Cybercrime investigations

Oerlemans, J.; Galič, M.; Wagen, W. van der; Weulen Kranenbarg, M.

9 Cybercrime investigations

Jan-Jaap Oerlemans & Maša Galič*

9.1 Introduction

Digital traces, such as an IP address or a nickname, are oftentimes the only traces available in criminal investigations relating to cyber-dependent crimes. The investigation process therefore differs greatly from investigations of traditional crime, where a physical crime scene exists. When it comes to cybercrimes eyewitnesses, DNA material or video recordings will usually not be available. As such, law enforcement authorities need to rely much more on data available from internet service providers and data located on the victim's and offender's computers, which can be found with the help of digital forensics.

This chapter focusses on criminal investigations and the investigative methods that are used in cybercrime cases. The chapter is structured according to the three main challenges that arise in cybercrime investigations: jurisdiction, anonymity and encryption. These challenges help explain why certain investigative methods are commonly used in cybercrime investigations. The chapter also offers a bird's-eye view on the regulation of these investigation methods in international treaties, particularly the 2001 Council of Europe Cybercrime Convention (hereinafter 'Convention on Cybercrime').[1] The aim of this chapter is to provide an insight into cybercrime investigations and the regulation of investigative methods. We also touch upon ethical and legal dilemmas that arise in cybercrime investigations.

Section 9.2 starts with a brief introduction into the regulation of digital investigative methods in Europe and the limits of enforcement jurisdiction. Section 9.3 discusses the investigatory process, where an IP address serves as

* Prof. Dr. J.J. Oerlemans is assistant professor in Criminal Law at the Institute of Criminal Law & Criminology at Leiden University and endowed professor of Intelligence and Law at Utrecht University. Dr. M. Galič is assistant professor in Privacy and Criminal (Procedure) Law at the department of Criminal Law and Criminology at the VU University Amsterdam.

1 Council of Europe, Convention on Cybercrime (ETS No. 185). Adopted on 8 November 2001 in Budapest.

a digital lead, and the investigative methods used in this process, such as data production orders and search and seizure of computers. Section 9.4 discusses the use of anonymisation by cybercriminals, open-source investigations on the internet and online undercover operations. Section 9.5 discusses the problem of encryption in cybercrime investigations and hacking powers as a solution to this problem. Section 9.6 briefly discusses why the strategy of 'disruption of cybercrime' is increasingly being used as a response to cybercrime. The chapter concludes with discussion questions and key concepts relating to cybercrime investigations.

9.2 Digital investigations and criminal procedure law

Before delving into digital investigation methods used in cybercrime investigations, some basic knowledge of criminal procedure law and the underlying concepts of the regulation of investigative methods is required.

9.2.1 Regulating investigative methods

National criminal procedure laws are not excluded from the scope of international human rights law. This is so because all aspects of the investigation and prosecution of crime, including cybercrime, have the potential to interfere with human rights. When it comes to cybercrimes, the right that may be most significantly affected is the *right to private life* (also referred to as the *right to privacy*). The jurisprudence of the European Court of Human Rights (hereinafter 'ECtHR') can thus be used to explain the system for regulating investigative methods, including the digital investigative methods used in cybercrime investigations. Through developing case law, the ECtHR requires member states to implement certain 'qualitive requirements' in their regulation of investigative methods. These requirements depend on the seriousness of the interference with the right to private life.

The right to respect for private life in Article 8 of the European Convention on Human Rights (hereinafter 'ECHR') reads as follows.

1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the

> economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

As can be seen from the text of the provision, the right to respect for private life protects the following four aspects of one's life: (1) the right to respect for private life, (2) the right to respect for family life, (3) the right to respect for the home, and (4) the right to respect for correspondence. In practice, however, other aspects of one's privacy might be interfered with, when investigative methods are used (see Koops et al., 2017). For this reason, the ECtHR deliberately does not provide an exhaustive definition of the general notion of 'private life'.[2] This allows the ECtHR to recognise and include new (types of) privacy interferences and to interpret the fundamental right to private life in a dynamic and flexible manner. Decades of ECtHR jurisprudence show the flexibility of Article 8 ECHR in light of the development and use of new technologies in criminal investigations.

