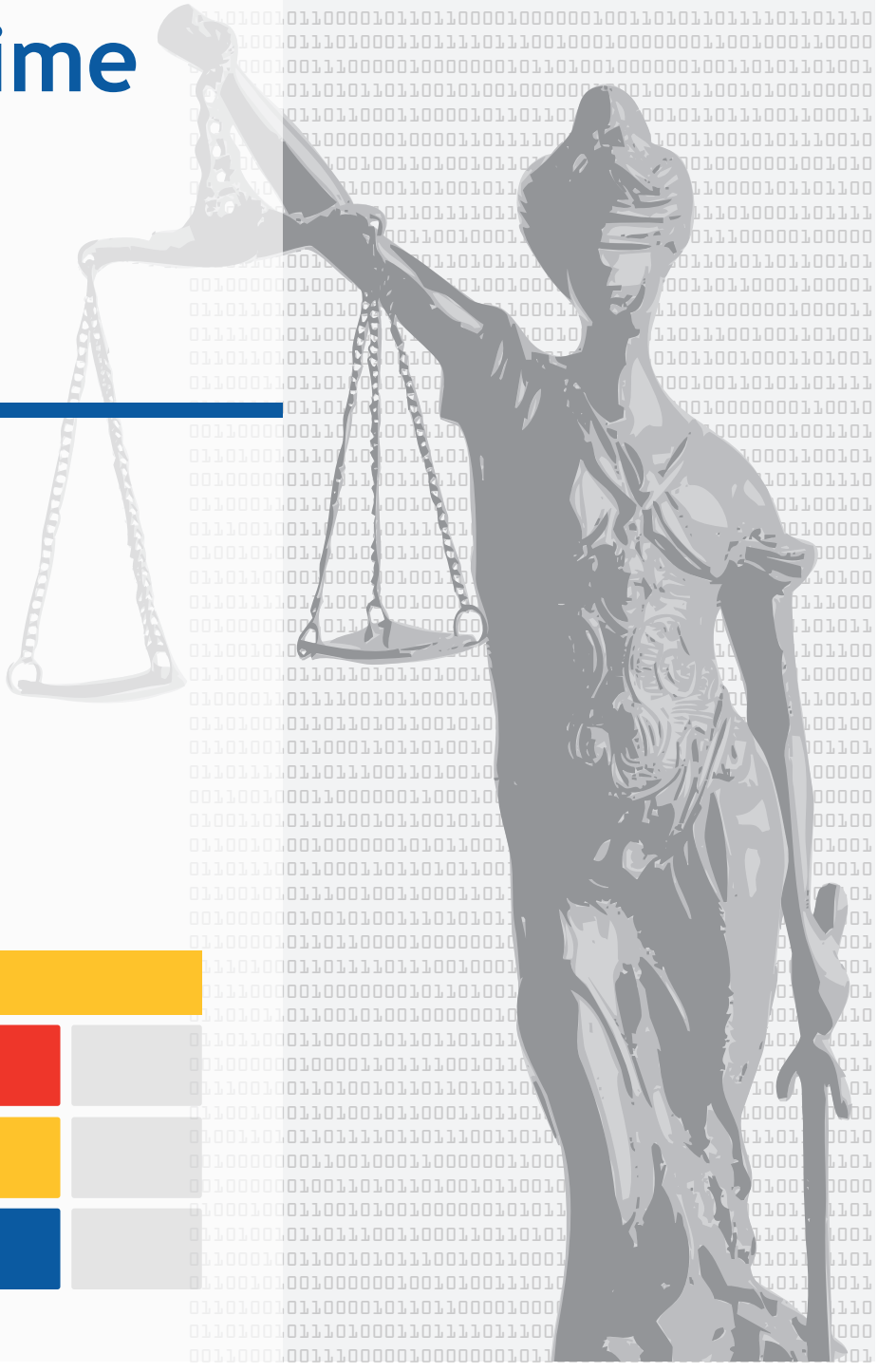
Cybercrime Judicial Monitor

Issue 4 - December 2018



Contents

1. Executive Summary

Eurojust presents this fourth 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. It is produced on the basis of information provided by members of the European Judicial Cybercrime Network (EJCN).

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 2018.

The judicial analysis section presents legal analyses of court rulings rendered by courts in different Member States. The courts ruled on different cyber-related matters such as law enforcement authorities (LEA) accessing an e-mail account with found credentials, or accessing a device by use of a suspect's fingerprint and covert investigation. In a Swedish case, the court qualified the fact of forcing children to perform online sexual acts on themselves as rape. In addition, the European Court of Human Rights ruling in the case of *Benedik v. Slovenia* is analysed in detail. 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. A preliminary ruling of the Court of Justice of the European Union, following interlocutory questions made by a Spanish court, is analysed and an overview is given of other national legal and case law developments.

The topic of interest in this issue of the CJM is the role of encryption in criminal investigations. The chapter details the legislative landscape in relation to bypassing and attacking encryption, as well as issues encountered.

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 2018. The main sources of information presented in this section are contributions collected through the EJCN, unless specifically stated otherwise.

2.1. EU Level

European Commission

On 17 April 2018, the Commission published proposals for a Regulation and a Directive in relation to e-evidence-gathering in criminal matters. The objective of the Commission, with these 'e-evidence proposals', is to adapt cooperation mechanisms to the digital age, and to overcome certain obstacles with which law enforcement and judicial authorities are faced when gathering e-evidence for the purpose of investigating crimes.

At the time of drafting this CJM, the e-evidence proposals were under discussion at the Council.[1]

Source: EUR-Lex

- **Regulation of the European Parliament and of the Council on European production and preservations orders for electronic evidence in criminal matters**

The proposed Regulation introduces the European production and preservation orders for collecting cross-border electronic evidence in criminal matters within the European Union, regardless of the location of the data.

A judicial authority in one Member State (MS) will be able to address a mandatory cross-border order directly to a service provider offering services in the European Union or its legal representative in another MS:

- via a **European preservation order**, to preserve specific data in view of a subsequent request to produce this data. Service providers should preserve the data as long as necessary to produce the data upon request, provided that the issuing authority confirms within 60 days after having issued the order that it has launched the subsequent request for production; or

[1] On 7 December 2018, the Council agreed its position on the proposal for a regulation.

- via a **European production order**, to obtain electronic evidence within 10 days, and within six hours in cases of emergency (imminent threat to life or physical integrity of a person or to a critical infrastructure).

All types of data stored by service providers can be ordered to be preserved and produced: subscriber data, access data, transactional data and content data. More stringent conditions are to be met for the production of data of a more sensitive nature (transactional and content data). European preservation orders, regardless of the data category, and European production orders, for subscriber and access data, can be issued or validated by a prosecutor, judge or court. European production orders, for transactional and content data, **can only be issued or validated by a judge or a court**.

Preservation and production of **data** that is already **stored** at the time of receipt of the order can be requested, but not data that will be stored in the future or real-time interception.[2]

The proposal covers **service providers** that provide opportunities for interaction between users, i.e. communication services, storage of data and internet infrastructure services. The Regulation only covers such service providers that are **offering services in the European Union**, enabling the use of services in one or more Member States (MS) and/or having a substantial connection to the European Union.

A service provider has only limited circumstances in which non-compliance with an order is permitted or enforcement of an order can be opposed.

In the event of non-compliance with an order, an **enforcement procedure** can be initiated. In this situation, the issuing authority decides to pursue enforcement via the enforcing authority (the competent authority of the MS in which the service provider is established or has its legal representative appointed).

- **Directive of the European Parliament and of the Council laying down the rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings**

The proposed Directive introduces an obligation for service providers that are offering services in the European Union to designate a legal representative in the European Union. This legal representative will be responsible for receiving/complying with preservation and production orders on behalf of the service provider(s). The Regulation and Directive are complementary, as the designation of a legal representative under the Directive facilitates the receipt of, compliance with and enforcement of orders issued on the basis of the Regulation. This situation will provide legal certainty for law enforcement and service providers, as the same rules will be applied to all service providers offering services in the European Union. The Directive is proposed under Title IV, Chapter 2 TFEU (internal market).

