Cybercrime Judicial Monitor

Issue 3 - December 2017

Contents

1. Executive Summary

Eurojust presents this third issue of the Cybercrime Judicial Monitor (CJM). The CJM is published once per year and distributed to law enforcement and judicial authorities active in the field of combatting cybercrime and cyber-enabled crime.

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 2017.

The judicial analysis section presents legal analyses of court rulings rendered by courts in Belgium, the Netherlands, Norway and Switzerland. Several cyber-relevant issues and topics are addressed by the courts, such as the use of surveillance devices by law enforcement authorities (LEA) and undercover operations online, Internet Service Provider (ISP) cooperation, Torrent technology and malware, and admissibility of evidence. In addition, summaries of other interesting court decisions rendered in Ireland, the UK and Switzerland are presented.

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 given of relevant court decisions. So far, none of the courts have invalidated national data retention rules.

The topic of interest in this issue of the CJM is *'online investigations into Darknet criminality'*. An overview is given of the investigative possibilities as well as legal and practical challenges for LEA and judicial authorities when conducting Darknet investigations. In addition, the opportunities and challenges of some investigative tools, such as umbrella investigations and joint investigation teams are highlighted.

2. Legislation

The objective of this section is to provide information on recent developments in international, EU and national legal instruments in relation to cybercrime and e-evidence in 2017. The main sources of information presented in this section are contributions collected through the European Judicial Cybercrime Network, unless specifically stated otherwise.

2.1. Member States

Belgium

Statute of 25 December 2016 containing miscellaneous amendments to the Code of Criminal Procedure and the Criminal Code, with a view to improving special investigative methods and certain investigative measures with regard to the Internet and electronic and telecommunication, and establishing a database of voice recordings.

This Statute introduces several changes to the Belgian criminal procedure law provisions on seizure of data, computer and network searches, mainly which authority (prosecutor or investigative judge) can authorise such investigative measures and under what circumstances.

New legal provisions are introduced on expedited preservation and disclosure of computer data and traffic data, in accordance with articles 16, 17, 29 and 30 of the Budapest Convention. The provisions stipulate rules for preservation of data in Belgium as well as abroad.

Several provisions have been amended to be in line with the (scope of the) Yahoo rulings, particularly if the court ruled on the obligation to cooperate under Belgian law for:

> *'anyone making available or offering a service within the Belgian territory, in any way whatsoever, consisting of transmitting signals via electronic communications networks, or allowing users to obtain, receive or distribute information via an electronic communications network. This includes the provider of an electronic communications service.'*

These stipulations have been incorporated in the provisions on requests for basic subscriber information, traffic and location data (for real-time interception), and legal hacking by law enforcement authorities.

Furthermore, some of the conditions and criteria for hacking by law enforcement authorities (including bypassing or breaking encryption through the use of technical tools) as well as observation and infiltration online, have been amended.

A novelty introduced by the Statute is that voice recordings will not be deleted. They will now be retained in a database.

This Statute was published on 17 January 2017 and entered into force on 27 January 2017.

Germany

§100a (interception of telecommunication) and §100b (online search) of the Code of Criminal Procedure

New legal provisions have been incorporated in the German Code of Criminal Procedure on interception of telecommunication and online searches. Under specific conditions and in relation to crimes of a particularly serious nature, law enforcement authorities are allowed to use technical means to remotely search and seize data covertly, if necessary to enable monitoring and recording, particularly in an unencrypted form.

A specific tool can now be placed on the device targeted by the measure, which enables source interception, meaning that the communication can be intercepted from the device even before transmission takes place and the data is encrypted.

Hungary

Act 110 of 2017 on the Code of Criminal Procedure, Sections 214-260 (undercover investigations) and Section 315 (seizure of virtual currencies)

In Hungary, new provisions on covert investigations have been introduced in the Code of Criminal Procedure. The new Act covers three types of covert data gathering, according to whether or not prior prosecutorial or judicial consent is needed. Specific types of covert investigations as well as methods to be used are now regulated in more detail. Noteworthy in this respect, the Act stipulates that covert agents, who were previously not allowed to participate in crimes of willful killing, are also no longer allowed to participate in crimes causing bodily harm with a permanent deterioration of health. Moreover, they are not allowed to convince anyone to commit a crime or a more serious crime than they intend to commit.

Section 315 of the new Code of Criminal Procedure stipulates that the seizure of electronic data usable for payment (i.e. virtual currencies) can be done through the use of a method that blocks the user from utilising electronic data for payment, which in practice means that when a virtual currency wallet and its access credentials are identified during a seizure, the investigator can create a different wallet to move the seized virtual currencies, thereby blocking their further use.

Ireland

New provisions and amendments introduced by the Criminal Justice (Offences Relating to Information Systems) Act 2017 and the Criminal Law (Sexual Offences) Act 2017

Two pieces of cybercrime-specific legislation have been introduced since 1 January 2017.

The Criminal Justice (Offences Relating to Information Systems) Act 2017 repeals the previous provision of the Criminal Damage Act 1991 which dealt with attacks against data and computer systems. It introduced five new offences that criminalise:

- Accessing information systems without lawful authority;
- Interfering with information systems without lawful authority;
- Interfering with data without lawful authority;
- Intercepting data transmissions without lawful authority; and
- Using computer programs, passwords, code or data to commit any of the above.

The Criminal Law (Sexual Offences) Act 2017 introduced new offences that would involve the sexual exploitation or abuse of children:

- Obtaining a child for sexual exploitation;
- Inviting a child to engage in sexual touching;
- Engaging in sexual activity in the presence of a child;
- Causing a child to watch sexual activity;
- Meeting a child for the purpose of sexual exploitation; and
- Using ICT to facilitate the sexual exploitation of a child.

The Act also amended the existing provisions of the Child Trafficking and Pornography Act 1998 by amending the definitions of child pornography (*'...a person who is or is depicted as being a child and who is engaged in or is depicted as being engaged in real or simulated sexually explicit activity'*); exploitation of children; production and distribution of child pornography; and possession of child pornography. New prohibitions were added in relation to the participation of a child in child pornographic performances and the accessing of child pornography by means of information technology. Furthermore, the age of a child has been raised from 17 to 18 years.

Italy

Law no. 71/2017, '*Regulation for the safeguarding of minors and the prevention and tackling of cyberbullying*'

New legislation was approved in Italy, addressing cyberbullying. Law no. 71/2017, entitled *'Regulation for the safeguarding of minors and the prevention and tackling of cyberbullying'*, was created to fight the phenomenon of cyberbullying in all its manifestations, through prevention, education, and criminalisation. Cyberbullying is defined as 'any form of pressure, aggression, harassment, blackmail, injury, insult, denigration, defamation, identity theft, alteration, illicit acquisition, manipulation, unlawful processing and/or dissemination through electronic means of personal data of minors, including the dissemination of online content depicting also one or more components of the minor's family, for the intentional and predominant purpose of isolating a minor or a group of minors by effectuating a serious abuse, malicious attack or a widespread and organised ridicule'. Website hosts are considered responsible for the management of website content. Minors older than the age of 14 who have been victims of

online abuse, as well as their parents, can ask website hosts and social platforms to remove and block abusive content online within 48 hours.

Law no. 103/17 of 23 June 2017, implementing the delegation of powers to the government for introducing new provisions concerning the interception of conversations or communications

This Decree implements a revision of the rules on interception, to make the safeguarding of specific rights and interests, equally protected by the Constitution, more balanced: the freedom and secrecy of correspondence and of any other form of communication, and the efficiency of investigations.

The new rules also cover the right of the media to disseminate information. New provisions have also been included, particularly regarding the use of so-called 'Trojan horses'.

These new legal provisions will be published in the Official Journal of the Italian Republic in the near future.

UK

Investigatory Powers Act 2016

On 29 November 2016, the Investigatory Powers Act was passed. Although it became law from that moment, most of its provisions only entered into force on 30 December 2016, having implications effectively only from 2017.

The present Act is designed to consolidate and give transparency to the existing surveillance powers, as well introduce new ones, regarding gathering and retaining data on citizens, and forcing technology companies to hand over data that they have stored. It expands the electronic surveillance powers of the UK intelligence community and police and, at the same time, improves the safeguards of the exercise of those powers.

This new legislation contains provisions on interception of communications, equipment interference and the acquisition and retention of communications data and other information, as well as the treatment of material held as a result of such measures. In addition, it also establishes a new framework of oversight intended to prevent abuse, which includes setting up an independent body – the Investigatory Powers Commissioner – tasked with reviewing and reporting on the government's surveillance activities.

