 combatting cybercrime and cyber-enabled crime. It is produced on the basis of information provided by members of the European Judicial Cybercrime Network (EJCN). All existing and future issues of the CJM will now also be publicly accessible via the Eurojust website.

This issue of the CJM contains four main sections. The first section covers legislative developments in the area of cybercrime, cyber-enabled crime and electronic evidence in 2019.

The judicial analysis section presents legal analyses of court rulings rendered by courts in different Member States and third countries. The courts ruled on different cyber-related matters, such as law enforcement authorities (LEA) accessing an account of a suspect using a keylogger, or accessing a device by use of a suspect's fingerprint and access to data abroad via a third-party network search. In addition, a Belgian ruling of the Court of Cassation is analysed, focussing on the obligation for service providers to cooperate with LEA. Several other national court rulings are also briefly summarised.

The next section is devoted to the topic of data retention, particularly the recent developments within the European Union with regard to the application of data retention rules. An overview is provided of recent national legislative and case law developments.

The topic of interest in this issue of the CJM is 'handling of virtual currencies in criminal investigations and proceedings'. The chapter touches upon the concept of virtual currencies, the legal framework and policies in the different countries covering the seizure and handling of virtual currencies during investigations, as well as challenges and obstacles encountered when seizing and possibly converting virtual currencies at different stages of the investigation.

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 2019. The main sources of information presented in this section are contributions collected through the EJCN, unless specifically stated otherwise.

2.1. EU level

- *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*

On 9 April 2019, the Council formally adopted the Directive on combating fraud and counterfeiting of non-cash means of payment.

The Directive updates the existing rules to ensure that a more technology-neutral legal framework is in place. In addition to the traditional non-cash means of payments, it covers means that have been developed more recently, such as virtual currencies, electronic wallets and mobile payments.

The Directive establishes minimum rules concerning the definition of criminal offences and sanctions in the areas of fraud and counterfeiting of non-cash means of payment.

Furthermore, the Directive requires Member States to establish jurisdiction over the offences listed in the Directive when certain conditions apply. The Directive also aims to tackle operational obstacles that hamper investigation and prosecution, and foresees actions to enhance public awareness of fraudulent techniques such as phishing and skimming.

Finally, the new instrument facilitates the prevention of the offences that are covered by the Directive, and the provision of assistance to and support for victims.

The Directive was published in the Official Journal of the European Union on 10 May 2019. Member States have two years to implement the Directive.

The full text of the Directive can be found here.

- *Council conclusions on combating the sexual abuse of children*

On 8 October 2019, the Council adopted conclusions on combating the sexual abuse of children. Although these conclusions do not have legally binding effect, they do underline that the protection of children against sexual abuse, offline and online, remains an important priority within the European Union.

In its conclusions, the Council invites the European Union and its Member States to assess periodically the effectiveness of legislation on combating the sexual abuse and sexual exploitation of children. This assessment should particularly address the prevention, investigation and prosecution of such crimes.

The Council also reiterates the importance of timely action to investigate and prosecute offenders and invites competent authorities to make the widest possible use of the existing tools and mechanisms available at national and EU level, particularly at Europol and Eurojust.

For competent authorities to be able to exploit the data collected during investigations, and conduct effective prosecutions, the Council reiterated that data retention is essential.

The Council encourages Member States to develop and apply innovative investigation methods as well as to consider allocating specialised law enforcement resources to combat child abuse and sexual exploitation. Moreover, the importance of providing law enforcement agencies and other authorities with appropriate training in this context was stressed.

Given the exponential increase in child sexual abuse material online, the Council urges the industry, including online service providers, to ensure lawful access to digital evidence for law enforcement and other competent authorities. The Council invites online service providers to remove or disable access to contents identified as child sexual abuse material online as soon as possible after becoming aware of such content. It calls on the Commission to propose measures to address this growing challenge.

A global, coordinated approach to fight this type of crime is important, including cooperation with third countries and other key stakeholders.

The full text of the Council conclusions can be found here.

2.2. Member States

Finland

- *Regulations on network traffic intelligence*

New regulations concerning network traffic intelligence have come into force since 1 June 2019, accompanied by laws concerning a new authority called 'Intelligence Ombudsman', who will supervise the application of intelligence legislation. The new regulations affect the Finnish Security Intelligence Service's competence in intelligence gathering related to national security. In short, new powers have been granted for combating serious threats against national security.

The regulations stipulate that network traffic intelligence operations are allowed if this can provide further details of a known and serious threat. The threat must be sufficiently serious to jeopardise national security, and the intelligence must be required to safeguard democratic values such as policymaking or freedom of expression. The use of network traffic intelligence is decided by a court of law. Technical screening of messages is not done via message content, but via communication metadata. Exceptions to this method are malware and the communications of foreign powers that do not enjoy the protection of confidential messages.

Italy

- *Law of 19 July 2019, n. 69*

Article 10 of the Law of 19 July 2019, n. 69 provides for the criminalisation of so-called 'revenge porn'. Punishable by imprisonment from one to six years, and fines ranging from EUR 5 000 to 15 000, is anyone who, after having produced or stolen sexually explicit images or videos, intended for private use, sends, delivers, sells, publishes or broadcasts said audiovisual materials without the express consent of the persons concerned. The law also stipulates that the punishment is increased if the offence of illegal dissemination of the material is committed by the spouse, even if separated or divorced, or by a person who is or has been in a relationship with the offended party. The same applies if the material is disseminated through IT or digital tools or if the offence is committed against a person in a condition of physical or mental inferiority or against a pregnant woman. In these cases, the penalty is increased

by one-third to one-half of the abovementioned sentence and is also punishable by way of *ex officio* indictment, while it is normally prosecuted upon complaint by the offended party.

Netherlands

- *Computer Crime Act III*

The Computer Crime Act III entered into force on 1 March 2019.

The objective of this law is to improve the investigative powers and prosecution of cybercrime. The law includes some changes to the Criminal Code and Code of Criminal Procedure. New or amended provisions are put in place for criminalising the publication of non-public data, the fencing of data and online fraud. The definition of child grooming is also changed so that an undercover agent can now pose as an adolescent online to facilitate the identification and prosecution of groomers who approach minors online for sexual purposes.

The most relevant new investigative method is 'hacking', introduced in Article 126nba of the Dutch Code of Criminal Procedure. This provision allows, under certain conditions, a public prosecutor to order a competent law enforcement officer to gain remote access to an automated system/work used by the suspect and to perform an investigation, whether or not using a technical tool. This feature was the most debated aspect of the new law, which was heavily discussed in parliament. Hopefully, it will provide a solution in some cases for encryption, continually changing networks and anonymising tools as well as jurisdiction issues. In addition, the possibility to order a takedown of criminal content is added.

3. Judicial analysis

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

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

3.1. Selected court rulings

➢ Belgium

Court of Cassation, case nr. P.17.1229.N, 19 February 2019

Keywords: obligation for Skype to facilitate wiretap, Belgian territorial jurisdiction

INTRODUCTION

In October 2016, Skype was convicted for not complying with an order to wiretap from the Belgian investigating judge, as well as not providing technical assistance in performing the wiretap on a Skype account. *For the full analysis of the case, please see Cybercrime Judicial Monitor nr. 3, page 11.*

The Court of Appeal confirmed the judgement of the Court of First Instance in 2017.

APPEAL IN CASSATION

This appeal in cassation is directed against the judgement of the Antwerp Court of Appeal. The most relevant sections of the ruling are mentioned below.

1. The plaintiff alleged infringement of Article 56 TFEU. The assessment of the judgement concerning the plaintiff's obligation to cooperate on the basis of Articles 88bis and 90quater of the Code of Criminal Procedure necessarily implies that, if the plaintiff does not have an establishment in Belgium, it must have some infrastructure or physical presence if it wishes to offer its electronic communication services in Belgium. This obligation must be considered as a prohibition, or at least an obstacle, or a way of making the plaintiff's activity as a provider of services in Belgium less attractive, contrary to the prohibition on restricting the freedom to provide services laid down in Article 56 TFEU.

   Moreover, Article 2, § 1 and § 2, of the Royal Decree of 9 January 2003 laying down the possibilities for the legal obligation to cooperate in judicial orders relating to electronic communication stipulates that every provider of an electronic communication service must designate several persons by name and charge them with the tasks arising from this duty of cooperation. These persons form the 'Justice Coordination Unit'. The second section of paragraph 2 of that article stipulates that the unit must be established on Belgian territory. In addition, this provision implies

a prohibition, or at a minimum a hindrance, or making the plaintiff's activity as a provider of services in Belgium less attractive.

The Court of Cassation, having had a closer look at the Appeal judgement, stated that the conclusion of the judgement that the requested technical information must be provided in Belgium does not imply that the plaintiff should have a branch or any infrastructure or physical presence in Belgium if it had the intention to offer its electronic communications services in Belgium. In this respect, the plaintiff's argument is based on an incorrect interpretation of the judgement, according to the Court.