[2] Reconfirmed at the JHA Council meeting held on 11-12 October 2018.

2.2. Member States

Austria

Section 135 para 2a and Section 135 para 2b of the Austrian Code of Criminal Procedure

On 1 June 2018, two new legal provisions of the Code of Criminal Procedure (CPC) concerning communications data entered into force.

The new Section 135 para 2a CPC regulates the use of an IMSI-Catcher to obtain the geographical location or the IMSI-Number of a suspect. This clarification is only legal. The use of an IMSI-Catcher was already possible under the general provisions of Section 135 para 2 CPC.

The new Section 135 para 2b CPC introduced a new investigative measure for retaining telecommunication data based on probable cause (Quick Freeze). If an initial suspicion exists that specific criminal activities have been committed, telecommunication providers shall be obligated, upon order of a public prosecutor, to store telecommunications data (traffic data, access data and location data) for up to 12 months. Should the suspicion be substantiated, such data may subsequently be unfrozen by court approval. Should initial suspicion not be substantiated, the public prosecutor's order shall cease to be in force, and the suspect shall be informed about the incident.

Latvia

Section 243, paragraph 5 Criminal Law

On 1 January 2018, an amendment to paragraph 5, Section 243 of the Criminal Law entered into force. According to this paragraph, the offences in Section 243 related to 'interference in the operation of automated data processing systems and illegal actions with the information included in such systems' are now punishable with a higher sentence if committed by an organised group.

Luxembourg

Article 48-26 and 48-27 of the Luxembourg Code of Criminal Procedure, introduced by the Law of 27 June 2018 in relation to terrorist matters

Since 1 January 2018, two new provisions have been incorporated in the Code of Criminal Procedure. Article 48-26 CPC covers undercover investigations online. Article 48-27 CPC provides the possibility to gather from service providers: (i) the identification of the subscriber or the usual user of an electronic communications service or the means of electronic communication used, and (ii) the identification of the electronic communications services to which a particular person subscribes or which are customarily used by a specified person.

Such information must be provided and updated on a daily basis by the relevant service providers and will be stored on a platform operated by the State.

Netherlands

'Computer Crime Act III' amending the Dutch Criminal Code and Code of Criminal Procedure with a view to improve and reinforce investigations and prosecutions of cybercrime

The Computer Crime Act III recently passed the Dutch Senate, and will enter into force in the near future (most likely 1 January 2019).

The intention of this law is to improve the investigative powers and prosecution of cybercrime. The law includes some changes to the Criminal Code. New or amended provisions will be introduced on publishing of non-public data, the fencing of data and online fraud. The definition of child grooming is also amended to make contact with an undercover agent posing as an adolescent punishable by law.

In the Code of Criminal Procedure, hacking as an investigative method will be added. This feature of the new law generated the most interest, and it was heavily discussed in parliament. This provision might bring a solution in some cases, overcoming issues with encryption, continually changing networks and anonymising tools as well as jurisdiction issues. In addition, a provision including the possibility to order a takedown of criminal content is added.

2.3. Third States

USA

Clarifying Lawful Overseas Use of Data (CLOUD) Act

On 23 March 2018, the US Congress adopted the Clarifying Lawful Overseas Use of Data Act (CLOUD Act). The CLOUD Act introduced two main changes/novelties when requesting (content) data from US service providers:

- US service providers are obliged to comply with US orders to disclose content data regardless of where such data is stored. The CLOUD Act thereby clarifies the authority that might issue search warrants.
- Under certain conditions, executive agreements with foreign governments can be concluded, on the basis of which foreign authorities can request US service providers to deliver content data using domestic orders, thus without having to resort to MLA. This basis applies to all types of data, stored or real-time interception, but only pertains to data of non-US persons.

With regard to these executive agreements, broad general support is expressed at EU level for a common EU approach in this matter (EU agreement), rather than EU MS concluding bilateral agreements with the USA. The Commission is requested to present a negotiation mandate for a possible EU agreement with the USA under the CLOUD Act.

This Act will allow EU authorities to (swiftly) obtain content data from US service providers without resorting to MLA procedure.

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: Constitutional Council, decision n° 2018-696 QPC, France

Date: 30 March 2018

Key words: encryption, *nemo tenetur* principle

Question put to the Constitutional Council

The appellant claims that the Article 434-15-2 Criminal Code, in so far as it sanctions the refusal of a person suspected of an offence to hand over to the judicial authorities, or to implement at their request, a decryption key that may have been used to commit that offence, would infringe the right to remain silent and the right not to incriminate himself (*nemo tenetur*). This provision would be contrary to the right to a fair procedure, guaranteed by Article 16 of the 1789 Declaration of the Rights of Man and Citizen and to the principle of the presumption of innocence guaranteed by Article 9 of the same declaration. Finally, these same provisions would also violate the right to privacy and the secrecy of correspondence, the rights of the defence, the principle of proportionality of sentences and freedom of expression.

The Constitutional Council thus examined the question of whether Article 434-15-2 CC was constitutional.

French Law

The concerned Article 434-15-2 of the Criminal Code reads as follows:
'Shall be punished by three years' imprisonment and a fine of €270,000 anyone who has knowledge of the secret code to decrypt a means of encryption that may have been used to prepare, facilitate or commit a crime or offence, and refuses to hand it over to the judicial authorities or to apply it, upon the request of those authorities issued pursuant to Titles II and III of Book I of the Criminal Procedure Code.
If the refusal is made when the handover or application of the decryption key would have prevented the commission of a crime or offence or limited its effects, the penalty is increased to five years' imprisonment and a fine of €450,000'.

Court proceedings and ruling

The Constitutional Council first recalls Article 2 of the 1789 Declaration: the purpose of any political association is the preservation of the natural and imprescriptible rights of man. These rights are freedom, property, safety, and resistance to oppression. The freedom proclaimed by this Article implies the right to respect for private life and the secrecy of correspondence. To comply with the Constitution, infringements of these rights must be justified on grounds of general interest and implemented in a manner adequate and proportionate to that objective. Article 9 of the 1789 Declaration concerns the *nemo tenetur* principle, from which the right to silence is derived.

The first paragraph of Article 434-15-2 of the Criminal Code, as seen from the case law of the Court of Cassation, also applies to a suspect.

The Court reasons that the legislator has pursued the objectives of the constitutional value of crime prevention and the search for the perpetrators of offenses. In doing so, two conditions were incorporated in the concerned Article with a view to safeguarding the rights and principles of constitutional value. The requirement to hand over or apply the decryption key only applies if the means of cryptology is likely to have been used to prepare, facilitate or commit a crime or misdemeanor, and only if the request comes from a judicial authority.

The Court argues that the provisions impose on the suspect the obligation to issue or to apply the decryption key only if the fact is established that he has knowledge of it. The Court continues that the provisions are not intended to obtain confessions from the suspect and carry neither recognition nor presumption of guilt but only allow the decryption of encrypted data. Moreover, the investigation or instruction must have identified the existence of data processed by means of cryptology that may have been used to prepare, facilitate or commit a crime or offence. Finally, these data, already fixed on a data carrier, exist independently of the will of the suspect.

The Court concluded from the foregoing that the contested provisions do not affect the right not to incriminate oneself or the right to respect for private life and the secrecy of correspondence.

Procedure: Court of First Instance The Hague, case 09/818727-17, Netherlands

Date: 12 March 2018

Keywords: unlocking telephone with finger by force

Facts

The defendant physically abused his partner on several occasions and intentionally removed the children from the custody of the mother, picked them up from school and brought them to a family member. They were then locked in a room, and were found by the police later that day.

Note: The current analysis will only focus on the cyber element of the case, and not go into further substantial details.

Evidence

The police wanted to unlock the suspect's telephone. They first asked the suspect whether he wished to cooperate. He refused to do so. They then ordered the accused to cooperate in unlocking the telephone and placed the accused against the wall to prevent further escalation, since the accused was physically resisting. When placing the accused's thumb on his telephone, the police saw that the accused tried to destroy his telephone and, with it, any evidence. The police prevented this situation, after which the defendant cooperated and, after attempts to unlock the telephone by his fingerprint failed, entered the code of his telephone.