Sentencing guidelines (England and Wales)

The Sentencing Council for England and Wales promotes greater consistency in sentencing, while maintaining the independence of the judiciary. For this purpose, the Council produces guidelines on sentencing for the judiciary and criminal justice professionals. Courts are bound to follow guidance issued by the Sentencing Council.

The Sentencing Council has, for example, issued guidance in relation to the sentencing for 'indecent photographs of children'. The sentence should be determined on the basis of three steps. As a first step, the court should determine the offence category, based on what is depicted in the photographs and whether it concerned possession, distribution or production of such photographs. Having determined the category, the court should then use corresponding starting points for sentences within the different category ranges. Further steps to determine the sentence are 'factors which indicate a reduction, such as assistance to the prosecution', 'reduction for guilty pleas', 'dangerousness', 'totality principle', 'ancillary orders', 'reasons' and 'consideration for time spent on bail'.

The link to the webpage of the Sentencing Council can be found here

2.2. Third States

Norway

Article 199a Code of Criminal Procedure

A Bill, approved by the Norwegian Parliament earlier this year, gives law enforcement legal access to computer systems that require biometric authentication. The provisions of the new Bill were incorporated in the second paragraph of the Code of Criminal Procedure. This new legislation is a direct consequence of last year's Supreme Court decision concerning the denial of access by police to the contents of a seized smartphone that was locked with a fingerprint code.

The new provisions now stipulate the following: 'When conducting a search of a data-processing system, the police may order everyone who is dealing with the said system to provide the information necessary for gaining access to the system or to open it by use of biometric authentication.'

In the event of refusal to comply with such an order, the police may perform the authentication by use of force, which needs to be authorised by a prosecutor. In the event of urgency, the police may use force at the scene and promptly report it to the prosecutor afterwards.

Switzerland

Art. 269bis (use of technical tool for monitoring telecommunication) and 269ter (use of government software for monitoring telecommunication) of the Code of Criminal Procedure

The Swiss federal law on surveillance of post and telecommunication traffic was amended, and new provisions were inserted on surveillance by means of government software or by use of a technical tool (IMSI catcher). The revised law will enter into force in 2018. The Swiss Code of Criminal Procedure will be amended to incorporate these new provisions.

The public prosecutor can order the use of government software or a technical tool for interception of telecommunication only if the measures taken so far to monitor the telecommunications have been unsuccessful or would make monitoring them impossible or disproportionately difficult. Further conditions apply to the application of both measures; and government software may only be used when investigating crimes of a certain gravity.

The use of government software will allow for the surveillance of end-to-end encrypted communication. Other – theoretically possible – activities of the software, such as computer searches, will however not be allowed.

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 States.

3.1. Selected court rulings

Procedure: Court of First Instance Antwerp, section Mechelen, ME20.F1.105151-12, Belgium

Date: 27 October 2016

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

Facts

In the framework of a judicial inquiry into activities of a criminal organisation, the investigative judge of Mechelen ordered a measure of wiretapping and registration of a suspect's Skype account. The suspect was using the services of Skype Communications SARL (hereinafter 'the accused') to communicate from Belgium with other persons by means of Skype software. The ordered wiretap and registration measure was accompanied by a request to the accused to give technical assistance.

The accused replied that only the registration details were available and that they did not have any records of Skype-to-Skype communications because they use a peer-to-peer network. Moreover, Skype user data is subject to Luxembourgish law, as the accused was located in Luxembourg, and any information outside of the voluntary disclosure compliance would need to be requested via MLA. The accused did not reply with regard to the giving of technical assistance.

Charges

The accused was charged with:

Violation of articles 88bis §2 and 90quater §2 of the Belgian Code of Criminal Procedure (C.C.P.) by having refused, as a telecommunications operator or as a provider of a telecommunications service required by an Investigating Judge to communicate data [...], to deliver the said data and/or to have given the said technical assistance.

Defence case

The accused introduced several arguments on the basis of which the public prosecution would be inadmissible. According to the accused, the Belgian judge had no jurisdiction because the offence for which the accused was prosecuted had no territorial link with to Belgium. The accused emphasized that the company is established in Luxembourg and has no establishment in Belgium.

The main arguments brought by the accused in relation to the substance of the case were the following:

- It does not fall under the application of articles 88bis and 90quater C.C.P. in the sense that it is not a telecommunication network operator nor a provider of a telecommunication service.
- It is established in Luxembourg, and therefore Articles 88bis and 90quater C.C.P. cannot be imposed upon it, as they do not apply outside Belgian territory. The accused is therefore not obliged to cooperate.
- It did not refuse to lend assistance to the Belgian authorities, but was not technically able to procure further data.

Court proceedings

Admissibility of the public prosecution

With regard to the claim of the accused that the offence had no territorial link to Belgium, the Court explained that the aforementioned penal provisions stipulate that the data requested must be communicated by the telecommunication network operator and telecommunication service provider. The operator or provider is obliged to lend technical assistance if requested by an investigative judge. These legal dispositions imply, therefore, that the **said data and technical assistance be made available to the investigators on Belgian territory**. Furthermore, the Court made reference to the ruling of the Supreme Court in the Yahoo! case, stating that *'the offence [of not providing the requested data] has been committed in the place where the requested data have to be received. As a consequence,* ***the operator or provider who refuses to communicate the data is susceptible of being punished in Belgium, wherever he is***

established.[1] The Court therefore concluded that sufficient links with Belgium were present and, consequently, the Belgian judge has jurisdiction.

The other arguments introduced by the accused as to the (in)admissibility of the public prosecution were also not accepted by the Court. The Court thus stated that public prosecution was admissible.

Substance of the case

According to articles 88bis §2, first section and 90quater §2, first section C.C.P., the obligation to cooperate rests on the telecommunication network operator and on the provider of a telecommunication service. The Court stated that the accused, in the period of the indictment, **made available to users in Belgium and elsewhere in the world free software that enabled these users to communicate and exchange information via an electronic network (the Internet) with other users**. Therefore, the Court concluded that the accused should be considered a **provider of a telecommunication service**. The fact that the exchanged information is transmitted directly between the users' computer systems without intervention of the accused itself (peer-to-peer), does not change this qualification.

In relation to the obligation of the accused to cooperate, the Court again referred to the Supreme Court ruling in the Yahoo! case *(see supra)*, which stipulated that *'the measure consisting in the obligation to provide data, is taken on Belgian territory with regard to every operator or provider who is economically active in Belgium …'*. The Court continued by stating that the obligation to make available the necessary information, data and/or technical assistance for the accused is considered to be complied with on Belgian territory. Therefore, the Court concluded that the execution of the **coercive measure does not require any intervention outside Belgian territory**.

To be subject in Belgium to a coercive measure in the sense of articles 88bis §2 and 90quater §2 C.C.P., a provider of a telecommunication service established abroad must have a **sufficient link with Belgian territory**. The Court considered that such a sufficient link can consist of the active participation in the Belgian economy of the service provider. As the accused (a) made its software available to users on Belgian territory; (b) made its website accessible in Dutch to users in Belgium; and (c) provided focused publicity ads, the Court stated that an inference can be made that **the accused, in its capacity as service provider, participated actively in the Belgian economy** at the moment of the facts. Therefore, a sufficient link with the Belgian territory was demonstrated. As a consequence, the Investigating Judge was allowed to directly address the request to the accused without having to do so by way of an MLA request. The Court therefore concluded that the accused was obliged to comply with the request.

With regard to the third substantial claim of the accused, the Court found that the accused appeared, from its reactions to the reiterated requests made by the Belgian police, to have never had a genuine intention to comply. As to the claim of the accused that it cannot comply with its obligation of **technical assistance** because it is not capable from a technical point of view, the

[1] Cass. 1 December 2015, AR No. P.13.2082.N

Court stated that **the accused itself caused this material impossibility** by organising in its own way the supply of services to its clients. Given the fact that the accused voluntarily chose to be present in the Belgian market as a service provider, **it was required to take into account Belgian legislation that obliges it to give technical assistance if requested**.

Court ruling and sentence

When determining the sentence, the Court took into account the seriousness of the facts, namely the conscious choice of the accused to be active in the Belgian market but its unwillingness to fulfill the obligations resulting from that presence. The Court also took into consideration the lack of judicial antecedents of the accused.

The Court convicted the accused to a fine of EUR 30 000.

Note: On 15 November 2017, the Court of Appeal in Antwerp confirmed the judgement of the Court of First Instance.