Furthermore, the Appeal judgement rules that the plaintiff is being prosecuted for failure to provide the requested information in accordance with Article 88bis of the Code of Criminal Procedure and failure to provide technical assistance with the wiretapping measure pursuant to Article 90quater of the Code of Criminal Procedure, but not for failing to have a technical infrastructure on Belgian territory. Thus, the judgement does not support the conviction of the plaintiff on the grounds of the Royal Decree.

The Court thus concluded that, in so far as a claim can be made that Article 2, § 1 and § 2, of the Royal Decree infringes Article 56 TFEU, the claim cannot lead to cassation and is therefore inadmissible due to lack of relevance.

2. The plaintiff further claimed that, to the extent that the judgement should be interpreted as implying that the measure ordered by the investigating magistrate must be implemented in Luxembourg when the plaintiff does not have any infrastructure or physical presence in Belgium, without a request for legal assistance having to be made in accordance with Article 18, § 1 and § 2, of the MLA Convention of 29 May 2000, and without taking Luxembourg legislation into account, the aforementioned provisions are infringed.

The Court reasoned that Articles 88bis and 90quater of the Code of Criminal Procedure allow the Belgian investigating magistrate, in the context of his judicial investigation, to order the disclosure of the information referred to in this case by any operator of an electronic communications network or provider of an electronic communications service that actively directs its economic activity to consumers in Belgium, to request assistance with regard to electronic communications conducted in Belgium, regardless of the location of that operator or provider. After all, such a provider is sometimes subject to Belgian legislation because of the mere fact of its active participation in economic life in Belgium. The cooperation obligation referred to here does not require intervention by the Belgian judicial authorities abroad. Consequently, the investigating magistrate is not obliged to make a request for mutual legal assistance to Luxembourg, where the provider has its establishment or infrastructure.

The Court furthermore referred to the Appeal judgement by agreeing that the services provided by the plaintiff on Belgian territory to residents of Belgium are governed by applicable Belgian law and not by Luxembourg law.

The Court found the decision was therefore justified and rejected the plaintiff's claim.

3. The plaintiff alleged infringement of Article 8 ECHR and Article 2 of the Luxembourg Law of 11 August 1982 on the protection of privacy. According to the plaintiff, the judgement wrongly finds that the cooperation to be provided by the plaintiff falls under Belgian law and not under Luxembourg law and the plaintiff was obliged to lend this cooperation on the basis of an order from the Belgian examining magistrate, while the plaintiff, as a legal entity established in Luxembourg without infrastructure in Belgium was required to comply with Luxembourg law. If the plaintiff is obliged to submit usage data to the Belgian examining magistrate in violation of Luxembourg law, she is forced to disregard the privacy of the persons who use her services.

The Court referred to the aforementioned unsuccessfully alleged infringements, namely that Luxembourg legislation is not applicable, and therefore declared the claim inadmissible.

COURT DECISION

The Court of Cassation rejected the appeal.

➢ Netherlands

Court of North-Holland – criminal chamber, 14 December 2018

Keywords: search of mobile device using fingerprint/PIN code, *nemo tenetur*, evidence gathering

INTRODUCTION

In this case, a person was suspected of importing drugs as well as having drugs in his possession.

DEFENCE

The defendant's counsel argued that the information found on the defendant's smartphone should be excluded as evidence, as the investigation of the telephone was unlawful. According to the defence, the defendant did not give the PIN code of his telephone voluntarily, but under threat of physical coercion (the police would force him to give his fingerprint). The defendant provided the PIN code because he wanted to avoid this physical coercion. Since the PIN code of the telephone was obtained as a result of unlawful pressure, the defence claimed a a violation of the *nemo tenetur* principle. As a consequence, the statement of the defendant (giving the PIN code) as well as the information obtained from the telephone should be excluded as evidence.

COURT REASONING

The Court assessed whether the police were allowed, after receiving authorisation from the public prosecutor, to use the biometric data of the defendant against his will to unlock his phone.

The Court reasoned that the *nemo tenetur* principle was not violated and the police were authorised - with the permission of the public prosecutor - to forcibly take the fingerprint from the accused to unlock the smartphone. Such an order is comparable to the (forced) taking of fingerprints during investigations. A fingerprint concerns biometric material that exists independently of the will of the defendant and that could be obtained without his cooperation (which is different in case of unlocking the telephone by a password). The Court also takes into account a major interest in unlocking the telephone (given that the accused was detained for a serious criminal offence) and that the infringement on physical integrity is minor. The fact that the defendant ultimately - and therefore in a certain way not entirely voluntarily - gave his password does not, therefore, mean that a formal default has occurred.

In addition, the search of the telephone itself cannot be regarded as unlawful. In the present case, the public prosecutor gave permission to the police to investigate the telephone, which provides sufficient legitimacy for that investigation.

COURT RULING

The Court dismissed the claim of the defence and found the evidence admissible.

Court of Appeal of Amsterdam, 14 December 2018

Keywords: use of evidence from telephone with Pretty Good Privacy (PGP) application

INTRODUCTION

In this case, the Court of First Instance in Amsterdam previously convicted the defendant for, among other offences, complicity in an attempted murder. One aspect of the ruling of the Court of Appeal is analysed in detail below, namely the assessment of the evidence with regard to messaging using Pretty Good Privacy (PGP).

DEFENCE

The defence argued that the investigation of the seized BlackBerry telephones was unlawful and carried out without the authorisation of the judge. The defence pointed out that the telephones were equipped with the PGP application, the use of which is focused particularly on protection of privacy. Therefore, the decoding of the content of the telephones by the police resulted in an unacceptably broad intrusion into the personal privacy of the defendant.

COURT REASONING

The Court first of all stated that, to arrive at the truth, seized objects may be investigated to obtain data for the criminal investigation. This also applies to seized electronic devices and automated systems, including BlackBerrys. However, if a conclusion can be made that the investigation has been so far-reaching that a more or less complete picture has been obtained of certain aspects of the personal life of the user of the BlackBerry, the investigation may be unlawful.

The Court stated that on telephones equipped with the PGP application, as in the present case, several functions have been disabled. As a result, the device is only suitable for sending and receiving messages and for taking and storing notes. For example, making calls is not possible and the camera and microphone functions are usually removed or deactivated. Consequently, many aspects of the suspect's private life cannot be seen on the device because the device is not equipped for this purpose.

The Court is of the opinion that the data found on the defendant's telephone gave particular information about his contacts and business activities. The inspection of the contacts, notes and messages sent and received by the defendant only resulted in a very limited infringement of his personal privacy. This data, however, does not contain extensive information that provides a more or less complete picture of certain aspects of the defendant's personal life. Therefore, the Court concluded that the investigation of the BlackBerry telephones was lawful.

COURT RULING

The Court rejected the defence's request, as well as the requested exclusion of evidence.

Court of Appeal of Amsterdam, 14 December 2018

Keywords: use of keylogger by LEA, child sexual abuse via webcam

INTRODUCTION

In this case, the Court of First Instance in Amsterdam previously convicted the defendant for, among other offences, possession, production, distribution of child sexual abuse material, (attempt to) sexually abuse children, computer intrusion and possession of software for this purpose, extortion and swindling. The focus of the analysis below is solely on aspects of the ruling of the Court of Appeal that are relevant in the field of (investigations into) cybercrime.

FACTS

The investigation in the current case started in 2013, following the receipt by the Dutch police of two reports from Facebook. According to Facebook, an unknown person with at least 86 interconnected Facebook accounts was collecting, producing and distributing images of child exploitation. This unknown person also blackmailed dozens of underage girls, using the images in question. He also blackmailed a number of adult men. He recorded images on which these men masturbated while they assumed that they were in contact via the webcam with underage boys. He subsequently demanded money to be paid, threatening to distribute the images among the friends and family of the men. According to Facebook, false identity credentials, protected IP addresses, protected Internet connections and a Dutch IP address were used.

During the investigation, the suspect's telephone number and house address were found. With the authorisation of the judge, a keylogger was placed on two computers in the suspect's house, and microphones were placed to record confidential communications. The suspect was arrested at home in 2014. Many objects were seized, including a laptop, a desktop and a large number of hard disks. Digital investigation has shown that a number of these data carriers contained many files that can be linked to the facts.

COURT PROCEEDINGS

Use of and results from the keylogger

The defence argued that the results of the keylogger installed on the laptop and desktop computer in the defendant's home, with which screenshots and keystrokes have been recorded, cannot be used for evidence purposes because (a) the keylogger was used unlawfully, and (b) the accuracy of the keylogger's results is in doubt.

(a) The keylogger was examined before its use. The tool needed some adjustments during the installment. These adjustments included selecting which computer programs needed to be recorded, the time lapse between recorded screenshots, as well as the information to be sent to the police. According to the defence, the keylogger should therefore not only have been examined before the use of the tool, but also afterwards, to assess whether it functioned properly throughout its use (and after the adjustments had been made).