Defence

The defendant claimed that the police, by forcing him to unlock his telephone, violated his rights under articles 3, 6 and 8 ECHR.

Court proceedings

The Court concluded on this point that no violation of article 3, 6 or 8 ECHR occurred. The accused was suspected of very serious acts, including the unlawful deprivation of liberty of two young children, and, at the time when his cooperation in unlocking his telephone was requested, the police had no idea about the location of the children. Therefore, the location of the children was urgently needed. In such a situation, some coercion is permitted and also necessary. The police did not appear to have acted disproportionately. The Court was therefore of the opinion that the limited use of force was proportionate and lawful.

Note from the NL EJCN member: This decision is the first regarding the use of biometric data from a suspect to unlock a device. In this case, involving the urgent matter of two missing children, the Court ruled the limited use of force proportionate and lawful.

Procedure: Supreme Court, case 17/02592, Netherlands

Date: 29 May 2018

Keywords: LEA finding password and logging on to e-mail account

Rulings Court of First Instance and Court of Appeal

In this case, the defendant was convicted for murder and attempt to persuade another person, through gifts and by providing information, to commit murder. He was sentenced to 24 years' imprisonment (first instance and appeal procedures). The defendant appealed the decision and the case was brought before the Supreme Court.

Evidence

During the investigation, the police seized the defendant's telephone, on which they found a WhatsApp conversation. In that conversation, the defendant gave a clue to the other person about his password for his Hotmail account. The investigating judge was requested to provide an authorisation, on the basis of Article 177r CPC, for recording of (future) communication of (amongst others) historical information via the e-mail address of the defendant. The police subsequently tried to access the defendant's e-mail account by testing several passwords, one of which was the correct one.

Defence case

The defence argued that the police did not lawfully access the defendant's e-mail account, as they did so following an authorisation given on the basis of Article 177r CPC, and not on the basis of Article 177s CPC, concerning the authorisation to request service providers to provide stored data. As a consequence, a procedural error occurred and should lead to the inadmissibility of the obtained evidence.

Court proceedings

The Supreme Court stated that the authorisation as stipulated in Article 177s CPC would no longer have served any purpose, as the police already had access to the data by logging in with the password, and, therefore, requesting the data from a service provider was not necessary. In this sense, according to the Court, no procedural error occurred.

In cases in which a procedural error was made, the Court determines whether any consequences should follow from that error. The Court at that point needs to take certain elements into account, such as the underlying interest of the legal provision, the severity of the error, and the damage caused. The Court would only render the evidence inadmissible if the unlawful evidence-gathering would have violated an important principle of law.

The Court continued by arguing that, even if a procedural error had been made, which would imply a violation of article 8 ECHR concerning the right to privacy, this situation does not (automatically) mean that the defendant's right to a fair trial (article 6 ECHR) has been violated. Only in exceptional cases can this lead to such a violation. The Court therefore did not render the evidence inadmissible.

Court ruling and sentence

The Supreme Court rejected the appeal.

Note from the NL EJCN member: This case addresses a common cyber-related problem in law enforcement investigations, namely whether or not logging on to an e-mail account belonging to a suspect when in possession of the login credentials is permitted.

Dutch law foresees the possibility to request service providers to provide content (e.g. of an e-mail account); however, no specific provision allows police to log on to accounts and get that content themselves. In this case, an investigative judge was consulted beforehand and approved the interception of communication. However, this authority does not provide for interception of stored communications.

Procedure: ECtHR, case of *Benedik v. Slovenia* (application no. 62357/14)

Date: 24 April 2018

Key words: dynamic IP address, judicial order

Facts

In 2006, Swiss law enforcement authorities conducted a monitoring exercise of users of the so-called 'Razorback' network. The Swiss police established that some of the users owned and exchanged child pornography in the form of pictures or videos. Files containing illegal content were exchanged through a peer-to-peer file-sharing network. Among the dynamic Internet Protocol ('IP') addresses recorded by the Swiss police was a dynamic IP address later linked to the applicant.

Based on the data obtained by the Swiss police, the Slovenian police, without obtaining a court order, requested a Slovenian Internet Service Provider (ISP) to disclose data regarding the user to whom the above-mentioned IP address had been assigned. The Slovenian police based their request on section 149b(3) of the Criminal Procedure Act (CPA), which requires the operators of electronic communication networks to disclose information to the police regarding the owners or users of certain means of electronic communication whose details were not available in the relevant directory.

Slovenian law

Section 149b(3) of the Criminal Procedure Act:
If there are grounds for suspecting that a criminal offence for which a perpetrator is prosecuted ex officio *has been committed or is being prepared, and information on the owner or user of a certain means of electronic communication whose details are not available in the relevant directory, as well as information on the time that the means of communication was or is in use, needs to be obtained in order to uncover this criminal offence or the perpetrator thereof, the police may request that the operator of the electronic communications network furnish them with this information, at their written request and even without the consent of the individual to whom the information refers.*

National Court rulings

At the Kranj District Court hearing of 8 October 2008, the applicant lodged a written request for exclusion of evidence obtained unlawfully, including the information concerning the user of the IP address obtained without a court order. The court rejected the applicant's request, finding that the data concerning the user of the IP address had been obtained in compliance with Section 149b(3) of the CPA. The Court found the applicant guilty of the criminal offence with which he had been charged.

The Ljubljana Higher Court confirmed that the first-instance court had correctly established the facts of the case; moreover, it held that the data concerning the user of the IP address had been obtained lawfully, as no court order was required for such a purpose.

The applicant lodged an appeal on points of law before the Supreme Court, claiming that a dynamic IP address should be considered as traffic data, as a new IP address is assigned to a computer every time a user logs on. Such traffic data is connected to electronic communication to which the protection of privacy of communication applies (Article 37 Slovenian Constitution). The Slovenian police should consequently have obtained a court order to obtain the data on the identity of the subscriber associated with the IP address. The Supreme Court dismissed the appeal on the points of law. In its view, the Slovenian police had not acquired traffic data about the applicant's electronic communication, but only data regarding the user of a particular computer through which the Internet had been accessed.

The applicant lodged a constitutional complaint before the Constitutional Court. The Constitutional Court pointed out, at the outset, that in addition to the content of communications, Article 37 of the Constitution also protected traffic data. It considered that IP addresses were included in such traffic data. The Constitutional Court, however, concluded that the applicant, who had not hidden in any way the IP address through which he had accessed the Internet, had consciously exposed himself on the (public) Internet and could not legitimately have expected privacy. As a result, the data concerning the identity of the user of the IP address

were not protected as communication privacy under Article 37 of the Constitution, but only as information privacy under Article 38 of the Constitution, and no court order was required to disclose them in the applicant's case. The Constitutional Court thus dismissed the applicant's complaint, holding that his constitutional rights had not been violated.

Ruling European Court of Human Rights

The applicant complained that his right to privacy had been breached because the police had obtained subscriber data associated with his dynamic IP address and consequently his identity arbitrarily, without a court order, in breach of article 8 ECHR.

The Court stated that a dynamic IP address falls under the protection of article 8 ECHR, as the applicant reasonably expected that his sharing of files would remain private and that his identity would not be disclosed. The Court thus did not follow the Constitutional Court's reasoning in this respect.

Given the fact that article 8 ECHR applies, interference by a public authority is only allowed insofar as it is prescribed by law and necessary in a democratic society. The Court notes that (a) no regulation specifying the conditions for the retention of data obtained under section 149b(3) CPA and (b) no safeguards against abuse by State officials in the procedure for access to and transfer of such data were in place. Furthermore, no independent supervision of the use of police powers was in force.

The Court concluded that the Slovenian law on which the contested measure was based and the way it was applied by the domestic courts lacked clarity and did not offer sufficient safeguards against arbitrary interference with article 8 rights.

Note from the SI EJCN member: the main recommendation for police after the ECtHR judgement is to always obtain a court order to get information on a user of a specific IP address from an ISP. No distinction shall be made between static and dynamic IP addresses.