Procedure: Court of Cassation, case P.16.1245.N, Belgium

Date: 28 March 2017

Key words: LEA conducting online investigation on publicly accessible forum

Ruling of the Court of Appeal

In November 2016, the Court of Appeal of Antwerp convicted the defendant of selling and exporting drugs on a Darknet forum. The police discovered the illegal online activities through the use of specific software, search queries via search engines and a website that monitors Darknet markets, so that they could receive an invitation link to the forum. Upon receipt of the invitation link, they registered on the forum, using an alias, and subsequently accessed the forum. By doing so, the police merely entered a place accessible to the public, according to the Court of Appeal, and thus did not access places of the internet that were private.

Defence

The appellant argued that the forum was only accessible upon invitation by a member of the forum, which constituted a virtual private club, limited to certain persons for private communications. The police were therefore only allowed to access the 'private' forum upon authorisation of an investigative judge.

Court ruling and decision

The Court of Cassation stated that **autonomously gathering information and evidence in places on the Internet accessible to the public is within the mandate of police authorities**, in the same way as the public can enter these places and without prejudice to the provisions of the Belgian Code of Criminal Procedure on the special investigation methods and Internet investigations and interceptions. The use of an alias for this purpose can be the normal way of visiting parts of the Internet, provided that such use does not imply adopting a credible false identity and the alias used does not provoke the commission of a crime.

Furthermore, the Court indicated that the mere fact that **admission conditions apply to access a place on the Internet, does not make that place 'private'**. The forum thus was publicly accessible. As the police fulfilled the admission requirements, they were allowed to access this part of the Internet without the need for prior judicial authorisation.

The Court dismissed the appeal.

Procedure: Court of 1st Instance, District Court Amsterdam, case no. 13/995008-13

Date: 16 March 2017

Key words: child sexual exploitation online, use of surveillance device by LEA

Facts

In May 2013 the Dutch police received a report from Facebook identifying 86 linked accounts that contained and were used to disseminate images of sexual exploitation of children. Some of those accounts were also used to blackmail dozens of underage girls using pornographic images obtained via a webcam. The accounts' owner used a false identity to create the accounts and hid his IP address and Internet traffic behind a 'Virtual Private Network' (VPN). Based on the IP address and telephone number used to register one of the accounts, Facebook determined that the user of that account was located in the Netherlands.

The Dutch police started an investigation and identified the telephone number, IP address and location of the computer used. In the course of their investigation, the police entered the apartment of the defendant and installed surveillance software on his computer, which recorded keystrokes and made screenshots when the browser or communication software were used, such as Skype, which allowed the police to bypass restrictions caused by the use of a VPN.

In the course of the investigation the police discovered that the suspect, while pretending to be a child himself, made contact online with underage girls and obtained images showing those girls

in intimate situations. He subsequently threatened that he would circulate those images online, to force the girls to perform sexual acts on the webcam that he then recorded. If a girl did not comply, he sent the images to her family and friends and posted them online.

After arresting the suspect in 2014, the police seized the computers and hard drives found in his apartment. These contained compelling evidence confirming his involvement.

Charges

The charges brought against the accused included

- Child pornography, including possession, distribution, acquisition and production of child pornography;
- Factual and attempted indecent assault (via Internet) of 34 girls;
- Computer trespass; and
- Blackmail, swindling, document forgery and possession of narcotics.

Court proceedings

The use of the technical tool (software) by the police

The defence argued that the use of the surveillance software on the defendant's computer was unlawful and that the information obtained was not a reliable.

In its response the Court relied on the Decree on Technical Tools in Criminal Proceedings of 20 October 2006, which sets out rules on the use of technical tools to guarantee that the data obtained through the use of such tools is reliable as evidence. The 2006 Decree stipulates that such a device must meet certain technical requirements and an inspection report must be made. The Court referred to earlier decisions of the Supreme Court, which stated that a court should assume that the surveillance device complies with technical and legal requirements if it possesses a certificate from an inspection service. Given the fact that such a **certificate was indeed provided for the surveillance software**, the Court concluded that the software met the legal requirements for use.

The defence pointed out that the matters on which the Supreme Court ruled related only to *equipment* and that the Supreme Court's decision is not necessarily applicable to *software*. The Court stated that the 2006 Decree only uses the term 'technical tool', without distinguishing between hardware and software, and concluded that **the term technical tool also covers software**.

The investigative judge made a prior assessment regarding the workings of the tool vis-à-vis the issued certificate. The defence argued that the software cannot be tested prior to its use and should therefore have been tested afterwards, and that certain settings needed to be adjusted

during installation of the software. The Court stated that the **adjustments of the settings did not alter the functioning of the software to the extent that they annulled the prior certification**. Moreover, it is not because certain settings need to be adjusted during installation of the software, that the software itself cannot be tested prior to use. The Court therefore dismissed the argument.

In relation to the use of the surveillance software, the Court concluded that it had been **tested and approved prior to use**. The Court also stated that no irregularities were indicated during its use or that the results of its use would be unreliable. Therefore, the information gathered through the use of the surveillance device could be used as evidence.

Physical proximity not necessary for sexual assault charge

The defence argued that there cannot no assault took place because of lack of physical proximity due to the Internet nature of the communication.

In relation to this argument the Court relied on the ruling of the Supreme Court case, in which a victim, again an underage girl, was forced to perform sexual acts on the webcam. The Court ruled that **sexual assaults do not always require physical proximity,** and that a person can be sexually assaulted also via a webcam.

Court ruling and sentence

The Court sentenced the defendant to a maximum punishment of ten years and eight months imprisonment. The Court handed down the maximum penalty because it considered the defendant very dangerous to society and capable of committing similar crimes in the future. In justifying its sentence, the Court referred to the defendant's cynical attitude in the course of committing his crimes and lack of remorse, and the devastating effect that his crimes had on his victims, who were mostly very vulnerable children, some of whom were only nine years old.

Procedure: Court of 1st Instance, case no. 10/960260-16, the Netherlands

Date: 7 April 2017

Key words: Malware, webinjects, Telegram chats

Facts

In 2015, criminals illegally gained access to banking websites, using specially designed malware. First webinjects were used, so that the Internet browser would display a fake website instead of the authentic one. Subsequently, the criminals collected and transferred information from the

victims' computers through the use of Tinba and ReactorBot software. With the illegally gained credentials, one of the criminals (subject of the below court ruling) transferred money from the victims' accounts and ordered goods online.

Charges

The accused was charged with:

- developing, acquiring and/or spreading of technical tools (malware) for the purpose of illegally accessing a computer system;
- multiple counts of illegally accessing a computer system;
- multiple counts of theft; and
- making a habit of money laundering.

Evidence

Through the analysis of a seized telephone, Dutch police were able to retrieve conversations with a person called 'Murpa Boy'. The messages, sent using Telegram, revealed close criminal cooperation between the owner of the telephone and 'Murpa Boy'. They included information on the testing of malware, the exchange of pieces of written text to be used for fraud and phishing, postal addresses for the receipt of bank cards, personal credentials and details of third persons and information about the skimming of bank accounts and the laundering of money.

Court proceedings

The Court first assessed the evidence to establish that 'Murpa Boy' and the suspect are the same person.

The Court found sufficient proof in the Telegram chats, which contained specific identification details matching the suspect, as well as a telephone call to the suspect's telephone number and the complaint of one of the banks, which noticed suspicious behaviour by one customer (the accused) at the time it was looking into the malware-attack.

The Court then continued by stating that the accused had worked closely together with the owner of the seized telephone to commit the crimes. This information follows from the **Telegram chats**, in which they discussed a variety of actions: illegal access to computers, sending requests to banks to connect bank accounts, intercepting bank cards and online orders, and retrieving money from fraudulent transactions. The **coordination of these (subsequent) activities**, which is clearly shown in the chats, **proves the deliberate intent and cooperation between both persons**. Without this intent and cooperation, commission of the crimes would not have been possible. The Court therefore concluded that the accused was co-author of the crimes committed.

The defence argued a lack of sufficient proof that the accused had himself developed, acquired and/or spread the malware. The Court refuted this argument by referring to the chats, during

which the accused explained that he wanted to (have) develop(ed) malware targeted to a specific bank. Also, from the complaint filed by the bank, the accused appeared to have done some 'tests' with money transfers and requests for a new bank card. Moreover, the usefulness of a webinject is not only determined by the programming code, but also by the quality of the displayed fake website. The Court stated that the **accused at least supplied essential information regarding the format/content of the website, so that the proper programming code could be created**. The Court thus concluded that the accused did develop, acquire and/or spread the malware.