(b) The defence raised several arguments to point out that the keylogger did not function properly, including discrepancies between the text visible on the screenshots and the text recorded/forwarded by the keylogger. In addition, after the arrest of the suspect, the keylogger appeared to be no longer present on the desktop computer. The keylogger would also have recorded more than just confidential communication.

The advocate-general opposed both points, stating that the inspection of the keylogger before its installation was both possible and sufficient. Furthermore, the irregularities with regard to the keylogger did not affect the reliability of the results.

In view of assessing these arguments, the Court first took a closer look at the relevant legal provisions. The applicable 'Technical aids criminal procedure Decree' provides for the possibility of using an approved technical tool, and contains provisions relating to the inspection thereof. The inspection serves to ensure the reliability and traceability of data obtained by means of technical tools. An inspection report needs to be issued by an independent inspection service, which also can provide a declaration of approval. The Court stated that, as such an approval was issued by an inspection service for the keylogger prior to its deployment, it can be assumed that this keylogger complied with legal requirements.

The Court disagrees with the defence in arguing that this is a technical tool to which modifications must be made after installation on a computer in such a way that an inspection prior to use is not possible. After installation, the programmes to be recorded need to be ticked, a decision needs to be taken whether results should be sent, and at what time interval screenshots need to be taken. None of these preconditions mean that this technical tool would not lend itself to inspection prior to deployment. The nature and operation of the keylogger were not changed by ticking these settings in a way that could not be included in the prior inspection. The Court therefore rejects the defence that the keylogger was used unlawfully.

Subsequently, the Court assessed whether the keylogger had been used in a normal way, and whether the usefulness of the results of the keylogger had been hampered by irregularities in the deployment of the keylogger. With regard to the discrepancies between the text visible on the screenshots and the text recorded/forwarded by the keylogger, the Court referred to the statement of an expert saying that information may be missing from the technical tool, but that the technical tool will never record anything that has not happened.

Secondly, with regard to the absence of the keylogger on the defendant's computer after his arrest, the Court reasoned that the user of the computer himself has likely disabled or deleted unwanted software from his computer, including the keylogger.

Finally, with regard to the recording by the keylogger of other (non-confidential) communication, the Court stated that this additional recording could be regarded as an unavoidable side-effect of the recording of screenshots. However, this situation does not justify the conclusion that the keylogger has not been used in a normal way or that an irregularity has occurred. Therefore, in the opinion of the Court, for each of the points mentioned under (b), considered neither in isolation nor in combination with each other, a conclusion cannot be made that the results of the keylogger would not be usable for the evidence due to doubts about the reliability of these results.

Use of the accounts by the defendant and extent of the network of accounts

The Court further took a closer look at whether the defendant actually used the accounts and the extent of the network of accounts.

The offences of which the defendant was charged were committed via the Internet. The Court elaborated why the defendant was the person behind the accounts that were used for this purpose. Given the fact that the accounts refer to each other, it seemed that the accounts were used by one person and that they belong together. In this way, they constitute a network of accounts. In addition, on different occasions, a link could be made between the online accounts and the physical, real world. The Court found sufficient proof to show that the incriminating facts and the data carriers containing incriminating information were linked to each other and the defendant.

The Court continued by explaining which accounts were part of the network of the defendant. Several arguments were raised in this respect, such as the presence of an account on a data carrier seized in the defendant's house, messages sent from a Facebook-account requesting the recipient to add a Skype or

MSN account made those accounts linked, the use of similar/the same aliases and the link between the aliases and accounts used, etc.

Sexual assault of minors

The defence argued that, for a claim that sexual assault has taken place without any physical contact (as contact was via the webcam), proof needs to be given that a form of force was placed on the victim. This force must be of such an extent that the victim had no other option than to cooperate. As the victim gave no sign of resistance, this force was not an issue. Moreover, the defence stated that this type of conduct should rather be called 'sextortion'. According to the defence, no (attempt to) sexual assault had taken place.

The Court assessed whether any use of force was demonstrated by the defendant. The Court reasoned that the rationale behind Article 246 Criminal Code means that *'forcing a person to commit an act by means of threat of fact can only exist if the suspect, by means of the threat of that fact, has deliberately caused the victim to have committed those acts against her will'*. The fact that the defendant deliberately put pressure on the victim, threatening to distribute nude pictures of her to friends and family, clearly showed that the victim felt forced to commit the sexual acts. The Court also dismissed the argument regarding the terminology used as being irrelevant in this matter.

COURT DECISION

The Court convicted the defendant to the maximum penalty of 10 years and 243 days imprisonment.

Appeals Court of The Hague – criminal chamber, 19 December 2018

Keywords: phishing, 'hacking-defence', judicial authorisation for network search

INTRODUCTION

This case concerns an appeal against an earlier judgement of the Court of The Hague. Two main elements of the case, namely the judicial authorisation for the network search at a location other than where the computer has been found, and the 'hacking-defence' made by the defence, are the focus of the analysis of the judgement given below.

FACTS

By means of phishing e-mails, the defendant induced victims to log on to a fake website, where he copied their login details and placed orders in their names. The accused then switched to a different *modus operandi*, using fake invoices for outstanding payments. Here, too, victims were encouraged to provide various login details. The defendant subsequently made payments via the victims' PayPal accounts by making use of their obtained login details.

Investigation of computer – network search

During a house search, the police found a computer at the defendant's house. The judge (*'rechter-commissaris'*) had given authorisation to the police to copy/preserve data stored on digital devices in the house. In view of this authorisation for search and seizure, the public prosecutor had also requested authorisation to perform a network search from another location (police station) than the location of the house search (defendant's house). Such a network search is provided for in Article 125j of the Dutch Criminal Procedure Code.

The judge considered that, as mentioned by the public prosecutor, many files are no longer stored locally on a computer, but on the Internet. As a consequence, making an image of the computer, including searching for data stored on a network somewhere else, could take a very long time. Moreover, having the police present for a long time in a house while performing the search would be a significant intrusion into the inhabitants' privacy. Based on these considerations, the judge subsequently granted the authorisation for the network search to be performed at the police station.

DEFENCE

The defence claimed that another party misused the defendant's laptop as well as the IP addresses that were used to gain access to the internet with it, so that the criminal acts could be carried out with it (a so-called 'hacking-defence'). According to the defence, the e-mails, websites and e-mail addresses contained in the present criminal file do not belong to the defendant, and those e-mails were not prepared and sent by him. In support of this claim, the defence submitted an expert report by Fox-IT. This report describes how a hacker can gain access to a computer and the possible consequences.

COURT REASONING

1. Authorisation for the network search from the police station

The Court wanted to assess whether the authorisation granted by the judge to conduct a network search at a later time and from another location than the location in which the computer was found was legitimate. For that purpose, the Court took a closer look at the (historical) legislative process concerning Article 125j of the Dutch Criminal Procedure Code. The article was introduced in 1990, stipulating that the extended network search can be done '*from the place where the search is taking place [...]'.* The article was amended in 2006 to include searches in webmail or cloud environments. The legislator reiterated at that time that the network search should be done from the place of the house search.

The Court of Appeal therefore deduced from the legal history that the legislator did not want to offer any room for the application of a network search at a location other than (at the time of) the location of the search. The Court also inferred that the network search cannot take place after the actual moment of seizure of the computer, and thus at a later moment and from another location.

If the network search takes place at the police station, the search will take place at a (much) later time than the time of the search itself. In that case, certainly in the current era of extensive (Internet) interconnectivity between automated works, a strong probability exists that at a later stage of the network search, data will be obtained that were not yet available at the time of the initial search. However, as discussed above, the legislator considered the latter to be undesirable in the context of network searches.

The Court of Appeal concluded that the network search as referred to in Article 125j of the Code of Criminal Procedure cannot be carried out at a location other than the location of the search. This conclusion also leads to the opinion that the judge could not reasonably have reached his opinion about the authorisation he had granted, as he had thereby gone beyond the relevant legal framework. The subsequent search for a network, and the associated interference into the private life of the accused, can therefore also not be regarded as being 'provided for by law' as referred to in Article 8 ECHR. As a consequence, the Court concluded that the authorisation should not have been granted and entails an irregularity in the form. The Court, however, did not connect any consequences to it.

2. 'Hacking-defence'

In the present criminal case, the content of the factual findings with regard to the digital evidence is not disputed, nor is its qualification as a criminal offence. However, a so-called 'hacking-defence' is

conducted, which in short boils down to the fact that these punishable acts were not carried out by the defendant himself or with his knowledge, but by a (mostly unknown) third party who had gained access to his computer.

The Court started by making some general considerations regarding 'hacking-defences'.

In any case, whenever a 'hacking-defence' is raised in a case, it is not required as proof to exclude the possibility that the concerned computer has been hacked.