Procedure: Court of Appeal Stockholm, case B 11734-17, Sweden

Date: 16 April 2018

Key words: forcing children to perform online sexual acts on themselves qualified as rape

Facts

A 41-year-old Swedish man searched for girls in a specific age range on websites that offered people the opportunity to connect with each other based on common interests. The suspect

subsequently approached his victims by sending them private messages threatening to post pictures of them on pornographic websites or to kill their relatives unless they performed sex acts in front of the webcam. When the victims obeyed, he watched and directed them from his home in Sweden. In most cases, the victims performed the sexual acts on themselves, alone in a room. He also recorded everything on his computer.

The international case came to light when the suspect was being investigated for another coercion case involving Swedish victims. During that investigation, police found videos at his home of English-speaking girls. The investigation in the case involved close and productive cooperation between international authorities and partners, such as the Department of Justice, police officers, child interviewers and forensic investigators.

Swedish Law

In Sweden, rape is defined as 'a sexual act that is deemed *equally violating* as intercourse', a sexual act that, having regard to the nature of the violation and the circumstances in general, is comparable to sexual intercourse. The sentence for rape is imprisonment for at least two and at most six years.

Court proceedings

The Court stated that online sexual acts performed by child victims on their own bodies can be *equally violating* as intercourse and outlines what is legally required for such an act to be regarded as rape. The Court took into consideration relevant factors, such as the victim's age, if the act caused them pain, the degree of humiliation (including what objects were used, the risk of exposure, the nature of the act and which words the suspect used) and that the event was monitored and documented by the suspect.

Recent research from Sweden and Great Britain shows that the victim's trauma often is connected to the fear of being confronted with images from the assault in the future.

The suspect admitted coercing most of the teens — all under age 15 at the time — but denied his actions constituted rape.

Court ruling and sentence

The Svea Court of Appeal convicted the accused to 10 years' imprisonment, guilty of 59 different sex crimes against Canadian, American and British girls, entirely through online contact. The verdict includes four convictions of aggravated rape of a child, and 12 convictions of rape of a child or rape, depending on whether the victim was younger or older than 15.

Note from the SE EJCN member: This verdict sets a precedent. It marks one of the first known times that someone has been found guilty of the offence of rape without the perpetrator or anyone else being physically in the room with the victim. Similar verdicts have come from courts in Norway.

Procedure: Appeal Court, High Court of Justiciary, HMA v IP [2017] HCJAC 56, United Kingdom

Date: 18 July 2017

Key words: covert investigation, entrapment

Facts

The accused was indicted at Falkirk Sheriff Court, charged with contravention of section 30 of the Sexual Offences (Scotland) Act 2009 by engaging, between 25 and 31 May 2016, in online conversations with 'other persons', arranging to meet these persons 'for the purpose of gaining access to a 14 year old girl', travelling, with condoms and lubricant, to, and attempting to meet the other persons at, a hotel 'for the purpose of engaging in sexual activity with a child'. There was an alternative libel of conspiracy to participate in such conduct.

On 6 June 2017, the judge at first instance (Sheriff) sustained a plea in bar of trial based upon the entrapment of the accused. The essence of the plea was that the accused, who was not predisposed to commit the crime, was lured or incited by undercover police officers, using a website to converse about the prospect of engaging in sexual activity with a 14-year-old. The prosecution (Crown) appealed that decision.

Evidence

The police were investigating a website following reports that certain communications on it, between two unnamed persons, contained messages relating to the sexual abuse of children. Following the execution of several warrants and the recovery of computer equipment from these two persons, a large number of chat logs were examined to see if any others had an interest in such abuse. Nineteen persons were regarded as being 'of concern'. They were divided into those of medium and high risk. The accused, who was a teacher, was one of those in the medium-risk category. The message content of his chat did not involve children, but included animals. However, the accused had had contact with one or both of the two persons originally identified as having expressed an interest in the abuse of children. Authority was given to conduct an undercover operation.

The evidence was in the form of chat logs between the accused and the covert internet investigator from the police (a/k/a 'Lisa') on various dates in May 2016. These included chats about several deviant sexual practices which, the sheriff observed, most people would consider 'highly unpleasant and indeed repellent'. Those were not relevant for purposes of the case, but references to children were relevant. On 24 May, in the course of general sexual chat, Lisa mentioned that she had a daughter and a dog. No discussion of a sinister nature about the child occurred. Further chat took place the following evening, again involving nothing of note.

On the evening of 26 May, Lisa asked the accused what he was 'into'. The accused referred to a number of sexual practices, but none involving children. Lisa asked him about his fantasies. The involvement of the dog was mentioned, but none regarding children. The first reference to the daughter was when Lisa used her fictional presence to avoid online camera contact. The accused and Lisa then attempted to arrange a meeting, but Lisa said that her daughter would be in the house. The accused asked about her bedtime, suggesting that sexual contact would only take place after the daughter was out of the way. He asked Lisa if she would be comfortable engaging in sex while her daughter was in the next room. The following exchange took place:

'Lisa: But how would you feel if she came in?

Accused: Surprised – but I'd carry on doing whatever xx.

Lisa: With me or her?

Accused: With you ... I wouldn't run away though if she wanted to join in.'

A short chat took place about sexual activity between the accused, Lisa and her daughter, in which the accused stated that he had not previously been involved with an under-age girl. Lisa proposed meeting the accused with her daughter and husband at her house on the following Tuesday (31 May). On 30 May, an arrangement was made for the accused to meet Lisa's husband at a hotel before being taken to her home. During this call, the accused made reference to engaging in sexual activity with the daughter.

Court of First Instance proceedings

The Sheriff reported that the law on entrapment was not in dispute. It was set out in Renton & Brown: *Criminal Procedure* (6th edition at para 9-20.1) as occurring in situations in which the crime was committed 'as a result of instigation or persuasion by the police or other authority, and ... by a person who would not otherwise have been engaging in the activity in question'. To be legitimate, participation by an undercover police officer in a criminal conspiracy required that participation to be preceded by a reasonable suspicion that a crime was being, or about to be, committed (Jones v HMA [2009] HCJAC 86).

The parties agreed that the basis of the plea in bar of trial was that the conduct of the police was such that prosecution would be oppressive.

The law was as stated in *Attorney General's Reference (No. 3 of 2000) sub nom R* v *Loosely* [2002] 1 Cr App R 29. The focus was on the role of the police in their formation of the accused's intent to commit the offence. If the accused had already formed an intention to commit the offence, or one of a similar kind, and the police did no more than provide an opportunity to do so, that action was unobjectionable. The matter would be different if the accused lacked such a predisposition and the police were responsible for implanting the intent.

The Sheriff held that no evidence was produced that the accused had a predisposition to commit such an offence when he was first engaged by the police. He had had no involvement in the

abuse of children, and the police had no basis for suspecting that he had. The police had implanted the necessary intent by persisting with the idea that a child could be involved in the accused's sexual activity.

Appeal

The prosecution (Crown) appealed on the basis that the Sheriff had erred: (i)(a) in holding that the police did not have reasonable suspicion that the respondent was about to commit a crime such as that libelled; (b) in concluding that the respondent had no predisposition to engage in the conduct libelled; and (ii) in holding that the acts of the police were designed to lure the respondent into activity that he would not otherwise have undertaken. The respondent had willingly participated in a dialogue inviting sexual conduct. The police had made reference to a 14-year-old child, but had not suggested that the respondent should engage in sexual conduct with the child. The police had simply offered an opportunity rather than luring the respondent into expressing a criminal desire.

Court ruling

In Jones v HMA [2009] HCJAC 86, the question was 'whether or not an unfair trick was played upon the particular accused whereby he was deceived, pressured, encouraged or induced into committing an offence which he would never otherwise have committed'. The resolution of the matter 'will depend on the facts and circumstances of the individual case'.

In this case, the significant facts were, first, that no evidence was produced that the respondent had ever expressed any interest in sexual activity with children in the original chat logs examined by the police. Second, when the existence of the daughter was referred to initially by the police, the respondent did not react. Third, when he was asked specifically about what he was 'into', and then what his fantasies might be, he made no mention of the daughter or children in general. Fourth, at the point of the initial discussion about the daughter being in the next room, the context of what he said did not involve sexual activity with the daughter, but concern in relation to her presence. Fifth, only when the police introduced the idea of the daughter entering the bedroom, during sexual activity between the respondent and other adults, did he mention engaging in any activity involving the daughter.