According to the defence, insufficient proof was demonstrated that the defendant infected the computers with the webinjects and malware. The Court dismissed this argument by stating that the accused and his accomplice had **received login credentials and personal data from victims through the webinject**, which was only possible because they had first infected the victims' computers.

With regard to the charges for making a habit of money laundering, the Court agreed with the defence that money laundering had only been committed once by the accused, and therefore acquitted him of this particular charge.

Court ruling and sentence

The Court of First Instance of Rotterdam convicted the accused and sentenced him to 36 months' imprisonment and ordered the payment of damages of EUR 13 201 to one of the victims, a foundation for food aid.

Procedure: Court of 1st Instance Rotterdam, case no. 10/960360-16, the Netherlands

Date: 14 April 2017

Key words: Bitcoin, money laundering

Facts

For several months, a Dutch national was selling drugs on the Darkweb. He gained more than EUR 100 000 in profit from this illegal business. During a search of the suspect's house and car, the Dutch police found large sums of money, both in cash and in bank accounts, including Bitcoin.

Charges

The accused was charged with multiple offences of drug trafficking, drug possession and money laundering.

Defence

The accused confessed to most of the drug-related offences, but disputed the allegation that he had laundered the proceeds of the drug trafficking. According to the defence, the money found during the house search came directly from the committed crimes and the suspect did not hide its origin. Therefore, according to the defence, the accused should not be charged with money laundering.

Court proceedings

The Court of First Instance of Rotterdam considered the drug-related offences proven, given the confessions made by the accused. The Court therefore mainly focused on the charge of money laundering.

First, the Court agreed with the prosecution and the accused that the **receipt of payment in Bitcoin does not constitute money laundering,** but rather the mere possession of proceeds of crime. The Court therefore disregarded the possession of Bitcoin in its consideration of the charge of money laundering.

The Court further considered as fact that the cash found during the house search was laundered. Indeed, the accused was paid in Bitcoin by his customers, and he subsequently **converted the virtual money into cash and transferred the Bitcoin into euro** in his accounts (which constituted a change in currency, the first act of concealment). He **subsequently withdrew sums of cash** from those accounts. By doing so, the accused **concealed the criminal origin of the money and thus laundered the proceeds of crime**. According to the Court, the defendant was not able to provide compelling evidence to suggest that the seized cash did not originate from his criminal activities.

Court ruling and sentence

The Court found the accused guilty of several counts of drug trafficking, drug possession and money laundering. He was sentenced to 30 months' imprisonment.

Procedure: The Hague Court of Appeal, case no. 10/960317-16, the Netherlands

Date: 9 May 2017

Key words: Darkweb, undercover operation, weapon sale

Facts

On 7 August 2016, the suspect sent an e-mail to a vendor on the Darknet, indicating that he wanted to buy a gun and, potentially, hand grenades. In fact, the vendor was a Dutch undercover

police officer. The officer presented himself with a pseudonym on the Darkweb for weapons trade. Using information gathered from subsequent communication, the police were able to arrest a suspect with the help of Australian law enforcement authorities.

Charges

The accused was charged with attempt to acquire weapons (Art. 2.1 category II of the Law on Weapons and Ammunition).

Proceedings Court of First Instance

The Rotterdam Court of First Instance convicted the accused and sentenced him to eight months' imprisonment for attempting to purchase objects that have as their object attacks on persons by fire or explosion, within the meaning of Article 2(1) Category II(7) of the Law on Weapons and Ammunition. The convicted filed an appeal against the ruling.

Defence

In appeal, the appellant claims he was **incited by the police to purchase the explosives**, and that the police first contacted him and continued to put pressure on him, including by lowering the price, to reach an agreement on the sale. According to the defence, the (attempted) purchase would not have taken place without the intervention and insistence of the police. The criterion for unacceptable incitement was therefore met, according to the appellant.

Additionally, the appellant claimed that the **police engaged in a so-called pseudo-buy of the objects, for which they did not have the proper judicial authorisation**. To perform a pseudo-buy, a judicial order is required under Article 126i of the Dutch Code of Criminal Procedure. According to the defence, the order under which the police were acting was limited to structural collection of information (Article 126j C.C.P.), and, as a consequence, the Court should declare the Public Prosecutor's Office's case inadmissible, or, as a subsidiary argument, exclude the evidence acquired on the basis of the incorrect order.

As a subsidiary argument, the defence claimed that the appellant acted in a clumsy, childish and amateurish manner, and that the sale agreement only went through because the police informant was actively steering towards that result.

Court proceedings

The Hague Court of Appeal first assessed the argument that the police informant had incited the defendant According to the Court, the **accused clearly was the one initiating the contact**, as he sent the first e-mail to inquire about purchasing weapons. Therefore, the Court does not find that any form of incitement was used.

As for the alleged pseudo-buy of the explosives, the Court rules that **mere communication by e-mail does not mean that the police had the actual intention to sell explosives**. In the

absence of such intention, the conditions for pseudo-buy as defined in Article 126i C.C.P. were not met, and, therefore, the judicial order was not required.

Regarding the final, subsidiary argument, the Court concludes that the accused acted in an effective way by gaining access to the Darkweb and creating an encrypted e-mail address, and initiating and maintaining contact with the police officer. The suspect's behaviour was therefore considered proper and effective, and the Court dismissed the argument.

Court ruling and sentence

The Court concluded that the appeal must be rejected. The Appeal Court found the defendant guilty and sentenced him to eight months' imprisonment.

Procedure: Supreme Court of Norway, HR-2016-2263-A, Norway

Date: 3 November 2016

Keywords: handling of proceeds of digital data abuse, social media, Torrent technology

Facts

At the end of 2014, during a house search, the Norwegian police found a large amount of photographs and videos stored on a suspect's computer. The files contained images of young women, many of a private and sensitive nature. The suspect had downloaded the images via BitTorrent, a peer-to-peer file sharing tool on the Internet. The photographs appeared to have been secretly collected from numerous social platforms and were shared online, through the use of BitTorrent, without the owners' knowledge or consent.

Charges

The accused was charged with violation of the Penal Code (1902) section 317 subs. 1 on 'handling and/or receiving of proceeds of crime' in conjunction with the Copyright Act, section 54, cf. section 45c, regarding downloading and sharing of large numbers of photographs and films without consent.

District and Appeal Court rulings

The District Court acquitted the defendant of the abovementioned charges, following which the judgement was appealed by the public prosecutor. The Appeal Court found the accused guilty of violating section 317 of the Penal Code and sentenced him to 120 days' imprisonment. Both the prosecuting authority and the convicted appealed against the sentencing.

Evidence

The investigation disclosed that the photographs found on the suspect's computer were downloaded by means of **BitTorrent Sync., a file-sharing tool that applies Torrent technology to transfer large quantities of digital material between users' computers**. The computers using BitTorrent form a network and are synchronized, meaning that, even if a person does not upload material, he will contribute to the file sharing, since other users can download what he himself has downloaded from BitTorrent. Given the fact that the **suspect had downloaded the photographs, he thereby facilitated the spreading of the materials** to other users.

Moreover, one of the purposes of sharing with BitTorrent was to enable **identification of women** to the extent possible, by linking photographs to addresses. A folder system was created for this purpose. All in all, 36 270 files and 442 subfolders were found, more than 200 of which were named after specific women or users.

Examination of the photographs also showed that many of them were stored initially by means of *Snapsaved* or as screenshot copies. Snapchat is a mobile app that allows sharing of photographs with certain recipients and for a limited time, determined by the sender. The sender will receive a notification if a recipient takes a screenshot of his or her image. The application ***Snapsaved*** allows recipients to bypass that notification and thus to **save Snapchat images without the sender's knowledge and consent**.

Court proceedings

The Supreme Court followed the reasoning of the Court of Appeal regarding the illegal sharing of the photographs online. The photographs were initially shared by the women themselves through social media such as Snapchat, Facebook and Instagram. The photographs were subsequently saved without the knowledge and consent of the women and shared anonymously on the Internet on forums such as anon-ib.com, where users were urged to share a large number of photographs by means of BitTorrent Sync. The Court concluded that the defendant, by means of file sharing and the use of Torrent technology, had stored and made available to others these photographs without the consent of the women. He thus facilitated the downloading of the material by others from BitTorrent.

The Supreme Court thereby **applied the offence of handling proceeds of crime to downloading and file sharing** by means of Torrent technology of a large number of images of a private nature of young women without their consent.