In assessing whether a 'hacking-defence' is more or less plausible, various factors may be taken into account, including, but not limited to:

- the presence or absence of digital traces relating to the actual or potential intrusion by third parties into the computer in question;
- the level of physical and digital protection of the computer against third-party use/(digital) intrusion;
- the presence or absence of digital traces (and/or other facts and circumstances) from which can be deduced, for example on account of the content, who (also) was the user of the computer at or around the time of the commission of the criminal conduct;
- the extent to which, and the moment at which, the defendant has cooperated in further investigation into his defence;
- other facts and circumstances that point to a special (substantive) involvement of the defendant or a third party in the behaviour committed on or via the computer in question;
- witness statements concerning the use of the computer in question by the defendant or by third parties; and
- the presence or absence of a motive for third parties to hack into the computer of the defendant.

The Court then continued by assessing such factors in the current case. To begin, the Court stated that the defence did not give any concrete factual substantiation for the 'hacking-defense', but rather made general statements based on the report of Fox-IT. Moreover, the defendant was not willing to provide the password of the router in his house, made at the request of the police. In addition, when requested to provide the PIN code of his mobile telephone, he provided several times, intentionally or unintentionally, an incorrect code, which permanently locked the mobile telephone. In doing so, the defendant showed a lack of support for an alternative interpretation of the facts, which would have been be beneficial for him. Lastly, several actions, which could allegedly have been carried out by the hacker, could be attributed to the defendant. As a result of the foregoing arguments, the Court concluded that the 'hacking-defense' was not plausible and therefore rejected it.

COURT RULING

The Court of Appeal convicted the defendant of (attempted) fraud, theft, computer intrusion, the possession of malicious software and the acquisition and possession of computer passwords to commit computer intrusion.

Court of Rotterdam – pre-trial chamber, 22 February 2019

Keywords: end-to-end encryption, LEA logging in to Telegram account of suspect

INTRODUCTION

This ruling concerns a pre-trial decision of the Court of Rotterdam. In an earlier decision, the judge *('rechter-commissaris')* had rejected a request from the public prosecutor to give authorisation to the police to gain access to a suspect's Telegram account and subsequently copy the data found on the servers. The public prosecutor appealed this decision.

FACTS

The defendant is under investigation for the distribution of malware (phishing software) that was used to gain access to several banks' and companies' customers' login details. He sent phishing text messages to the customers with the objective of getting them to visit the phishing website so that he could obtain their login credentials.

During a house search, the defendant's mobile telephone was found. Given the other evidence found, it is plausible that the defendant made use of that telephone and used it to communicate, among other things, by means of Telegram. Messages sent via a Telegram-account are, however, end-to-end encrypted and can therefore only be 'readable' by using the account through which they are sent/received in combination with the Telegram-software. The police officers were not able to break the encryption of the telephone and gain access.

In addition, Telegram does not store or process the contents of the data itself, but rather random sequences of symbols that have no meaning without the keys, which they do not have. Moreover, Telegram may not voluntarily provide the data following a production order, even if they have the data available. Consequently, the public prosecutor did not want to request the data from the service provider, but chose to gain direct access by logging in to the Telegram account of the defendant. The Court was therefore asked to assess whether the facts of the case justify the authorisation to gain such access.

COURT REASONING

The Court first assessed whether the conditions of Article 126ng, second paragraph, of the Dutch Criminal Procedure Code were met. This article stipulates that a prosecutor can order a service provider to provide data, stored on the server of that provider, after authorisation of a judge. The Court found that the breach of privacy (confidential Telegram account) of the defendant was justified in view of the weight given to the role of the financial payment system and the trust that citizens should be able to have in financial and communication services. Therefore, the authorisation, on the basis of Article 126ng, second paragraph, can in principle be given.

The Court continued by explaining what the legislator had in mind when drafting Article 126ng, second paragraph, of the Dutch Criminal Procedure Code. The goal was for the prosecutor to be able to have access to all content of the stored communication. The legislator could not, however, take into account

the future technological developments and business processes of service providers, and thus could not foresee (the consequences of) end-to-end encryption.

Precisely because of the consequences of end-to-end encryption *(see facts above)*, the prosecutor does not want to request the data from the service provider, but rather to gain direct access to the data by logging in to the Telegram account of the defendant.

The Court reasoned that logging in to the account of the defendant via the web version of Telegram can be justified under certain circumstances, namely when, according to the provider, the data is not available in another readable format. Therefore, such a way of gaining access is permitted. Moreover, the Court also pointed out that the newly drafted legislation *(see previous chapter)*, introducing additional special methods for investigating in a digital environment, will allow for even more far-reaching forms of investigation.

The specific server on which the data are stored, as well as the location of that server, is unknown. Therefore, whether the data are located in a foreign jurisdiction, and whether this situation may constitute a breach of sovereignty of another State, remains unclear. In this respect, the Court ruled that there is no reason to assume that such a breach will take place. In addition, no concrete procedure is available to request international legal assistance with the objective of receiving the data.

COURT RULING

The Court annulled the decision of the judge. In the authorisation to be granted, the chamber of appeal imposed a limit (in time) on the information that may be taken into account.

Supreme Court, 9 April 2019

Keywords: possession and use of malware, insufficient proof of computer intrusion

INTRODUCTION

This case concerns an appeal for annulment of a judgement pronounced by the Court of Appeal of The Hague in November 2016.

PROCEDURE AND RULING COURT OF APPEAL

The Court of Appeal ruled that proof had been provided that the defendant had intruded intentionally and unlawfully into an automated system for the storage or processing of data of a company, in which he gained access by means of a technical intervention by using (among other things) a software program (Acunetix).

This conclusion is based on evidence received from witness statements by an Information Security Officer of the company, who had received an e-mail from another company that monitors their website via an intrusion protection system. The latter company informed the Officer that an attack had been performed on the website. They also provided a log file containing the data of the attack carried out. In this log file, one could see that the web vulnerability scanner called 'Acunetix' was used. The Acunetix tool searched for several vulnerabilities in the website, some of which were blocked. The Officer also noticed that some attacks were performed with the Permit action. He stated that 'because of this permission it was not inconceivable that a successful attack had taken place'.

Another attack on the website was performed a few days later. A log file was provided showing that Cross Site Scripting and Directory Traversal attacks were carried out on the website. The log also shows that several attempts with regard to Cross Site Scripting were blocked and that Directory Traversal was used to try to get into the root of the server. However, the extent to which this attack had been successful

was not yet known. The Officer claimed that, since several attacks were carried out with the Permit action, a successful attack could have taken place.

The Court therefore concluded that the defendant had intruded into the automated system and found him guilty of the offence.

SUPREME COURT REASONING

The plea alleges that the evidence of the indictment, as far as it implies that the defendant had intruded into a part of an automated system, cannot be deduced from the evidence used in Court.

The Supreme Court took a closer look at the relevant provision in the Dutch law, Article 138ab of the Criminal Code. The term 'penetrated', used in the indictment and the evidence supporting the Court's ruling, should have the same meaning as the term used in Article 138ab of the Criminal Code. This article stipulates that:

'[…] Intrusion occurs, in any case, if access to the system is obtained:

a. by breaking through a security system,
b. by technical means,
c. using false signals or a false key; or
d. by assuming a false capacity.'

The Supreme Court subsequently concluded that from the evidence, one cannot simply deduce that the defendant had indeed intruded into an automated system or into a part thereof. The contested decision is not well founded according to the requirements of the law. The mere circumstance that the defendant examined the website of the company for vulnerabilities by means of a scan program, some of which were blocked, and that, as a result, 'it is not inconceivable that a successful attack has taken place' is not sufficient for this decision.

SUPREME COURT RULING

The Supreme Court annulled the judgement of the Court of Appeal concerning the abovementioned decision.

➢ UK

Appeal Court, High Court of Justiciary, Redpath v Her Majesty's Advocate, [2019] HCJAC 38, 14 June 2019

Keywords: assessment level of knowledge required to prove possession of indecent images of children

INTRODUCTION

On 11 June 2018, the appellant was convicted of having indecent photographs of children in his possession, contrary to the Civic Government (Scotland) Act 1982 Section 52A(1).

The appellant was a 63-year-old retired electrician. He had an interest in repairing computers and had considerable quantities of computer hardware in his house. Much of this equipment was seized, and three items contained the material that ultimately resulted in his conviction.

The appellant appealed the decision. The case involved a technical assessment of the level of knowledge required in a charge of possession of indecent images of children.

BACKGROUND AND FIRST INSTANCE - EVIDENCE

The appellant testified that he had not known that any indecent images were present on the hardware seized. He often scavenged for computer parts. Third parties often left equipment with him if they had asked him to repair something that turned out not to be economically viable. He did not check all accessible material on such equipment. The appellant's partner gave evidence that she had never seen the appellant viewing indecent images of children.