Against that background, the court was satisfied that the judge at first instance, whose views, having heard all the relevant circumstances, are entitled to be given some weight, was entitled to strike the balance that he did in determining that what may be a relatively fine line had been crossed. For those reasons, the appeal was refused.

Note from the UK EJCN member: The case is the first example in Scotland of the Appeal Court applying the established principles of entrapment to a case involving covert internet investigations. Such police investigations regularly take place and normally result in the conviction of the accused person. However, on this occasion, the Appeal Court said that the judge at first instance was

entitled to hold that the covert internet investigators had simply strayed too far and lured or incited the accused to commit an offence that would not otherwise have taken place.

3.2. Other Court rulings in brief

Procedure: Court of Appeal, *Director of Public Prosecutions v Arkins*, Ireland

Date: 11 June 2018

In November 2017, the appellant was convicted for possession of child pornography, and possession of child pornography for the purpose of distributing, publishing, exporting, selling or otherwise showing it, and he was sentenced, respectively, to four (first count) and three (second count) years of imprisonment. The appellant appealed the sentences on the basis that they were too high. The appellant opposed the consecutive sentencing, as the facts related to the possession of child pornography and distribution of child abuse material (CAM) dated from 2009, to which he pleaded guilty when arrested in 2016. The facts related to the second count stemmed from a separate investigation into a person who posted an image on Facebook, which the police traced back to the appellant in 2016.

The Court, in its ruling, took into account several grounds, such as the volume of the CAM in the appellant's possession, the nature and gravity of the material, the fact that the appellant shared the CAM, and that the appellant offended a second time after the first offence five years earlier, after which he sought therapeutic services. The fact that the appellant re-offended after he participated in therapeutic services indicates a significant degree of awareness on the appellant's part of his wrongdoing. The Court concluded, therefore, that the consecutive sentencing was justified and appropriate.

Procedure: Court of First Instance Rotterdam, case 10/960005-16, Netherlands

Date: 6 March 2018

The defendant exchanged bitcoin for cash. He offered his services on the Internet, and met with his clients in public places, during which the clients transferred the bitcoin to him, and he paid the value in cash after deduction of a commission. The defendant subsequently sold the obtained bitcoin to exchange companies such as Kraken and Bitstamp. The companies paid for the bitcoin by transfers to bank accounts in the defendant's and other persons' names. Most of that money was withdrawn in cash by the defendant. In total, more than EUR 11 million was transferred to bank accounts.

To establish whether the defendant was guilty of money laundering, proof needed to be demonstrated that the defendant knew or should have known that the bitcoin was obtained by

his clients through criminal activity. The following circumstances were taken into account to establish knowledge of criminal origin of the bitcoin: the defendant charged a unusually high commission rate, he used several different accounts to receive the funds from the bitcoin exchanges, he paid the bitcoin owners very large sums of cash in public places, he did not keep any books, nor did he verify the identity of his clients. The defendant did not provide a reasonable explanation. The Court therefore argued that the combination of before-mentioned circumstances justifies the assumption that the defendant knew about the criminal origin of the bitcoin.

The defendant was found guilty of participating in the commission of habitual laundering of bitcoin and intentional conduct in violation of Article 3B of the Narcotics Act. As a result, he was sentenced to four years' imprisonment.

Procedure: Court of First Instance Midden-Nederland, case 16/700016-16, Netherlands

Date: 3 April 2018

Six defendants were convicted for laundering bitcoin with a value ranging from EUR 100 000 up to EUR 10 million, and sentenced to imprisonment ranging from one to three years. Suspects were divided into two groups: bitcoin exchangers and their clients. The main suspects exchanged bitcoin for large sums of cash. A bitcoin mixing service was used to make tracking the bitcoin more difficult. Anonymity was guaranteed for their clients. The cash amounts were handed over to the clients in public places. An unusually high commission rate was charged for this service. The main suspects did not inquire into the origin of the bitcoin, and could not provide any explanation.

The defendants did not start their bitcoin exchange with criminal intent, but they took risks in such a way that they must have known that the bitcoin was from criminal origin and that they were facilitating crime by exchanging them. Further circumstances that were taken into account were the fact that the defendants had exchanged bitcoin for large sums of cash, that during that process they charged their clients a commission that was considerably higher than regular exchanger Bitonic B.V., and that the exchanges were made in public places. Given that the defendants could not provide a reasonable and probable explanation regarding the possible legal origin of the bitcoin, and considering the abovementioned specific circumstances, the Court ruled that the bitcoin must have originated from criminal activities, and convicted the defendants of money laundering.

Procedure: Court of First Instance Rotterdam, case 10/750248-14, Netherlands

Date: 3 May 2018

In this case, the defendant hacked into computer systems of different companies, and copied/downloaded data. For this purpose, he made use of software (Medusa, Hydra and RWW_Attack) to illegally access the computer systems.

The public prosecutor argued that the software, which the defendant had in his possession, is a malware that is mainly created to illegally access network systems. The Court, however, did not find sufficient proof that this software was designed solely for that purpose. In this case, there were only indications that Metasploit and Zenmap could also have been used to commit an offence. Therefore, the Court only found the defendant guilty of having had in his possession a technical devices (Medusa, Hydra and RWW_Attack) with which he illegally accessed a network system and recorded data.

The defendant was found guilty of multiple counts of hacking, as well as possession of a technical device enabling him to access computer systems unlawfully. He was sentenced to a four-month suspended sentence and 180 hours of community service.

Procedure: Court of First Instance Rotterdam, case 13/650686, Netherlands

Date: 16 May 2018

Defendant hacked online accounts of several Dutch celebrities. During the investigation, the investigating judge had granted a permit for a search of the suspect's mobile telephone. His computer was also searched, although no specific permit was granted for that device. The defendant therefore claimed that this search was a violation of his right to privacy under article 8 ECHR and, as a consequence, the information obtained from the computer should be excluded from the evidence in this case. The defendant also argued that article 6 ECHR was breached.

The Court ruled that the computer had indeed been searched unlawfully, as the investigating judge had only issued an order for the search of the suspect's mobile telephone. As a consequence, article 8 ECHR was violated, constituting a procedural error. However, no violation of article 6 ECHR was committed, as no intentional violation of the right to a fair trial by the authorities took place, especially also since permission was given to search the mobile telephone. The Court then assessed the gravity of the violation of privacy to ascertain whether the evidence was to be excluded. Given the fact that the police already had a good view of the suspect's private life as a result of the lawful telephone search, and the search of the computer did not bring up many additional facts about his personal life, the Court considered that the violation was minimal. As a result, the violation of article 8 ECHR did not lead to any consequences (excluding of evidence), as the defendant's privacy was not severely invaded. He was sentenced to 1 year of imprisonment (half of which was a suspended sentence).

Procedure: Court of First Instance Noord-Nederland, case 18/750065-16, Netherlands

Date: 18 June 2018

This case concerned a defendant who performed a large-scale cybercrime operation. He built websites for web shops and used that knowledge to gain access to login credentials of their customers. With those credentials, he was able to log in to customer accounts for other web shops and unlawfully order goods. Furthermore, he used the stolen credentials to commit fraud on the Facebook platform. He first studied the private communications of a subject and impersonated that person. He then contacted the subject's friends to try and trick them into sending money to him.

The Court found the defendant guilty of illegally accessing a computer system, swindling and habitual money laundering. The seriousness of these facts, the sophisticated and professional character of the operation, the consequences (financial losses and violation of privacy) for affected parties, the large scale on which these acts were perpetrated, the undermining of trust on the Internet and the duration of the activity, justified the maximum sentence for fraud: four years of imprisonment. The court also stated that it wanted to send a deterring message to cybercriminals with this maximum sentence, because the use of online services is heavily increasing and these criminal activities can be deployed with relative ease.