Court ruling and sentence

In determining the sentence, the Supreme Court took into account the very large number of photographs and films involved, and the large number of young and inexperienced victims, many of them having been identified. According to the Supreme Court, the potential damage that can be caused by sharing these photographs, poses a serious offence against a person's integrity. Even though the convicted had not himself posted photographs, the mere fact of downloading

them made him contribute indirectly to their dissemination. Lastly, the Supreme Court also stressed the need to ensure a general deterrent effect.

The defendant was sentenced to five months' imprisonment, 120 days of which were for the counts of receiving of proceeds of crime.

Procedure: Supreme Court of Switzerland, case no. BGer 6B_1293/2015, Switzerland

Date: 28 September 2016

Keywords: online undercover operation vs. undercover enquiry, attempted sexual acts with children

Facts

A Swiss police officer used a pseudonym and fake identity of a 14-year-old girl called 'Sabrina' for the purpose of detecting paedophile activity in online chat rooms. The suspect contacted 'Sabrina' and told her that he was looking to engage in sexual activity, following which they exchanged email addresses. The suspect subsequently sent messages and photographs, and they exchanged telephone numbers. After a few days of communicating, he arranged a meeting with 'her' to have sexual intercourse. When the suspect arrived at the agreed place and time, he was arrested by the Swiss police. During a house search, several data carriers that included child pornography were seized.

Charges

The accused was charged with attempted sexual acts with children and with partially attempted pornography.

Prior Court proceedings

The Supreme Court of the Canton of Zurich found the suspect guilty of attempted pornography, but acquitted him of attempted sexual acts with children because the disputed undercover operation required prior judicial authorisation, which was not provided. The Public Prosecutor's Office (PPO) appealed this decision, arguing that the police action online was initiated under police law, which did not require judicial approval.

Court proceedings

The key legal issue, according to the Supreme Court, is **how to qualify the operation conducted by the undercover police investigator** in light of Articles 285a and 298a of the Swiss Criminal Code (StPO) concerning, respectively, **undercover investigation** and

undercover enquiry/search. The law indeed makes a distinction between covert *search* (*verdeckte Fahndung*) under Article 298a and covert *investigation* (*verdeckte Ermittlung*) under Article 285a StPO. The former is relatively brief in time and uses simple lies about gender, age, and place of residence. The latter is much more extensive, with the objective of penetrating a criminal environment and building a relationship of trust with the targeted person, and is executed using a documented false identity (*Legende*) to investigate particularly serious crimes. Unlike the covert search, a covert investigation requires judicial authorisation under Article 285a StPO.

The Court thus had to decide whether the operation was a lawful search, or whether it constituted an investigation that should have been authorised. It assessed **four criteria** that distinguish the two definitions: the use of a documented false identity, the establishment of a trust relationship, the duration of the action, and the penetration of a criminal environment.

Firstly, with regard to the **false identity**, the Court stated that the police investigator did not use documents, such as a passport, ID card or contracts, to support his false identity. He merely used 'simple lies' about his identity to be able to act in a manner adapted to the environment. Moreover, he did not need any such documents to identify himself in the chatroom. Therefore, the first condition for covert investigation was not met.

Secondly, with regard to whether one of the objectives of the police investigator was to establish trust, the Court focused on the information he provided and the nature of the communication with the suspect. While 'Sabrina' provided personal information and 'her' e-mail address and telephone number, these data are still relatively anonymous and cannot be considered to reach the required level of trust. Moreover, since the objective of the communication was essentially to initiate sexual contact, this type of relationship is not of such a nature as to build a level of trust. The Court thus concluded that a **relationship of trust was not established** in this case.

Thirdly, the two communicated with more than 180 short text messages over a span of nine days. The Court therefore considered the **operation to be relatively brief** in the sense of Article 298a StPO.

Finally, the online chatroom is not a criminal environment, but a legal, publicly accessible environment that is abused by individual users. Therefore, the **criterion of intrusion into a criminal environment was also not met**.

In conclusion, the Court did not find that the elements of a covert investigation in the sense of Article 285a were met, and that the action fell within the definition of Article 298a StPO, namely a **covert enquiry**. The police action thus did not require prior judicial authorisation. The evidence gathered through the covert enquiry could therefore be used.

Court ruling and decision

The appeal was upheld by the Supreme Court of Switzerland, which referred the case back to the lower court for a new decision.

Procedure: Supreme Court of Switzerland, case no. 6B_656/2015, Switzerland

Date: 16 December 2016

Keywords: admissibility of evidence, direct request to ISP, court order

Facts

The appellant was sentenced by the District Court to 21 months of detention for sending multiple threats via e-mail. The e-mails were sent using a Google account. The Swiss police made a direct request to the ISP to receive information about certain e-mail addresses from where the e-mails were sent, without following the MLA procedure and without prior authorisation by the cantonal court of coercive measures. Key information resulting from that request led to the identification of the suspect and his subsequent prosecution.

Prior Court proceedings

Appealing the decision, the appellant claimed before the Supreme Court that the police request for particular IP address information, such as time and location of sending the e-mails, was authorised by a court. The Supreme Court of Zurich, however, referring to Article 32 of the Cybercrime Convention and to Article 14(4) of the Swiss Law on the Monitoring of Postal and Telecommunications Traffic (BÜPF), considered that the data related to an e-mail address, particularly to identify the owner of the address, constituted non-content data (*Bestandesdaten*). The Supreme Court of Zurich therefore upheld the judgement of the District Court of First Instance, claiming that the request did not require prior authorisation by a court.

Court proceedings

In the present case, the main consideration of the Federal Supreme Court of Switzerland is whether the type of data requested from the ISP necessitates prior authorisation by a cantonal court of coercive measures before the request is made.

In the case of criminal offences committed via the Internet, Swiss law requires service providers to provide enforcement authorities with all information necessary to identify the author (Art. 14(4) and 1(1-2) BÜPF). Article 14(1) BÜPF allows prosecuting authorities to request information about the holder of a telecommunication connection that is already known to them. No judicial authorisation is required for this non-content data (*Bestandesdaten*). However, Article 273(1) StPO requires prosecuting authorities to obtain such authorisation when the **data requested reveals a telecommunication connection that was previously unknown to them** (*Verbindungsdaten*). Enforcement authorities must thus obtain **judicial authorisation** when they have no known Internet connection of the suspect, for example if a request of IP history is necessary to acquire knowledge of the IP address and registered customer that corresponds with the criminal Internet communication.

In the present proceedings, the enforcement authorities received previously unavailable data from the ISP, which contained the IP addresses and providers used to generate the addresses

and send the criminal e-mails. **Because of the request to the ISP, the authorities were able to identify the connection of the suspect and, subsequently, the location from which the e-mails were sent**. The data acquired through the request thus constituted traffic data (*Verbindungsdaten*), the request for which the conditions laid down in Article 273(1) StPO apply, including the requirement that it is authorised by a Court. In accordance with Article 277(2) StPO, since the Swiss enforcement authorities did not obtain such authorisation, the Court rules that the **data is not admissible as evidence**.

Court ruling and decision

Ruling in favour of the appellant, the Federal Supreme Court annuled the sentence imposed by the Supreme Court of the Canton of Zurich, and referred the case back to it for a new decision.

Procedure: Supreme Court of Switzerland, case no. 1B_29/2017

Date: 24 May 2017

Keywords: use of password to access Facebook account, admissibility of evidence

Facts

In early 2016, a Swiss national was arrested on suspicion of drug trafficking. While awaiting his trial in prison, the suspect sought to communicate with potential co-defenders. He wrote his Facebook (FB) user name and password on a piece of paper and tried to smuggle it out of prison to a contact person. However, the note was passed on by prison staff to the Swiss enforcement authorities, who used it to check the FB chats of the suspect.

Defence

The defence argued that the public prosecutor had used his FB credentials to access his FB account without his consent. Moreover, the PPO had done so without having a proper legal basis for performing an internet search and the searching and securing of chat messages. Also, the accused claimed that the note contained private information and as such should not have been read due to protection of confidentiality.

The defence argued that the messages collected online were in fact electronic records stored on servers abroad, and therefore an MLA request should have been sent to the USA in order to receive the data.

Court proceedings

The Court first examined **how the FB credentials and the chat messages were obtained by the PPO**. It established that the PPO did not collect the credentials or the messages via online telecommunications surveillance. The Court then continued by stating that the accused never intended to seal the note in view of procedural secrecy, but instead wanted to use it for collusion purposes. This is proven by the fact that he tried to smuggle the note out of prison attempting to contact a third person involved in the drug trafficking activities. The Court stated that the **PPO is empowered to prevent acute collusion** and thus subsequently concluded that the **PPO was entitled to seize and use the note to check** whether the person was attempting to collude with others. Also with a view to securing evidence, the PPO was allowed to investigate the chat messages and provisionally secure them, as there were serious indications that the accused would have deleted or manipulated them if they had not been accessed without delay.