The sheriff stated that 'possession' required 'knowledge and control'. Knowledge involved 'awareness; knowing of something's existence'. The sheriff described how the Crown (prosecution) had approached this issue by saying that the appellant 'had knowledge of all the accessible images' given: (a) their accessibility; (b) the appellant's skills with computers; and (c) the images were found on a number of the discs or cards.

APPEAL

The defence stated that insufficient evidence had been provided to prove 'knowledge of the images'. The appellant argued that he did not have sufficient knowledge of what was on the computer to 'possess' the images. The appellant's knowledge of computers was irrelevant, as was the fact that the images were found in different units. No evidence was supplied that the devices could work on the computer in the appellant's house.

The Court first needed to assess what the term 'knowledge' entailed: if images were on the hard drive of a person's computer, possession could be inferred. If images were on unlabelled discs, which were not otherwise linked to an accused, and no device was seized in evidence that proved capable of accessing the images, possession was more difficult to establish.

The Court concluded that it is sufficient for the Crown to prove that the appellant was in possession of data stored on computer discs that could produce photographs of some kind, with no need for the Crown to prove that the appellant had knowledge of the nature of the images to which the data would convert. The Crown must prove knowledge of the existence of the items that were in the appellant's control (i.e. data convertible to images) but not his knowledge of the quality or content of the items. According to the Court, sufficient evidence was provided from which an inference could be drawn that the appellant was aware that he had a number of discs containing data. Some of the data related to the appellant's personal life, and its existence must have been known to him. The volume of such data over a series of discs, including those containing images, the possession of which was not criminal, would be sufficient for the inference to be drawn. In addition, a glance at some of the file titles on the disc would indicate the nature of their content. Thus, the Court concluded that the requisite knowledge was established.

COURT DECISION

The Court rejected the appeal.

➢ Norway

Supreme Court of Norway, case HR-2019-610-A, 28 March 2019, Norway
Keywords: third-party-search by LEA of Norwegian company, access to data abroad, Norwegian territorial jurisdiction

INTRODUCTION

This case concerns a third-party search at the Norwegian company Tidal Music AS in Oslo. Tidal is a group of companies with establishments, among other places, in the USA and several European countries that offers music streaming to subscribers. Tidal Music AS is a Norwegian company in this group. On 3 December 2018, a warrant was requested from Oslo District Court to conduct a third-party search at Tidal's office in Oslo. The request set out that the suspicion is against an 'unknown perpetrator', and that it concerns computer fraud in the form of manipulation of the numbers for some tracks to influence the calculation of royalties to certain rights holders. According to information provided, Tidal Music AS was not charged with or suspected of anything unlawful. The police wanted to access information assumed to shed light on criminal acts suspected to have been committed. The request also included the relevant data carriers and electronically stored information to which the person in question had access, including online data carriers in the form of servers, etc.

BACKGROUND AND FACTS

A search was conducted at the company's office in Oslo. Tidal opposed the search and any seizure involving downloading from the company's terminals in Norway of data stored by Tidal on servers abroad. More specifically, the dispute concerned 'source codes' that during the search – assisted by the technical director of Tidal – were downloaded from a server in the USA belonging to Amazon Web Services.

Moreover, Tidal disagreed with the extraction of e-mails from the technical director's Google account. This data is stored on servers abroad; the exact location is unknown. The downloading was commenced upon the police's order, but the process turned out to be lengthy. The police therefore asked the owner of the e-mail account to copy the data onto a hard drive that could be picked up at Tidal's office later. Due to the disagreement with regard to the search, the data was not surrendered to the police.

Tidal subsequently appealed the district court's decision to the Court of Appeal. Tidal argued that the police were not allowed to download from data terminals at the company's office in Oslo digital material that the company has stored abroad, as such a coercive measure falls outside the jurisdiction of Norwegian authorities.

The Court of Appeal dismissed the appeal, as it found that the conditions for a search were met under section 192 subsection 3 (3) of the Criminal Procedure Act. The Court also found a reasonable cause for suspicion and a high probability that evidence could be secured by a search of Tidal's data. As for the issue at stake – whether the search could be conducted despite the data being stored abroad – the Court of Appeal found that this coercive measure had to be considered taken in Norway, by a Tidal employee – upon an order – giving the police access to servers abroad from the company's office in Norway. Hence, no question arose of an intrusion into the server abroad. The Court also emphasized that any seizure of data on the server would be executed from Norway.

Tidal subsequently lodged an appeal with the Supreme Court.

SUPREME COURT REASONING

The Supreme Court first assessed the national legal basis for the requested measure. In the Court's view, nothing in the general interpretation of section 192 of the Criminal Procedure Act prevents the search from being conducted in the manner accepted by courts of lower instances.

The Court continued to look at international law and concluded that no legal basis was established under any treaty for conducting a search in a case such as this one. Moreover, under international law, states may only exercise coercion in their own territory. However, jurisdiction over information stored in the cloud becomes more difficult to establish. The Court therefore took a closer look at Norwegian and other countries' case law, and concluded that no custom under international law exists in this area, and case law that may serve as guidance is scarce. Yet, the Court stated that they found interesting that many States, in practice, seem to accept a search such as the one in the case at hand. In addition, no information exists on inter-state reactions to a country's authorities accessing data stored in another State through coercive measures against legal entities in its own territory.

The Court then continued by assessing the search of Tidal's data and stated that the coercive measure was initiated on Norwegian soil, and the data is made available through a coercive measure against a Norwegian company with an office in Norway, meaning that Norwegian authorities are not, on their own, intruding into data stored abroad. The search also only involved access to information the company had stored itself. The data was not altered and remained on the server abroad. According to the Court, such a search cannot affect another State to an extent that it constitutes a violation of the principle of sovereignty. Consequently, the Court of Appeal had correctly applied the relevant legal standards.

COURT DECISION

The Supreme Court dismissed the appeal.

3.2. Other court rulings in brief

- **Regional Court in Karlsruhe, 4 KLs 608 Js 19580/17, Germany**

  Date: 19 December 2018

In July 2016, a shooting took place in Munich. An 18-year-old killed nine people, injured five other people and then committed suicide. The perpetrator had bought the pistol and ammunition on the Darknet. The man who had sold him the weapon and ammunition was already sentenced to seven years' imprisonment.

This case concerned the administrator of the Darknet platform, which brought the seller and the killer together.

The Regional Court considered that sufficient proof had been demonstrated that the defendant, as administrator of the online platform he controlled, had enabled the perpetrator to acquire the weapon used in the commission of the crime. Therefore, the administrator was convicted of aiding and abetting numerous crimes related to illicit trafficking and acquisition of weapons, in conjunction with negligent homicide in nine cases and negligent bodily injury in five cases. The defendant had also been convicted of numerous drug-related offences. He was sentenced to a six-year term of imprisonment.

- **Court of Zeeland-West-Brabant, Case 02-665264-18, Netherlands**

  Date: 17 May 2019

In this case, e-mails were sent on behalf of Rabobank, asking victims to apply for a new debit card. They were directed to a website on which they could apply. In reality, a new registration for the Rabo Banking App was carried out using the data entered. The organisation behind this fraud applied for a new debit card, made sure it was intercepted and then emptied the bank account using money mules. The defendant was found guilty of theft of a debit card and withdrawal of cash from a victim's account (theft) and from money mule accounts (money laundering). In view of his role, the suspect was also convicted of participating in a criminal organisation and was sentenced to 240 hours' community service.

- **Court of Rotterdam, Case 10/960098-15, Netherlands**

  Date: 26 July 2018

Two brothers were convicted for contaminating computers with ransomware. This conviction was the first in the Netherlands regarding ransomware. They used Coinvault ransomware to infect thousands of computers, which were completely controlled with a command-and-control server. They demanded EUR 250 in Bitcoin to decrypt the infected devices. Without payment in Bitcoin, regaining access to encrypted data was impossible. The police found them through their IP address. They were convicted of extortion, computer intrusion and damaging (making inaccessible) data stored on a computer.

- **HMA v Matthew Bell, UK**

  Date: 25 July 2019

In this case, the accused was involved in the live-streaming of sexual abuse in the Philippines while residing in his home in Scotland. He was paying less than EUR 1 for each abuse to be committed. The offences of which he was convicted include conspiracy to rape and sexual offences against children.

The case was a first for a number of reasons. For the first time, a person was convicted of live-streaming the sexual abuse of children. The police relied almost entirely on the evidence of the offences that the accused had recorded. In addition, the identities of the victims are still unknown. Moreover, issues were encountered during the investigation, involving the transmission of intelligence from Terres des Hommes to the National Crime Agency in the UK and delay in them passing that intelligence on to Police Scotland. During this period, the accused continued to offend.

The accused pled guilty, so no trial took place and no judicial consideration was made of the charges used to prosecute. The judge in sentencing did explicitly state that he was sentencing as though the accused had committed the offences in person.