Procedure: Court rulings involving forfeiture of bitcoin, Slovak Republic

Date: 2018

The Slovak EJCN member reported the following information related to two court rulings:

The first judgement involving a forfeiture of bitcoin (as part of a forfeiture of property in a drug case) was issued in 2018. The case concerned production and cross-border trafficking of cannabis, including via the Darkweb. The offender sent cannabis to France, Hungary, Italy, the UK, Turkey, Bosnia and Herzegovina, etc. in envelopes by regular mail. The indicated sender was a fictitious company. The suspect was charged with the continuous and particularly serious crime of illegal production of narcotic and psychotropic substances, poisons or precursors, and possession and trafficking thereof. Although the amount of bitcoin is small –only 0,14299232 BTC, this ruling is nevertheless important.

A second final judgement was made regarding the particularly serious crime of illegal production of narcotic and psychotropic substances, poisons or precursors, their possession and trafficking, the criminal offence of carrying a concealed weapon, and arms trafficking. Two offenders were convicted. The cyber element concerns the use of the Darkweb.

More information on this judgement will be provided at a later stage, as a separate decision is expected on forfeiture, including bitcoin.

Procedure: Court of Appeal, Jönköping, Sweden

Date: 13 June 2018

On 13 June 2018, the Göta Court of Appeal in Jönköping convicted a 19-year-old Swedish man (who was a juvenile when the crimes were committed) to a conditional sentence, guilty of gross computer intrusion consisting of several DDoS-attacks against two major Swedish banks in October and November 2015. The crimes were considered serious given that the attacks:

- caused serious economic damage to the banks and also reduced public trust in the security of the banks' computer systems and their payment solutions;

- seriously disturbed and hindered the use of a large amount of information, as the banks' customers were unable to use the webpages for a long time; and

- were especially hazardous, as the banks' information and payment systems are considered part of the crucial infrastructure.

The investigation involved a number of international contacts and legal assistance, and, during the trial, a UK police forensic expert testified.

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. Case law of the Court of Justice of the European Union (CJEU)

Spain

On 2 October 2018, the CJEU pronounced a preliminary ruling in relation to the interpretation of Article 15(1) of Directive 2002/58/EC. Interlocutory questions were referred to the CJEU by the Provincial Court of Tarragona.

In the main proceedings, the Public Prosecutor's Office appealed against a refusal by an investigating magistrate to authorise the police to order various providers of electronic communications services to provide telephone numbers that had been activated during a specific timeframe with the IMEI code of a stolen mobile telephone, as well as the personal data relating to the identity of the owners or users of the telephone numbers corresponding to the SIM cards activated with the code, such as surnames, forenames and addresses. The mobile telephone was stolen during a robbery, during which the victim was also injured.

The Provincial Court subsequently referred the following questions to the CJEU for a preliminary ruling:

(1) Can the sufficient seriousness of offences, as a criterion that justifies interference with the fundamental rights recognised by articles 7 and 8 ECHR, be determined taking into account only the sentence that may be imposed in respect of the offence investigated, or is identification of particular levels in the criminal conduct of harm to individual and/or collective legally protected interests also necessary?

(2) If it were in accordance with the constitutional principles of the European Union, used by the Court of Justice in its judgement of 8 April 2014, *Digital Rights Ireland and Others,* as standards for the strict review of Directive 2002/58/EC, to determine the seriousness of the offence solely on the basis of the sentence which may be imposed, what should the minimum threshold be? Would a general provision setting a minimum of three years' imprisonment be compatible with this threshold?

The CJEU considered that the list of objectives set out in the first sentence of Article 15(1) of Directive 2002/58 is exhaustive, as a result of which that access must correspond, genuinely and strictly, to one of those objectives. As regards the objective of preventing, investigating, detecting and prosecuting criminal offences, the Court states that it refers to 'criminal offences' in general, and not only to serious crime. Interference with fundamental rights, due to access to data, can be justified by this objective.

The Court continued by stating that the requested data did not concern communications carried out with the stolen mobile telephones, and, as such, those data would not allow precise conclusions to be drawn concerning the private lives of the persons whose data is concerned. As a consequence, access to only the data referred to in the request in the main proceedings cannot be defined as a serious interference with fundamental rights of the concerned person.

The Court thus concluded that access of public authorities to data for the purpose of identifying the owners of SIM cards activated with a stolen mobile telephone, such as surnames, forenames and addresses of the owners, entails interference with their fundamental rights, which is, however, not sufficiently serious to entail that access being limited, in the area of prevention, investigation, detection and prosecution of criminal offences, to the objective of fighting serious crime.

Belgium

On 19 July 2018, the Belgian Constitutional Court brought the following interlocutory questions before the CJEU:

(1) Should Article 15.1 of Directive 2002/58/EG, read in conjunction with the right to security, as protected by article 6 ECHR, and the right to protection of personal data, as protected by articles 7, 8 and 52.1 ECHR, be interpreted as meaning that it precludes a national legislation that entails a general obligation for all operators and providers of electronic communication services to retain traffic and location data within the meaning of Directive 2002/58/EG which are generated or processed within the framework of offering those services:

- when this national legislation was not only adopted for the investigation, detection and prosecution of serious criminal offences, but also for guaranteeing national security, the defence of the territory and public security, the investigation, detection and prosecution of offences that are not forms of serious crime, or preventing the illegal use of electronic communication systems or other objectives as listed in Article 23.1 of Directive 2016/679 (GDPR); and
- when a number of precise guarantees are foreseen related to the retention of the data and the access thereto.

(2) Should Article 15.1 of Directive 2002/58/EG, read in conjunction with articles 4, 7, 8, 11 and 52.1 ECHR, be interpreted as meaning that it precludes national legislation that entails a general obligation for all operators and providers of electronic communication services to retain traffic and location data within the meaning of Directive 2002/58/EG that are generated or

processed within the framework of offering those services, when the objective of this national legislation is also to fulfil the positive obligations imposed on the government on the basis of articles 4 (prohibition of torture and inhuman/degrading treatment) and 8 (protection of personal data) ECHR, which entail providing a legal framework allowing for effective criminal investigation and an actual punishment of sexual abuse of minors, and to ensure the identification of perpetrators of this offence, even if electronic means of communication are being used?

(3) If, based on the responses given to the first and second preliminary questions, the Belgian Constitutional Court would come to the conclusion that the contested law would be in breach of one or more obligations arising from the provisions mentioned in the previous questions, could the Court temporarily uphold the effects of the law of 29 May 2016 regarding the retention of data in the sector of electric communications to avoid legal uncertainty and to allow that the data that have already been collected and retained could still be used for the objectives provided for in the law?

The case is still pending before the Court.

4.2. Other national developments

Czech Republic

Pending case before the Czech Constitutional Court

A petition is pending before the Czech Constitutional Court in relation to the constitutionality of the current data retention regime in the Czech Republic. The Court panel is currently deliberating.

Ireland

Data Protection Act 2018

This act was introduced to give effect to Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and Directive 2016/680/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data. Section 71(7) of the 2018 Act provides that a data controller must carry out periodical reviews on the necessity of retaining data. Section 213 of the 2018 Act amends Section 12 of the Communications (Retention of Data) Act 2011.

Netherlands

Proposal for a law amending the data retention rules with respect to criminal investigations

A legislative proposal is currently pending in the Netherlands to amend the rules on data retention for the purpose of criminal investigations. The proposal has been delayed because of developments in relation to Carrier Grade Network Address Translation and the technicalities linked to it (multiple users for 1 public IPv4 address). An assessment is currently being made to determine whether the legislative proposal needs to be adapted in light of these new developments.

Slovak Republic

Act No. 69/2018 Coll. on cybersecurity; amendment to Act. No. 351/2011 Coll. on electronic communications

Although this Act has no influence on the scope or period of data retention, the amendment now also allows access to data to the National Security Office for specified purposes.

UK

Data Protection Act 2018

This act implements the requirements of the GDPR in the UK.