In relation to the viewing of the stored chats, the Court deems that the police, upon request of the PPO, are entitled to do so when they have obtained the password that gives access to them. Only in the event of active communication (in transit) would a judicial surveillance order be required.

With regard to the argument that the data was stored in the USA and therefore not accessible to Swiss authorities without a formal MLA request, the Court simply rules that the **use of the Internet services provided by a foreign company via internet within Switzerland does not constitute an act 'abroad'**. The Swiss investigators, from computers in Switzerland, conducted their investigation on the Internet. Even if the data is stored on servers in the USA, an online search is not deemed to exceed the territorial boundaries of Switzerland and does not require international mutual legal assistance.

In response to the accused's argument that the information is protected under so-called secrecy of telecommunications, the Court notes that such protection may be, and indeed is, outweighed by the interest of prosecution. The measures undertaken by the Swiss authorities were a proportional response to the importance of the investigation.

Following the above reasoning, the Court concluded that the evidence obtained was admissible.

Court ruling

The Supreme Court dismissed the appeal.

3.2. Other Court rulings in brief

Procedure: Court of Appeal, DPP V RMcC 2017 IECA 84, Ireland

Date: 9 March 2017

During an investigation, a car passenger was wearing a recording device while in the car driven by another suspect (owner of the car). At a certain point, the driver made a telephone call, using the car's Bluetooth device, allowing the police to listen to the conversation between the two car occupants as well as the conversation between the driver and the person on the other end of the telephone. The surveillance operation had been authorised by a judge, but the recording of the ancillary conversation was not referenced in the application for the warrant. The (First Instance) trial judge therefore excluded the evidence from trial and acquitted the accused.

The Court of Appeal, although maintaining the acquittal on the basis of the argument that the excluded evidence, if reintroduced, might not ultimately be compelling evidence, did state that what occurred was not an interception. The police did not attempt to interfere with the call or intercept the call as such.

Procedure: Supreme Court of Switzerland, case no. 6B_656/2015

Date: 16 December 2016

Swiss police authorities were investigating a case of threatening e-mails. The e-mails were sent using a Google account. The Swiss police made a direct request, without a prior judicial order, to Google (USA) to receive information about the e-mail addresses from which the threat messages were sent. The ISP provided information on the IP addresses and providers used to generate the e-mail addresses and send the e-mails. Moreover, the ISP informed the police when the email addresses and messages were created.

With this information, particularly the IP address, the investigating authorities were able to determine when and from where the e-mails were sent. The Federal Supreme Court ruled that this direct request for data was not limited to subscriber data, as the objective of the request was to receive data through which the location of the IP address, and, thus, the suspect, could be identified. The Court stated that requests for this type of data required a prior court order by the cantonal court of coercive measures. The evidence gathered from the ISP could therefore not be used. The Court consequently annulled the decision of the lower instance court and referred the case back to the court of appeal.

Procedure: Central Criminal Court, UK

Date: 25 April 2017

From 1 September 2013 to 4 March 2015, a 16-year-old boy created and managed computer software capable of carrying out distributed denial of service attacks (DDoS). He subsequently registered a service online that offered to carry out DDoS attacks against users of the World Wide Web on behalf of individual subscribers. In order to receive (and hide) subscription payments, the minor created 328 separate PayPal accounts. When handing down his verdict, the judge stated that he would have passed a total sentence of six years imprisonment. However, several factors influenced the judge's decision and, in general, the entire discussion of the case. The most decisive factor was that the accused was diagnosed with Asperger's Syndrome. The medical condition of the defendant, in combination with the defendant's age at the time of his offences and the delay between his arrest and the entering of his guilty pleas reduced the total sentence to not more than two years.

4. Data Retention developments in Europe

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

Belgium

On 17 July 2017, an action for annulment by *De Liga voor Mensenrechten* and *La Ligue des droits de l'Homme* (League for Human Rights) was submitted to the Constitutional Court against certain provisions of the Statute which amended several provisions of the Code of Criminal Procedure governing investigations on the Internet. A decision is still pending.

Germany

A Munich-based company, that provides Internet access services for business customers in Germany and other EU Member States, had filed an application for a temporary injunction with the Administrative Court of Cologne to avoid having to comply with the obligation to store data. The Administrative Court had rejected this motion, following which the applicant appealed against this decision. In its judgement of 22 June 2017, the High Court for administrative cases in Münster upheld the decision against the applicant, although mentioning in its ruling that the retention laws are possibly unlawful as conflicting with EU law after the decision of the European Court of Justice.

- Since this decision was rendered, the German authority responsible for enforcing the retention rules (voluntarily) refrains from enforcing the legislation in general until the legal situation has been finally resolved.

Italy

In a case of attempted arson, the defendant requested the Court in Padua to exclude all his external telephone communication data as evidence, as the storage of the data and access to it contravenes the right to privacy and is not allowed following the invalidation of Directive 2006/24/EC (hereinafter 'the Directive').

The Court argued that no connection exists between Art. 132 of the Italian Data Protection Code (DPC) and the 2014 CJEU ruling. In fact, Art. 132 DPC came into force before 2006, and as such cannot be considered an implementation of the Directive. Therefore, the invalidity of the Directive does not influence the effectiveness of Art. 132 DPC.

With regard to the restriction of the right to privacy, the principle of proportionality is fully considered because the acquired telephone data from the defendant had been collected by the prosecutor for the purpose of establishing the defendant's attempt to commit arson. Consequently, the Court considered that the protection of public security justified the breach of the right to privacy.

The Court rejected the defendant's request.

- This rejection was the first time an Italian judge formally considered the effect of the 2014 CJEU ruling on data retention.

Portugal

In October 2016, the request by a public prosecutor for a Court authorisation to receive (source) data from an electronic communications provider to identify a user through a particular IP address was denied. The user in question was suspected of having committed crimes in relation to child pornography. The Court rejected the request by asserting the unconstitutionality of Art. 6 of Law no. 32/2008 (the Portuguese data retention law), which transposed Directive 2006/24/EC (hereinafter 'the Directive') into national law; as well as a violation of the constitutional principles of right to privacy at home, in correspondence or via telecommunications. The prosecutor appealed the decision.

The following reasoning was put forward by the Portuguese Constitutional Court:

In relation to the constitutionality of Law no. 32/2008

The invalidity of the Directive does not automatically render invalid the Portuguese law that transposes it. National legislative acts are independently valid and legitimate. Thus, the invalidity of a national law could only be concluded after a specific, independent analysis of that law, and not following the invalidity of the Directive it transposes.

Moreover, at the time of transposition of the Directive into national law, the Portuguese legislator established rules for data access, including the definition of the concept of serious crimes, and specific guarantees for data protection, etc. Law no. 32/2008 thus introduced more extensive rules for regulating data retention, meaning that the national law goes beyond the

requirements of the Directive. Most of the considerations made by the CJEU judgement had already been considered and taken up in domestic law. Therefore, the Court concluded that the rulings of the CJEU do not affect the validity of national law.

In relation to the secrecy of telecommunications and right to privacy

The type of data requested by the prosecutor concerned 'source data', which are data including elements necessary for network access (e.g. IP address, telephone number, etc.). These data are needed for a user to be able to access and use a network, and thus do not require 'communication' as such (contrary to traffic data).

According to the Court's case law, the protection of secrecy of telecommunications does not apply to source data, as data relating to the simple identification of a user to whom a certain IP address was assigned is not covered by the scope of protecting confidentiality of communications, because this presupposes an act of communication.

The data are, however, subject to the right to privacy. Restrictions on the right to privacy need to be proportionate. The Court considered that the public interest of investigating, detecting and prosecuting serious crimes by the competent authorities, to protect democratic legality and criminal prosecution, justified the restriction of the subject's right to privacy.

The Court concluded that the Portuguese data retention law was not unconstitutional and upheld the appeal.

- The Portuguese law on data retention is still valid and applicable.

Spain

In a case of drug trafficking and bribery, traffic and location data, as well as private communication data of the suspects was provided to the judicial authorities for the purposes of criminal proceedings. The defendants claimed a breach of their right to privacy and secrecy of communications on the basis of Article 18 of the Spanish Constitution. They also claimed that their convictions were ill-founded, taking into account the annulment of Directive 2006/24/EC.