UK EJCN member: Essentially, the domestic sexual offences law was tested to see if such behaviour committed while live-streaming could be prosecuted. As with previous online sexual offences, this test has been successful without any extensive discussion by the Court.

- **Constitutional Court No. II., US 78/2019-55, Slovak Republic**

  Date: 23 May 2019

Although this case was not particularly linked to cybercrime, this judgement of the Constitutional Court may have a significant impact.

The complaint was lodged by a journalist who alleged restrictions of certain freedoms because the police took her mobile telephone with the objective of copying data believed to be relevant in the murder case of a journalist and his spouse. Two important issues are covered by the judgement: (a) the confirmation of the legality of the procedure (the journalist provided the mobile telephone voluntarily) and legal grounds for such conclusion and (b) the question of computer data.

The Supreme Court considered the following: if a mobile telephone was taken from a person or was provided by a person in the context of criminal proceedings; if it was seized during a house search or search of premises or land; or if it was seized as a material footprint in a crime scene inspection, an order for seizure and disclosure of data from telecommunications is not needed. However, the Supreme Court also noted that despite the common technical features of the computer and mobile telephone, the data stored in a mobile telephone are not considered computer data under Section 90 of the Code of Criminal Procedure. The Constitutional Court noted that the Supreme Court did not consider traditional mobile telephones (used for telephone communication, MMS and SMS) and smartphones that provide more functions (as was in the situation with the journalist's mobile telephone). The Constitutional Court, referring to information from books and the Internet, concluded that the mobile telephone (that was involved in the case) obviously has characteristics of a computer and contained computer data. Therefore, the arguments cannot lead to a conclusion that the order was contrary to the Constitution.

Slovak EJCN member: *The latter arguments of the Constitutional Court may have a significant impact on the practice since computer data is not defined by Slovak legislation.*

- **Supreme Court of Switzerland, 1B_29/2017**

  Date: 24 May 2017

Anyone who uses a derived Internet service offered by a foreign company via a domestic Internet access does not 'act abroad'. Even the mere fact that the electronic data of the relevant derived Internet service are managed on servers (or cloud storage media) abroad does not make an online search carried out from Switzerland in accordance with the law appear to be an inadmissible investigative act on foreign territory (in the sense of the practice outlined).

- **European Court of Human Rights, case Rook v. Germany, ECHR 282 (2019)**

  Date: 25 July 2019

In the case of Rook v. Germany, the European Court of Human Rights held that no violation of Article 6 § 1 (right to a fair trial), taken together with Article 6 § 3 (b) (right to adequate time and facilities for the preparation of the defence) of the European Convention on Human Rights had taken place.

The case concerned the fairness of criminal proceedings in which approximately 80 000 items of telecommunications surveillance data had been produced and 14 million electronic files seized.

The Court particularly found that the defence had had sufficient access to the file and sufficient time to acquaint itself with the telecommunications surveillance data and the electronic files to prepare for the trial. The proceedings, considered as a whole, had therefore been fair.

Please find the link to the press release and full judgement here.

IE EJCN member: The fact that the defence did not have sufficient time to examine the file is a frequent complaint in common law jurisdictions.

4. Data retention developments in Europe

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

4.1. Developments at EU level

4.1.1. European Court of Justice

- **Case C-511/18**

On 3 August 2018, the French Conseil d'Etat lodged a request for a preliminary ruling from the CJEU. The following questions were referred to the Court:

(1) *'Is the general and indiscriminate retention obligation imposed on providers on the basis of the permissive provisions of Article 15(1) of Directive [2002/58/EC] of 12 July 2002 1 to be regarded, against a background of serious and persistent threats to national security, and in particular the terrorist threat, as interference justified by the right to security guaranteed in Article 6 of the Charter of Fundamental Rights of the European Union and the requirements of national security, responsibility for which falls to the Member States alone pursuant to Article 4 of the Treaty on European Union?*

(2) *Is the Directive of 12 July 2002, read in the light of the Charter of Fundamental Rights of the European Union, to be interpreted as authorising legislative measures, such as the real-time measures for the collection of the traffic and location data of specified individuals, which, whilst affecting the rights and obligations of the providers of an electronic communications service, do not however require them to comply with a specific obligation to retain their data?*

(3) *Is the Directive of 12 July 2002, read in the light of the Charter of Fundamental Rights of the European Union, to be interpreted as making the legality of the procedures for the collection of connection data subject in all cases to a requirement that the persons concerned are duly informed once such information is no longer liable to jeopardise the investigations being undertaken by the competent authorities, or may such procedures be regarded as lawful taking into account all the other existing procedural guarantees, since those guarantees ensure that the right to a remedy is effective?'*

On 10 September 2019, a hearing was held in this case, as well as case C-520/18 (Belgium). Delivery of the ruling will follow at a later time.

- **Case C-746/18**

On 29 November 2018, the Estonian Riigikohus referred the following questions to the CJEU for a preliminary ruling:

(1) *'Is Article 15 (1) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 20021 in the light of Articles 7, 8, 11 and 52 (1) of the Charter of Fundamental Rights of the European Union to be interpreted as meaning that, in criminal proceedings, access by public authorities to data enabling the place of dispatch and reception, the date, time and duration, the nature of the communication service, the receiving device and its location in connection with a telephone or mobile telephone communication of a suspect, constitutes such a serious interference with fundamental rights as guaranteed by the said articles of the Charter that such access is prevented in the field of prevention, investigating, detecting and prosecuting criminal offenses should be limited to the fight against serious crime, irrespective of the period for which the authorities have access, relate?*
(2) *Is Article 15 (1) of Directive 2002/58/EC based on the principle of proportionality, as set out in paragraphs 55 to 57 of the Court's judgment of 2 October 2018 in Case C-207/16, to be interpreted as meaning that: if the amount of data referred to in the first question to which the public authorities have access (both in terms of the nature of the data and in view of the period in question) is not large, the associated interference with fundamental rights may in general be justified by the objective of preventing, investigating, detecting and prosecuting criminal offenses and that, as the amount of data to which the public authorities have access, the more serious the offenses to be combated by the interference should be?*
(3) *Does the requirement laid down in the judgment of the Court of 21 December 2016 in Joined Cases C-203/15 and C-698/15, operative part 2, mean that the data access of the competent public authorities is subject to prior review by a judicial authority or an independent administrative authority, that Article 15 (1) of Directive 2002/58/EC must be interpreted as meaning that the Public Prosecutor conducting the investigation and is thereby required by law to act independently and is bound solely by law and in the context of the investigation investigates both the offending and relieving circumstances for the suspect, but later acts as a public prosecutor in the judicial proceedings, can be regarded as an independent administrative authority?'*

On 15 October 2019, a hearing was held in this case. The delivery of the preliminary ruling is expected next year.

4.1.2. Council of the European Union

On 6 June 2019, the Council adopted conclusions on the retention of data for the purpose of fighting crime.

The Council repeated that data stemming from telecommunications operators and service providers is very important, enabling judicial, law enforcement and other authorities to successfully investigate

criminal activities. Therefore, securing availability of data is of utmost importance. Data retention should, however, be guided by the need to protect fundamental rights and freedoms.

The Council underlined that the existence of different legal regulations in the area of data retention may cause limitations in cooperation and information exchange between competent authorities in cross-border cases. In addition, relevant case law at national and EU levels in relation to data retention must be followed closely.

The Council invited the Commission to gather further information regarding the needs of competent authorities to have data available. It furthermore tasked the Commission to organise targeted consultations as part of a comprehensive study on possible solutions for retaining data, including the consideration of a future legislative initiative.

Please find the link to the press release and Council conclusions here.

4.2. Other national developments

➢ Ireland

Judgement Dwyer v Ireland, European Court of Human Rights, 6 December 2018

Arising from a murder conviction in which traffic and location data from mobile telephones was a central part of the evidence, a challenge was raised to the provisions in the Communications (Retention of Data) Act 2011 for the retention of telephone data and access to such data by the police. Drawing particularly on the judgements of the Court of Justice of the EU in the cases of Digital Rights Ireland (C-293/12) and Tele2Sverige (C-203/15), the plaintiff argued that Irish legislation is inconsistent with EU law and the ECHR.

The High Court found that the 2011 Act provides for retention of data that is general and indiscriminate, and that this provision is precluded by EU law. It also found that access to data that is retained should only be granted by an independent administrative authority with adequate safeguards, which is not the situation in circumstances in which a police agency determined when access to that data should be permitted. The Court did say that the judgement only concerned retention and access for the prevention, detection, investigation or prosecution of serious crime and not for the safeguarding of the security of the State and the saving of human life. The Court has issued a declaration that Section 6(1)(a) of the 2011 Act is inconsistent with EU law and placed a stay on the enforcement of the declaration pending the lodging of appeal papers and adjudication on a continued stay by the Court seized for the appeal.

Please find the link to the full judgement here.