Court ruling

R. (on the application of National Council for Civil Liberties) v. Secretary of State for the Home Department, Divisional Court, 27 April 2018

The Investigatory Powers Act 2016 Pt 4 was incompatible with fundamental rights in EU law, as, in the area of criminal justice, access to retained data was not limited to the purpose of combating 'serious crime', and access to retained data was not subject to prior review by a court or an independent administrative body. The court decided against making an order of disapplication. The Act needed to be amended by 1 November 2018.

5. Topic of Interest

The role of encryption in criminal investigations

1. Introduction

In the current digital age, law enforcement authorities often depend on electronic evidence to build a case and find proof of crime. Encryption is, however, increasingly playing an obstructive role in criminal investigations. Even more, technologies are constantly changing and evolving, and so are the forms of encryption. As a consequence, law enforcement authorities are confronted regularly with issues concerning access to data/e-evidence. These issues are multiple: technical, legal and practical. When taking measures to bypass encryption, LEA and judicial authorities need to strike the right balance between a person's rights and a State's responsibility to protect its citizens, and thus to ensure that LEA and judicial authorities can investigate and prosecute effectively. The continuing discussions among practitioners on the topic of encryption, the measures taken at EU level[3], as well as European and national case law, demonstrate the complexity of the matter.

This chapter provides an overview of the legislative frameworks in relation to encryption, particularly the legal provisions related to handover of a decryption key or unencrypted data, and the legal provisions regulating 'bypassing/attacking' encryption through the use of LEA tools and techniques. Furthermore, some legal and practical challenges with which authorities are faced when dealing with encryption are elaborated upon. This overview provides a general outline and is by no means exhaustive in detailing all specific differences in the Member States and third States.

The information presented in this chapter was gathered via a questionnaire distributed in July 2018 to the experts of the EJCN. The questionnaire served a dual purpose, namely to gather information for this issue of the CJM, as well as to provide information for the first report of the Encryption observatory function. The European Commission, in its 11th progress report, proposed a continuous assessment of the legal and technical aspects of the role of encryption in criminal investigations, including through the development of an observatory function in collaboration with the European Cybercrime Centre (EC3), the EJCN and Eurojust. In total, replies from EJCN members of 21 countries were received, including one non-EU country (Norway). The tables on pages 34 to 37 containing relevant legal provisions on encryption of all countries have been completed with information received from four Eurojust National Desks.

[3] *See* 11th Progress Report towards an effective and genuine Security Union, COM (2017) 608.

2. Legal landscape: bypassing or attacking encryption

For the purpose of this chapter, two different categories for handling encryption are used: bypassing encryption and attacking encryption. Bypassing encryption can be done by requesting/ordering the unencrypted data or access key to be handed over. Attacking or breaking encryption would entail, for example, LEA applying brute force, installing tools or performing a lawful intercept. In the current legal landscape, very few Member States have specific legal provisions allowing LEA and judicial authorities to bypass or attack encryption. If no specific legal provisions are in force, Member States will often apply general legal provisions to effectively address encryption in criminal investigations. Although some practitioners consider the application of general provisions sufficient and effective, the interpretation by analogy of such general provisions might give rise to legal challenges in some cases.

2.1. Bypassing encryption by handing over access key or unencrypted data

When confronted with encrypted devices or files during a criminal investigation, police can request the access key or data to be handed over in an unencrypted format. Unless this handover happens voluntarily, successfully receiving the requested information will very much depend on the existence and effectiveness of legislative possibilities, compelling a suspect or a third party to hand over the key or data.

Suspect

Currently, only a few Member States (5) have a legal provision compelling a suspect to hand over the access key or (assist LEA to get access to) the data in an unencrypted format. Most Member States do not have such a provision, as it is considered irreconcilable with a person's right not to incriminate himself/herself (*nemo tenetur principle*).

Belgium, France, Ireland and the UK currently have specific legal provisions that compel the suspect to provide the authorities with an access key, produce the data in an unencrypted format, or enable authorities to access the data. The application of these provisions has, however, resulted in a number of cases being brought to court. In France, the *Conseil constitutionnel* has ruled that the legal provisions only allow the decryption of encrypted data and are not intended to obtain a confession of the suspect or carry a recognition or presumption of guilt. Moreover, the data, which is already stored on a server/device, exists independently of the will of the suspect. Consequently, no violation of the *nemo tenetur* principle has occurred. No consensus has been reached among Belgian courts. Nonetheless, the courts tend to accept that the decryption order is reconcilable with the *nemo tenetur* principle and the right to remain silent. The Belgian Court of First Instance in Antwerp has recently motivated its ruling in a similar way as in France, namely that the access key and content of a mobile telephone exist independently of the will of the suspect. The Court further stated that the right to remain silent ensures that the evidence-gathering process is not manipulated in such a way that it would result in untruthful evidence, for example by using force or torture to obtain confessions. In the case at hand, the Court stated that the force applied, i.e. compelling the suspect to hand over the key, could not result in the change of the access code or content of the telephone. Moreover, the seriousness of the facts justified the application of the measure. In addition to the potential

violation of *nemo tenetur*, another challenge encountered with the concerned legal provision in the UK is that, unless the suspect is under investigation for a terrorism or child abuse offence, the maximum penalty for non-compliance is two years imprisonment. For terrorism or child abuse offences, the maximum penalty is five years imprisonment. In many cases, the penalty for non-compliance will thus be much less severe than the penalty for being convicted of the offence. As a consequence, in some cases, non-compliance can be in the interest of the suspect.

In Croatia, under the general provisions of the Criminal Procedure Act regulating searches, everyone (thus including a suspect) can be obliged to provide authorities with access to an electronic device he/she is using or of which he/she has the means of access. However, the legal provision stipulates that the penalty clause for non-compliance, which is incorporated in it, does not apply to a defendant. Thus, in practice, a suspect will be unlikely to provide such access.

Although no legal provision exists in the Netherlands to compel a suspect to hand over an access key, in some cases, the Dutch authorities allow the use of biometric data from a suspect to unlock a device, as was recently supported by a court ruling in The Hague.[4]

By a recent amendment of the Criminal Procedure Code of Norway, law enforcement authorities can make use of biometric authentication to legally access mobile telephones and other electronic systems.

Third parties

Contrary to the limited number of country legislations that contain an obligation for suspects to provide access to encrypted data, most countries (19) do have specific or general legal provisions containing an obligation for third parties (persons and/or legal entities) to hand over the key or the unencrypted data. A few countries incorporated in their law a disclosure obligation particularly for online service providers.

Practitioners from countries that do not have a legal obligation for third parties to hand over access keys or data would consider such a provision incorporated in their law to be useful. Although countries that do have an obligation in force for third parties consider it useful, they still encounter some obstacles. First, the penalties for non-compliance by third parties are considered too low or not proportionate to the penalty of the crime under investigation. In Ireland, the legal obligations only exist for cyber-dependent or cyber-related offences. Second, even if service providers are obliged by law to provide access, they sometimes claim to be unable to comply with the request because they do not have the access key or are technically incapable of providing authorities with access to end-to-end encrypted data. In Hungary, the legal provision foresees such inability for service providers to comply with a request and allows for exceptional non-compliance. As a consequence, these obstacles can result in deliberate non-compliance by third parties, thus leaving the legal requirement void. Service providers particularly remain unaccountable.

[4] *See* chapter 3, Court of First Instance of The Hague, 12 March 2018.

2.2. Attacking encryption by using brute force, LEA tools and techniques

Brute force, forensic tools and techniques

LEA can try to gain access to data by breaking encryption in different ways. As a general understanding, if a key is legally found (finding/guessing the key) in the course of an investigation, it can generally be used for further investigation. Member States can also attempt to access a device with forensic tools. Only a few Member States have specific legislation in this respect. All other countries apply general provisions to access a device, i.e. the traditional rules on search and seizure.

On the one hand, as such general rules do not contain any specific legal limitations with regard to the use of any of such tools, they leave a certain margin of possibilities for LEA and thus no legal limitations appear on what can be done with legally obtained devices. From this point of view, the application of the general rules is considered sufficient.