The Supreme Court pronounced its ruling on 1 June 2017 and mainly relied on case law from the Spanish Supreme Court as well as the CJEU to support its findings.

The fact that the Directive was annulled by the CJEU ruling has no impact on the national law implementing such Directive (Law 25/2007 on the Retention of Data Generated or Processed in Connection with Electronic or Public Communication Networks). Law 25/2007 provides sufficient guarantees and safeguards in line with the CJEU ruling, as data retained by communication service providers can only be used in criminal proceedings upon prior judicial authorisation and in accordance with the purposes set out in that law. As those requirements were not contemplated by the Directive, the Supreme Court takes the view that the national law provides for more guarantees than the annulled Directive.

Moreover, in the same vein, under Article 588 ter j) of the Code of Criminal Procedure, data retained by communication service providers can only be used in criminal proceedings with prior judicial authorisation.

The Supreme Court considers that the additional requirements from the second ruling of the CJEU in 2016 are not incompatible with national law, as the release of data is always subject to judicial authorisation in the framework of criminal investigations and prosecutions of serious offences.

Limitations on the fundamental right to privacy and secrecy of communications are subject to prior judicial authorisation and must be adopted in the framework of criminal investigations and prosecutions of serious offences. The investigative judge in charge of the case decides on the release of data, a decision that needs to be in line with the principle of proportionality in accordance with the Code of Criminal Procedure. The Supreme Court considers that the latter, in principle, does not seem to be incompatible with the requirement that a national legislation must not admit the general and indiscriminate retention of all traffic and location data of all subscribers and registered users with respect to all means of electronic communication.

The Supreme Court concluded that the requirements established by the CJEU are already met in national legislation and that no breach of the right to privacy and secrecy of communications on the basis of Article 18 of the Spanish Constitution has been committed.

- The invalidity of the Directive has no impact on the Spanish law that implemented the Directive, as it foresees sufficient guarantees and safeguards.

5. Topic of Interest

Online investigations into Darknet criminality

The topic of online investigations is often debated in the cyber domain, as the investigative possibilities and limitations for LEA in the virtual world are often less straightforward, different or more complex than those they can apply in traditional investigations. This section provides an overview of the investigative possibilities LEA have, as well as the practical and legal challenges authorities are faced with when conducting Darknet investigations. This overview provides a general outline and is by no means exhaustive in detailing all specific differences in the Member States and third States.

A questionnaire on this topic was distributed in 2017 to the experts of the EJCN, as well as LEA from Member States and third States. It served a dual purpose, namely to provide information for a topic on the agenda of the Darknet Conference organised by Europol on 10 October 2017, as well as input for this issue of the CJM. In total, 21 replies were received.

Legislative framework for online investigations

In most countries, the general legal provisions on special investigative measures, such as infiltration and undercover investigations, are applied by analogy to conducting online investigations. Only three countries that replied have specific legislation in place regulating investigations on the Internet.

Passive and active online presence

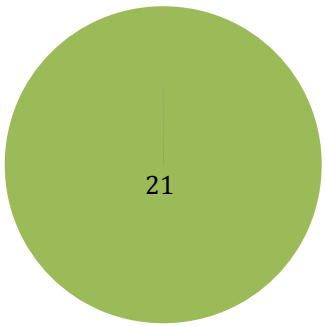
A distinction was made in the questionnaire between passive and active online presence, drawing the demarcation line at interacting with those present in the Darknet environment.

The possibilities for LEA in relation to passive online presence are roughly the same or similar in all countries. The situation is, however, different for active online presence: where more differences can be identified between countries with regard to investigative possibilities. This situation may inevitably lead to obstacles in cross-border investigations and judicial cooperation, and admissibility of evidence in court at a later stage.

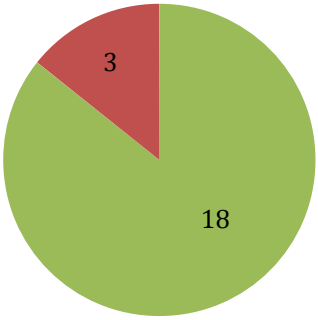
In most countries, establishing passive online presence is fully allowed and requires few or no prior conditions to be met. Establishment of passive online presence is considered to be part of the general competence of LEA, allowing them to enter and be present in publicly accessible places, as generally covered by the rules on observation. Some limitations or formal requirements do apply in several countries for establishing more intrusive passive online presence, for example when conducting surveillance in closed (non-public) online environments, in cases in which the special investigative measure is applied to investigate serious offences, or in the event of realtime monitoring or logging.

The below charts provide an overview of the different types of passive presence and whether or not they are allowed:

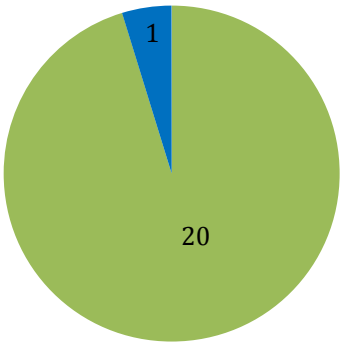
Monitoring of user activity



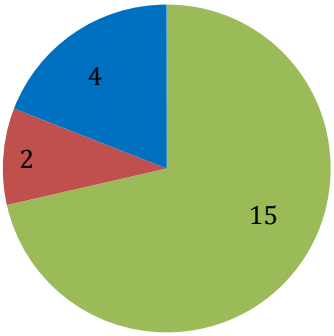
Lurking



Logging of user activity



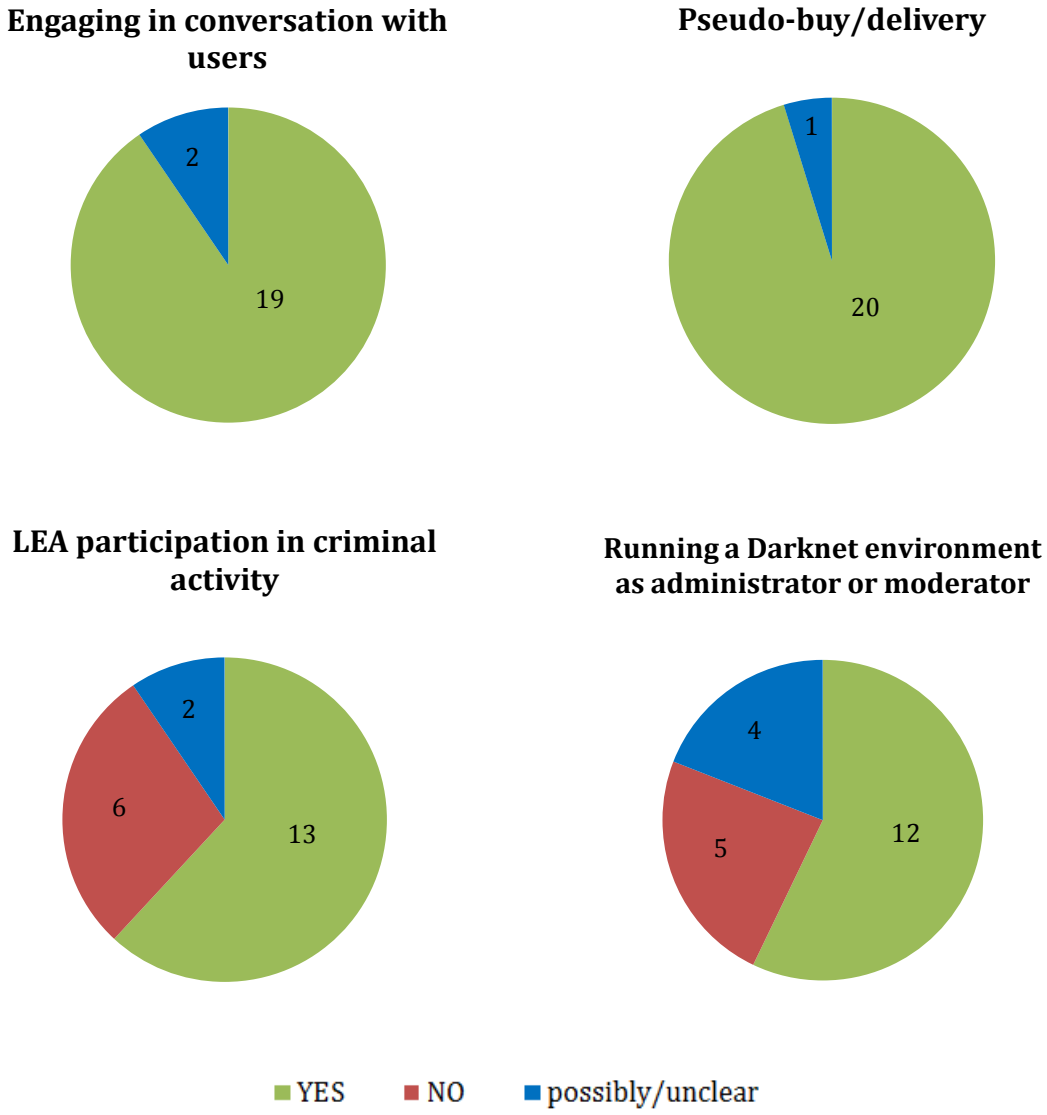
Scraping



YES NO possibly/unclear

The possibilities and practices for active online presence are more disperse in Europe. Most countries apply the legal provisions on undercover investigations, infiltration or surveillance. In general, all countries have minimum requirements that need to be met before any active presence may be established online, some of which are common to most countries: (a) the suspected or investigated offence needs to be of a particular gravity or explicitly listed in the legal provisions, (b) an initial suspicion or sufficient evidence of a crime having been committed needs to be present, (c) the intended results cannot be achieved through other means, (d) prior judicial authorization is required, (e) time limitations are in place, and (f) provocation is not allowed. Other (less commonly shared) requirements were also mentioned, such as the need to have the targeted suspects identified before establishing active presence, the need to have an open investigation, and the restriction for LEA not to commit crimes when performing online investigations.

The below charts provide an overview of the different types of active presence and whether or not they are allowed:



Two of the most intrusive forms of active online presence are the take-over and running by LEA of a Darknet forum as administrator or the take-over of vendor accounts. Sixteen respondents replied that this is or, theoretically, might be possible in their countries. However, in countries in which there is a legal limitation for LEA not to commit crimes, it is difficult in practice to do this. Also, with regard to taking over vendor accounts, one respondent replied that doing so is only possible with accounts that are no longer actively selling. Another respondent mentioned that taking over vendor accounts would be considered provocation, so such action would not be legally possible. Running a Darknet forum or taking over a vendor account implies, to a certain extent, the continuation of crime. This situation is also one of the reasons why running a Darknet

forum is not possible in some countries. The countries that do allow criminal activities to continue apply restrictions. Continuation of crime needs to be proportionate, assessed on a case-by-case basis and/or LEA must interfere as soon as possible. Some legislation does not allow crimes to be continued when doing so would entail a threat to life, the health of a person or serious harm.

LEA and judicial authorities are faced with several legal and practical challenges when establishing passive or active online presence. Listed below are the most important or referenced ones:

- *Legal challenges:*
  - Application of general legal provisions/lack of legal provisions/lack of specific legislation for online investigations
  - Jurisdiction issues
  - Need for (suspicion of) crime to have been committed
  - Need for knowledge of identity of persons investigated (to include in judicial order), which is often difficult due to online anonymity
  - LEA not allowed to commit crime/no provocation
  - Coordination between MS to avoid overlapping/hindering other investigations
  - Consider how long crime can continue

- *Practical challenges:*
  - Setting up/taking over account or forum in a credible way, which does not raise suspicion
  - Encryption and anonymisation hinder access to the Darknet, identification of users, as well as their location
  - Technicalities of operations
  - Tracing of virtual currencies
  - Protecting agent's identity
  - Administrative burden to get false documents for the creation of false identity
  - Lack of resources/capacity/training
  - Efficient evidence collection
  - Data retention issues
  - Measure is (too) limited in time

Use of private citizens

Although not possible in at least six countries, and several other countries have limited or no experience with it, LEA do sometimes make use of the assistance of private citizens if conducting online investigations. The legal provisions on informants or private experts are applied for this purpose. Most countries however do not allow private citizens to commit crimes or participate in a criminal organisation. The fact that many countries do not make use of private citizens' assistance stems from the significant challenges linked to it. First of all, legal provisions, or the absence of any, hinder the actual use of private citizens. Secondly, private citizens may not

always be aware of the legal limitations that apply when acting online in such a context. They might, for example, not know to what extent actions could be perceived as provocation. Moreover, exerting control over the actions of private citizens is difficult. All the foregoing challenges could pose risks for the admissibility of the evidence gathered.

Umbrella investigations and joint investigation teams (JIT)

Conducting umbrella investigations is possible in 16 countries, subject to certain conditions. In at least six of these countries, such (general) investigations can only be conducted at LEA level, and not at prosecutorial level, for the purpose of finding elements of crime and intelligence collection. If a reasonable suspicion exists of a crime being committed by (a) specific person(s), the prosecutor will need to initiate a criminal (spin-off) investigation, which can no longer be 'general' at that stage. One respondent mentioned that an umbrella investigation can be conducted in the form of joint proceedings of related criminal offences. Only one country reported having specific legislative provisions governing umbrella investigations.

Protection of such umbrella investigations is usually guaranteed by creating spin-off investigations to keep the umbrella investigation secret. In addition, rules on non-disclosure of sensitive information may be applied, and authorities will, in practice, agree on timing and coordination of actions so that parallel investigations are not exposed or hindered. Alternatively, the suspect's right to access the case file may pose a problem in certain situations.

All respondents considered JITs to be a useful tool for conducting Darknet investigations, because of the cross-border nature of the crime and consequential need to coordinate investigations across countries with different legal jurisdictions.

Five respondents highlighted that umbrella and spin-off investigations could limit participation in a JIT. Firstly, in some countries, a JIT can only be established in spin-off investigations and not in an umbrella investigation, because of the specific requirements for a JIT. In addition, the different legal systems with different rules on handling confidential information and collection of evidence can create obstacles to cooperation within the JIT.

The main challenges reported with regard to umbrella investigations and JITs in the context of Darknet operations are the following:

- *Legal challenges:*
  - Integrate different jurisdictions participating in a JIT
  - Different rules on confidentiality
  - Procedural problems when the umbrella and spin-off investigations are conducted by different authorities within one country
  - Umbrella investigations not possible at prosecution level
  - Not possible to set up JIT within an umbrella investigation
  - Not possible to keep persons in custody on the basis of information from another (separate/spin-off) investigation

- *Practical challenges:*
  - Decision-making in the event of many JIT participants
  - Information-sharing between JIT participants
  - Investigations in countries at different stages
  - Preparation of the JIT agreement is complex, time consuming and an administrative burden
  - Spin-off investigations need to wait to go to court until the umbrella investigation can be disclosed

Virtual currencies

Most authorities integrate investigation of virtual currencies into their Darknet investigations. Two main challenges to virtual currency investigations, which were highlighted by many respondents, are the lack of (national and EU-level) regulation of virtual currency status and lack of legislative provisions and procedures for seizure and management of seized virtual currencies.

Other reported challenges were:

- Unclear which jurisdiction applies for seizure of the virtual currencies (location of currencies)
- Obtaining access to and seizing a wallet is problematic because of encryption, two-way authentication, back-ups, etc.
- Identification of users
- Proving a link with criminal activities
- Non-cooperating, bulletproof or fraudulent exchangers
- Awareness and training of LEA on virtual currency investigations
- Lack of resources
- Difficulties with tracking the virtual currency flow
- Technical issues: analysis of blockchain when mixers are used
- Blockchain analysis tools are expensive or LEA only use publicly available tools

CONCLUSIONS

Out of the 21 replies received, it can be concluded that online investigations into Darknet criminality are essential in the fight against online criminality and cybercrime. Most countries are applying general legal provisions to the online environment. Given the fact that crimes committed on the Darknet are inevitably cross-border in nature, countries need to cooperate to effectively investigate and prosecute cybercriminals. Investigative tools such as umbrella investigations and JITs have proven useful in this respect. Clearly however, LEA and judicial authorities are faced with multiple problems, legal as well as practical, when conducting such investigations. Further discussions among practitioners on this topic would therefore be beneficial to see how some of these main challenges could be resolved.

6. The Way Ahead

As of 2017, the Cybercrime Judicial Monitor will be published once per year. It is distributed to LEA and judicial authorities active in the cybercrime domain. It can also be accessed on the restricted website of the European Judicial Cybercrime Network.

The focus of future issues of the CJM will remain on legislative developments in the area of cybercrime and the analysis of relevant court decisions. The topic of interest will be determined at a later stage, 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 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 the valuable contributions they provided for this CJM.

Eurojust December 2017

Catalogue number: QP-AG-19-003-EN-N
ISBN: 978-92-95084-00-1
ISSN: 2600-0113
DOI: 10.2812/673417