➢ Netherlands

A new legislative proposal is still pending in the Netherlands. It will likely still take quite some time for a new act to enter into force.

➢ Sweden

On 1 October 2019, a new law on data retention entered into force in Sweden. The new rules concern the retention of data. The rules regarding the judiciary will remain the same as before, but the rules regarding access to data for intelligence purposes will change.

For telephony and messaging, only communication via a mobile network access point should be retained. No data will be retained on telephony or messaging that takes place in the fixed-line (landline) telephone network or through fixed Internet access. Traffic data will be retained but the obligation to retain will be limited to data on who contacted whom and at which time. Location data at the beginning and end of a call will be retained, but no other location data. For unregistered prepaid phone cards, information about communication equipment and initial activation will be retained.

For Internet access, the retention obligation includes data that make identification of the subscriber or registered user possible: IP addresses and other technical data necessary to identify the subscriber or registered user, time data for logging in and out of the service providing Internet access, subscriber information and data identifying the equipment where the communication is finally separated to the subscriber.

The time period for data retention varies from two months (location data of calls) to ten months (data on Internet access). For all other data, the retention period is six months.

➢ UK

The Data Protection Act 2018 (DPA 2018) came into force on 25 May 2018. It implements the General Data Protection Regulation (GDPR) as well as supplementing and bolstering it.

Under the fifth data protection principle of the GDPR, personal data cannot be kept for longer than necessary. However, no specific time limit is set. How long you retain data will depend on the purpose for holding the data.

The Data Retention and Acquisition Regulations 2018 (the Regulations) entered into force on 31 October 2018 (some of the provisions did not enter into force until 2019). The Regulations concern the retention of communications data by telecommunications and postal operators and the acquisition of communications data by public authorities.

'Communications data' means data concerning a communication transmission, but not the content of the communication. For example, communications data includes the method of communication and the sender and receiver of the communication, but excludes what was said or written.

The Regulations were introduced following the Court of Justice of the European Union's (CJEU) ruling on the Tele2 and Watson case in 2016, which found that the scope of the UK's data retention regime was too wide to be compatible with EU law. The CJEU found that the retention and acquisition of communications data can only be justified if: (1) the objective is fighting serious crime, (2) only data that is 'strictly necessary' is retained, and (3) the retained data is kept within the European Union. Independent administrative or judicial authorisation for the retention and acquisition of communications data should also be obtained. The CJEU therefore required the UK to limit the scope of its data retention regime.

In response, the UK government introduced the Regulations, amending the Regulation of Investigatory Powers Act 2000 (RIPA) and Parts 3 and 4 of the Investigatory Powers Act 2016 (IPA), which provided for the interference of privacy in the interests of national security.

The amendments to the Acts include, for example, a new power for the Investigatory Powers Commissioner to authorise communications data requests made by a public authority; allowing for internal authorisation of requests in cases with urgency or in cases of national security; and a new threshold of 'serious crime'.

The Regulations will directly affect telecommunications and postal operators as the potential subjects of retention notices issued by the Secretary of State. A retention notice may relate to a particular operator or any description of operators and require the retention of all data or any description of data for up to 12 months. It may also relate to data that is not yet in existence. Public authorities will require separate authorisation to subsequently access this data.

The bodies that are able to access retained data as well as the justifications for accessing retained data in the UK are listed in the RIPA.

➢ Switzerland

Judgement 1C_598/2016, Supreme Court of Switzerland, 2 March 2018

In this judgement, the Supreme Court analyzes the conformity of the legal situation in Switzerland with the jurisprudence of the European Court of Human Rights and the court decisions of the Court of Justice of the European Union.

The Court assessed that the Swiss provisions regarding data retention are in line with the Convention for the Protection of Human Rights and Fundamental Freedoms.

Please find the link to the full judgement here.

5. Topic of interest

Handling of virtual currencies in criminal investigations and proceedings

Introduction

In the current digital age, electronic devices are increasingly used in our daily lives, as these tools are often applied to replace traditional ('offline') ways of conducting activities and daily business, both in professional and private contexts. The emergence of virtual currencies, as a 'new' form of non-cash means of payment, is one of those developments that has brought about a new manner of paying for goods and services online. More and more people are using virtual currencies to make financial transactions online instead of paying via the (regulated) monetary banking systems.

However, a number of important differences between the two payment systems exist. Transactions with virtual currencies are more difficult to trace back to physical persons, as they are anonymised and encrypted. In addition, virtual currencies are not regulated in the same way as traditional monetary systems, a situation that gives more freedom to the users in making transactions. Although virtual currencies provide users with a certain level of anonymity, privacy, security and freedom, they do, in combination with the lack of a proper criminal legal framework, create more problems for judicial and law enforcement authorities in investigating crimes that involve the use of virtual currencies. Indeed, tracing virtual currencies, identifying owners and recipients, and gaining access to wallets are often more challenging and (technically) resource-intensive than investigating traditional currencies.

This chapter will not go into technical details on the use of virtual currencies. Rather, it will focus mainly on the legal framework applied by judicial and law enforcement authorities when conducting investigations into virtual currencies, as well as practical experience, possibilities and challenges encountered in relation to seizures and further handling of virtual currencies throughout investigations and prosecutions.

The information presented in this chapter was gathered via a questionnaire distributed to the experts of the EJCN. In total, replies from EJCN members of 18 countries were received, including two non-EU countries.

General legal framework on virtual currencies

The experts were asked about the **legal nature of virtual currencies** in their country. The replies differed significantly, either because of the lack of a (clear) legal definition or because of what they are considered to be, or the way in which virtual currencies are defined and by which laws. Many countries replied that the legal nature is unclear or that no specific legal definition of virtual currencies exists. As a result, virtual currencies are not officially recognised. In several countries, virtual currencies are considered to be dematerialised assets or assets with monetary value. In one country, virtual currencies are considered to be money.

Nine countries have defined virtual currencies in specific legal provisions or apply a description of the term, stemming from tax or anti-money laundering laws. Only a few countries have virtual currencies defined or mentioned in their criminal (procedure) law. However, out of those nine countries, several explicitly did not grant legal status to virtual currencies or recognise them as a legal means of payment. Some even still consider the legal nature as controversial, given the fact that the term is only defined or clarified in a specific area of the law, such as for the financial sector.

Virtual currencies are defined or described in the abovementioned provisions or guidelines as:

- intangible property;
- assets;
- computer data that holds a value at a particular time;
- special electronic data;
- a digital representation of value, not issued by a central bank or central authority, used as a means of exchange to trade goods and services and transferred or stored electronically, which is not necessarily related to fiat currencies; or
- a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes.

The latter definitions are derived from the fifth Anti-money laundering Directive[1] of the FATF, which defines virtual currencies as *'a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically*.' This Directive should be implemented in the EU Member States by 10 January 2020. Together with Directive (EU) 2019/713[2], which provides the same definition of virtual currencies, these instruments, once implemented in domestic legislation, may provide somewhat more harmonisation in the (existence of) legal definitions of virtual currencies across the European Union.

Most countries do not have any specific (criminal) **legal provisions on virtual currencies**, and apply general provisions of criminal law on seizure and asset recovery or anti-money laundering and terrorism financing laws. Such anti-money laundering laws make virtual currency exchange and storage services subject to supervision and oversight from a competent authority and stipulate obligations for them to report suspicious transactions, disclose information and possibly track financial transactions. Two countries have specific criminal law provisions on seizure of electronic data used for payment (Hungary) and obtaining financial information from virtual currency services (Slovenia). In Luxembourg, two virtual asset entities, Bitstamp Europe S.A. and bitFlyer Europe S.A., were regulated by law as payment institutions, therefore falling under the provisions of the anti-money laundering and counter-terrorism financing legislation. Three countries mentioned upcoming amendments to their criminal procedure or anti-money laundering laws in the near future.

In several countries, practitioners have already successfully frozen and seized virtual currencies, despite the absence of specific criminal legal provisions for virtual currencies. Although practitioners in some countries have not (yet) encountered any difficulties or obstacles, for some, the application of such general provisions for seizing virtual currencies, or the lack of guidelines, has proven to be challenging.

The following **challenges** were mentioned:

- Due to the unclear legal nature of virtual currencies, deciding on the appropriate legal measure for seizure is more difficult;
- Pseudonymous worldwide transactions make establishing jurisdiction and prosecution difficult;
- Determining the value of the proceeds of crime is more cumbersome because of the volatility in prices of virtual currencies (value determined at which point in time?); and
- Establishing that the virtual currencies are proceeds from criminal activities, and, linked to this determination, ownership versus possession.

[1] Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU.
[2] *See* Legislation chapter, p. 3.

Given the lack of specific legal provisions and the complexity of handling and seizure of virtual currencies, many countries do have guidelines or handbooks available with guidance on the handling of virtual currencies for law enforcement and/or prosecution services.