On the other hand, practitioners point out that specific provisions on the use of particular tools could be of added value to provide more legal clarity. Such specific provisions should, however, not be too technically descriptive and detailed, in view of the evolving technological landscape. Also, given the difficulties encountered with end-to-end encryption, some practitioners do see a need for specific legislation in that area (cooperation by service providers). An example of such legislation is a new provision that will enter into force on 1 April 2020 in Austria, which allows LEA to install software on a computer system and enables them to obtain data streams of a message communication before the communication is encrypted or after the message is decrypted. This measure will be considered as 'monitoring communications' and therefore permitted under the same legal conditions.

Next to these legal challenges, LEA and judicial authorities are mostly confronted with technical and practical challenges when trying to get access to unencrypted data in criminal investigations. According to the EJCN practitioners, the main issues are the high cost of the forensic tools, the time-consuming nature of breaking encryption, the lack of or insufficient number of experts for decrypting, and lack of training. Practitioners see added value if forensic expertise and tools could be concentrated/pooled/shared at EU level, rather than each Member State providing its own tools and resources.[5]

[5] Report of the Eurojust Workshop on encryption, 7-8 June 2017.

3. Legal provisions in relation to encryption

Legal provisions compelling a suspect to disclose access keys or to provide data in an unencrypted format

COUNTRY	LEGAL PROVISIONS
Austria	No
Belgium	Article 88quater Code of Criminal Procedure
Croatia	Article 257 Criminal Procedure Act (searches)
Czech Republic	No
Denmark	No
Estonia	No
Finland	No
France	Article 434-15-2 Criminal Code
Germany	No
Greece	No
Hungary	No
Ireland	Section 48 Criminal Justice Theft and Fraud Offences Act 2001 Section 7 Criminal Justice Offences Relating to Information Systems Act 2017
Latvia	No
Lithuania	No
Luxembourg	No
Poland	No
Portugal	No
Romania	No
Slovak Republic	No
Slovenia	No
Spain	No
Sweden	No
The Netherlands	No
UK	Part III Regulation of Investigatory Powers Act 2000 Section 49 Regulation of Investigatory Powers Act 2000
Norway	No, exception: Article 199a Criminal Procedure Law (biometric data)

Blue	*General legal provisions*
Orange	*Specific legal provisions*

Legal provisions compelling a third party to disclose access keys or to provide data in an unencrypted format

COUNTRY	LEGAL PROVISIONS
Austria	Section 111, para 1 Code of Criminal Procedure (obligation to facilitate seizure) Section 93, para 2 Code of Criminal Procedure (penalty in case of non-compliance)
Belgium	Article 88quater Code of Criminal Procedure
Croatia	Article 257 Criminal Procedure Act (searches)
Czech Republic	Section 8(1) Code of Criminal Procedure Article 66 Code of Criminal Procedure (penalty in case of non-compliance)
Denmark	Section 804 Administration of Justice Act Section 10 Act on Electronic Communications Networks and Services (obligation for ISPs to foresee the necessary technical means to assist)
Estonia	No
Finland	No
France	Article 434-15-2 Criminal Code
Germany	Section 48, para 1 and 161a para 1 Criminal Procedure Code Section 95 Criminal Procedure Code
Greece	No
Hungary	Section 264, Article 3 Code of Criminal Procedure
Ireland	Section 980E(7) Taxes Consolidation Act 1997 Section 130 Data Protection Act 2018 Section 15(6) Criminal Justice Act 2011 Section 75(11) Criminal Justice (Mutual Assistance) Act 2008 Section 63(4) Criminal Justice Act 1994
Latvia	Section 190 Criminal Procedure Code Section 192 Criminal Procedure Code (owner, processor, keeper of electronic information system)
Lithuania	General legal provisions; a fine foreseen only for legal entity, not private person
Luxembourg	Article 66 Code of Criminal Procedure Article 141 Criminal Code (provision for obstruction of justice)
Poland	Article 218 Code of Criminal Procedure Article 236a Code of Criminal Procedure
Portugal	No
Romania	No
Slovak Republic	No
Slovenia	Article 219a, para 6 Criminal Procedure Act Article 223a, para 3 Criminal Procedure Act
Spain	Article 588ter (e) Criminal Procedure Code (duty of collaboration) Article 588sexies (c) Criminal Procedure Code (judicial authorisation)
Sweden	No
The Netherlands	Section 125k Code of Criminal Procedure
UK (England & Wales)	Part III Regulation of Investigatory Powers Act 2000 Section 49 Regulation of Investigatory Powers Act 2000 Section 20 Police and Criminal Evidence Act 1984
UK (Scotland)	Part III Regulation of Investigatory Powers Act 2000 Section 49 Regulation of Investigatory Powers Act 2000
Norway	Article 199a Norwegian Criminal Procedure Code (biometric data)

Legal provisions on attacking encryption by law enforcement

COUNTRY	LEGAL PROVISIONS
Austria	General provisions
Belgium	Article 39bis Code of Criminal Procedure (network search) Article 89ter Code of Criminal Procedure (sneak and peek in computer systems) Article 90ter Code of Criminal Procedure (legal hacking)
Croatia	Article 224 to 232 Criminal Procedure Act (searches)
Czech Republic	Section 113 Code of Criminal Procedure
Denmark	Sections 780-781 Administration of Justice Act (interception of communications) Sections 793-794 Administration of Justice Act (searches)
Estonia	§ 83 Code of Criminal Procedure (inspection and inquiries to electronic communications undertakings) § 91 Code of Criminal Procedure (searches) § 1265 Code of Criminal Procedure (covert surveillance, covert collection of comparative samples and conduct of initial examinations, covert examination and replacement of things) § 1267 Code of Criminal Procedure (wire-tapping or covert observation)
Finland	No
France	Article 230-1 to 230-5 Criminal Code (deciphering) Article 706-102-1 to 706-102-7 Criminal Code (GOVWARE)
Germany	Sections 94, 98 and 102 Code of Criminal Procedure (stored data) Section 100a, para 1 Code of Criminal Procedure (real-time interception - source interception enabling access to unencrypted data) Section 51 para 2 new Law on the BKA (real-time interception - terrorism prevention)
Greece	Article 258 et seq. Code of Criminal Procedure
Hungary	Sections 231 and 232 Code of Criminal Procedure
Ireland	General provisions - where the devices or accounts, etc., are accessed on the basis of a legal authority such as a search warrant, the investigators may utilise any means to gain access and give effect to the provisions in the warrant
Latvia	Section 179 Criminal Procedure Code (searches) Section 186 Criminal Procedure Code (seizure) Sections 159-161 Criminal Procedure Code (inspection) Sections 193-194 Criminal Procedure Code (expert examination) Sections 218-220 Criminal Procedure Code (control of data)
Lithuania	No
Luxembourg	General provisions
Poland	Article 19 §7 Police Act (request for the use of hacking techniques)
Portugal	General provisions
Romania	Article 138 Criminal Procedure Code (access to computer systems)
Slovak Republic	General provisions
Slovenia	General provisions
Spain	Genera provisions - pursuant to several technological measures that are regulated in the Criminal Procedure Code, the use of any technique to decrypt that can be audited and does not involve physical violence on a person is allowed Article 588septies (b) Criminal Procedure Code (remote search)
Sweden	General provisions
The Netherlands	General provisions

UK (England & Wales)	General provisions - if items have been lawfully seized, the police have the power to undertake an examination that may involve damage to or destruction of the item
UK (Scotland)	Various provisions in Regulation of Investigatory Powers Act 2000 Various provisions in Regulation of Investigatory Powers (Scotland) Act 2010 Various provisions in Investigatory Powers Act 2016
Norway	General provisions

6. The Way Ahead

The Cybercrime Judicial Monitor is published once per year. It is distributed to LEA and judicial authorities active in the cybercrime domain.

The focus of future issues of the CJM will remain on legislative developments in the area of cybercrime and e-evidence and the analysis of relevant court decisions. The topic of interest will be determined based on ongoing or emerging trends.

Importantly, the content of the CJM depends on the input of practitioners. We therefore kindly encourage 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 December 2018

Catalogue number: QP-AG-19-004-EN-N
ISBN: 978-92-95084-00-1
ISSN: 2600-0113
DOI: 10.2812/53430