Handling of virtual currencies in criminal investigations

A) Seizure of virtual currencies

Most countries apply the general criminal procedure rules on seizure when a need to seize virtual currencies arises. Only the Hungarian Criminal Procedure Code has specific stipulations determining that seizure shall be carried out by any technical means, as a result of which the virtual currencies are secured and available only for the authorities.

The actual **procedure for the seizure**, as well as the means used, can differ from country to country, and even domestically, between law enforcement offices. A prosecutor or investigating judge often issues the seizure order, following which the actual seizure is carried out by the police, who are sometimes assisted by IT experts. In a few countries, prosecutors can also perform the seizure. The seizure is performed by transferring the virtual currencies to wallets or pre-generated seizure addresses. This transfer is controlled by the police or prosecution office. They are then also responsible for the further management and secure storage of the seized virtual currencies.

In most countries, the seized virtual currencies are transferred to LEA wallets. In a few countries, judicial wallets are used. In other countries, no specific rules are in place to determine whether to use an LEA or judicial wallet. In one country, wallets are not used in the sense that the seized virtual currencies are immediately exchanged in traditional currency and subsequently transferred to a bank account of the State Treasury. Different types of LEA wallets can be used: offline or physical wallets (paper/nano-ledger/hard drive/USB stick), online wallets, or a combination of both offline and online wallets, or the choice of wallet can depend on the type of virtual currency seized.

Many countries do not have an agreed procedure within LEA or prosecution offices for the **management of virtual currencies**, i.e. seizure as well as further handling. Even if such an agreed procedure is applied within a certain police office, it may well differ from procedures applied in other offices in the same country. Only a few countries have implemented such virtual currency management procedures in a unified way at national level.

When seizing and storing virtual currencies, authorities can be confronted with many different **obstacles**. The following obstacles were mentioned:

- The many different ways to store and manage virtual currencies make it difficult to locate and identify existing virtual currency accounts, wallets or ledgers;
- Identifying the type of virtual currencies;
- Gaining access to a wallet;
- Encryption obstacles (private keys) and willingness of owner of the virtual currencies to cooperate in view of gaining access to a wallet;
- Expertise and thorough preparation in advance needed to perform the seizure;
- Transactions usually require a fee, and the bearer of the costs must be determined;
- Mistakes during the seizure may result in the loss of the virtual currencies;
- Lack of specific legal framework;
- Seizure of virtual currencies abroad via mutual legal assistance request;
- Secure LEA storage devices and storage locations;

- Protection of LEA wallets against unauthorised access, e.g. hacking; and
- Need to have multi-signature offline wallets to ensure secure storage as well as accessibility in the event any signatory leaves the office.

B) Further storage or selling of seized virtual currencies

After the seizure has been performed and the virtual currencies are stored, authorities have the **choice to further store them on LEA or judicial wallets or sell them** and thus exchange them for traditional currencies, which can subsequently be kept in a bank account during the further criminal investigation and proceedings. Depending on **national or local policies**, different considerations will be made before deciding on either option.

In most countries, authorities will keep the virtual currencies stored in a wallet. Among the reasons for this option are:

- selling the virtual currencies is considered too complicated;
- the risk that the value of the virtual currencies will increase significantly after selling (and virtual currencies would need to be returned to the owner); or
- simply because the owner of the virtual currencies needs to give his consent for the sale.

In a few countries, though, preference will be given to selling the virtual currencies because of the risk of loss of value due to the volatility of the price, or disproportionate storage costs. In addition, the opinion of the owner will be taken into account.

The **actual moment of the sale** will consequently also differ: in many countries, the virtual currencies will only be sold after a final court ruling in the case. However, selling the virtual currencies immediately or soon after the seizure is also possible, in view of the volatile nature of the price of the virtual currency and the risk of loss of value. In some cases, the sale takes place at the request of the owner during the ongoing proceedings. This course of action will usually be requested to avoid loss of value. In some countries, selling the virtual currencies will only be possible when the virtual currencies are no longer required as proof.

Selling virtual currencies can be **done in different ways**. In some countries, this process is not regulated; many other countries have no experience. However, in several countries, the sale must be carried out (by law) via a public auction. In some countries, the virtual currencies are sold via a (selected) virtual currency exchange or trading platform, which in some situations needs to be a domestic platform. Other options mentioned were to sell the virtual currencies on the open market to obtain the best price; to sell them to a virtual currency trader; or to commission an external partner to make the sale.

If national authorities have decided to sell the virtual currencies, they can also be confronted with different **obstacles**:

- Organising a public auction can be difficult, as many factors need to be taken into account in relation to the protection of the virtual currencies while at auction, including payment, prevention of money laundering and secure transmission of the virtual currencies;
- The exchanges or trading platforms need to be trustworthy and reliable;
- Identity is required for the Know Your Customer (KYC) process, which is applied by exchanges. This process is time-consuming;
- If the amount of virtual currencies to be sold is very large, market conditions may be impacted;
- If the (selected) exchange does not offer the type of virtual currencies for exchange; and

- State liability in the event of subsequent acquittal of the suspect and significant loss of value of the sold virtual currencies in the meantime.

During the course of the proceedings, the Court can dismiss the case and rule that the **virtual currencies need to be returned to the owner**, due to a lack of sufficient evidence or a lack of crime having been committed. In this situation, if the virtual currencies were still stored on a LEA or judicial wallet, they would simply be transferred to the wallet of the owner. This will be the most common situation, as seized virtual currencies are usually not sold before a final judgment is rendered in a case. If, however, for any reason, the virtual currencies were already sold in the meantime, the amount realised in the sale would be transferred to the person's bank account.

If a Court rules that the virtual currencies need to be returned, a risk of difference in value between the virtual currencies seized on the day of the court ruling, had they not been sold, and the amount received from the actual sale of those virtual currencies, is possible. For the reason explained earlier, this situation is unlikely to occur. However, if it does occur, the liability question for the loss of value will mostly be assessed on a case-by-case basis by a court. One possibility is that the amount of the sale of the virtual currencies is returned, without any additional compensation. In some countries, the State bears the risk of differences in value and the 'victim' could claim compensation, although compensation might only be paid in the event of a serious fault. In one country, full compensation for any losses is the main rule, and therefore the amount of the sale could be returned with additional interest.

	Legal provisions applied for seizure of virtual currencies
AT	General provisions: Sections 109 110 and 111 of the Code of Criminal Procedure
DE	General provision on asset recovery: Section 111b of the Code of Criminal Procedure
EE	General provisions
EL	General provisions: Article 68 Penal Code and Article 40 of Law 4557/2018
FI	General provisions
FR	General provisions on seizure of assets: Articles 706-153 Code of Criminal Procedure
HU	Act XC/2017 Code of Criminal Procedure Section 315; Decree 11 of 2003
IE	General provisions: Section 7 Criminal Justice Act 2006; Section 14 Criminal Assets Bureau Act 1996
IT	General provisions
LU	General provisions: Articles 31 and 66 Code of Criminal Procedure
LV	General provisions: Section 235 Code of Criminal Procedure
PT	General provisions
SE	General provisions
SK	General provisions: Article 90 Code of Criminal Procedure
SL	General provisions
UK (E&W)	Section 49 Regulation of Investigatory Powers Act, Section 84 of the Proceeds of Crime Act 2002, Section 47C of the Proceeds of Crime Act 2002
UK (S)	General provisions: Sections 127A-127Q of the Proceeds of Crime Act 2002
CH	General provisions
NO	General provisions

	Legal provisions applied in case of selling of seized virtual currencies, or legal provisions prohibiting the selling of seized virtual currencies
AT	Sections 115e and 377 Code of Criminal Procedure
CH	Article 266 Code of Criminal Procedure
DE	Section 111p Code of Criminal Procedure
EE	§ 126 Code of Criminal Procedure
EL	/
FI	Auction by Customs: Customs act 80§ Auction by police: law of enforcing State-collected fines/penalties 38§
FR	Article 99-2 Code of Criminal Procedure
HU	Articles 315 and 319 Code of Criminal Procedure; Section 67 Decree 11/2003
IE	Sections 4 and 7 of the Proceeds of Crime Act 1996
IT	/
LU	N/A
LV	/
NO	Section 213, §1 Criminal Procedure Code
PT	general provisions
SE	/
SK	N/A
SL	Article 506a Criminal Procedure Act
UK (E&W)	Section 41(7) of the Proceeds of Crime Act 2002
UK (S)	/

6. Way ahead

The Cybercrime Judicial Monitor is published once per year. It is distributed to judicial and law enforcement authorities active in the cybercrime domain and, as of this issue, published on the Eurojust website.

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 practitioners to send, throughout the year, relevant national legislative developments, court decisions, suggestions for topics of interest and other information considered useful for the purpose of future issues of the CJM to Eurojust.

We would like to 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-19-005-EN-N • *ISBN*: 978-92-95084-00-1 • *ISSN*: 2600-0113 • *DOI*: 10.2812/242576