In its case law, the ECtHR has stipulated that the regulation of investigative methods must fulfil the following three requirements in order to be considered 'in accordance with the law': (1) accessibility, (2) foreseeability, and (3) a certain quality of the law (meaning, compatibility with the 'rule of law' more broadly).[3] Accessibility means that the law must give an 'adequate indication' concerning which rules or procedures apply for using investigative methods in a given case. The applicable statutory law, case law, or guidelines for a certain investigative method must also be publicly available.

The second requirement of 'foreseeability' means that the law must indicate with sufficient clarity the scope of the power conferred on the competent authorities and the manner in which the investigative method is exercised

2 In the case of *Niemietz v. Germany* the ECtHR stated that it *does not consider it possible or necessary to attempt an exhaustive definition of the notion of 'private life'* (ECtHR 26 December 1992, ECLI:CE:ECHR:1992:1216JUD001371088, appl. no. 13710/88, para. 29).

3 See, e.g., ECtHR 4 May 2000, ECLI:CE:ECHR:2000:0504JUD002834195, appl. no. 28341/95, para. 52 (*Rotaru v. Romania*); ECtHR 1 July 2008, ECLI:CE:ECHR:2008:0701JUD005824300, appl. no. 58243/00, para. 59 (*Liberty and Others v. the United Kingdom*); and ECtHR 27 September 2005, appl. no. 50882/99, para. 76 (*Petri Sallinen and Others v. Finland*). It should be noted that in case law, the ECtHR does not always strictly divide these three requirements in this order. In certain cases, the ECtHR only tests the foreseeability of the law, which is then considered as part of the required quality of the law.

(see Gerards, 2011). In addition to written law and unwritten (case) law, relevant preparatory work for the legislation and publicly available guidelines are also taken into consideration in order to determine whether the law is sufficiently foreseeable in light of Article 8 ECHR (Ölçer, 2008). The ECtHR has made clear on numerous occasions that the 'essential object of protection' in Article 8 ECHR is to *protect the individual against arbitrary action by the public authorities*.[4] The foreseeability requirement in Article 8 ECHR thus offers *legal certainty* to the individuals who are involved in criminal investigations (Rainey et al., 2017). Legal certainty about the conditions and the manner in which investigative methods are applied is in turn a key element of the rule of law, because it helps holding governmental institutions accountable for their actions.[5]

The last requirement concerning the 'quality of the law' relates to the level of detail of the regulations and the minimum procedural safeguards that must be implemented in the domestic legal frameworks of contracting states to the ECHR (see Gerards, 2011). The more serious the interference with privacy, the more detailed the law and the higher the level of procedural safeguards will need to be.[6] Detailed regulations and procedural safeguards in domestic law aim to counterbalance the risk of abuse of power by the government. The limits and safeguards in criminal procedural law must therefore reflect the varying intrusiveness of investigative measures, ensuring that each measure is only used as necessary in a democratic society.

From the case law of the ECtHR, a 'scale of gravity' can be identified regarding the privacy interferences that are caused by the use of investigative methods and the level of detail of regulations and safeguards that they demand (Oerlemans, 2017a; Ölçer, 2008). The workings of this 'scale of gravity for privacy interferences' are illustrated in Figure 9.1.

4 See e.g., *Niemietz v. Germany*, para. 31, and ECtHR 27 October 1994, ECLI:CE:ECHR:1994:1027JUD001853591, appl. no. 18535/91, para. 32 (*Kroon and Others v. The Netherlands*).

5 See also the Council of Europe Commissioner for Human Rights, 'The rule of law on the Internet and in the wider digital world', Issue Paper of 8 December 2014, p. 8.

6 See, e.g., ECtHR 25 September 2001, ECLI:CE:ECHR:2001:0925JUD004478798, appl. no. 44787/98, para. 46 (*P.G. and J.H. v. the United Kingdom*); ECtHR 4 December 2008, ECLI:CE:ECHR:2008:1204JUD003056204, appl. nos. 30562/04 and 30566/04, para. 96 (*S. and Marper v. the United Kingdom*); and ECtHR 26 October 2000, ECLI:CE:ECHR:2000:1026JUD003098596, appl. no. 30985/96, para. 84 (*Hasan and Chaush v. Bulgaria [GC]*).

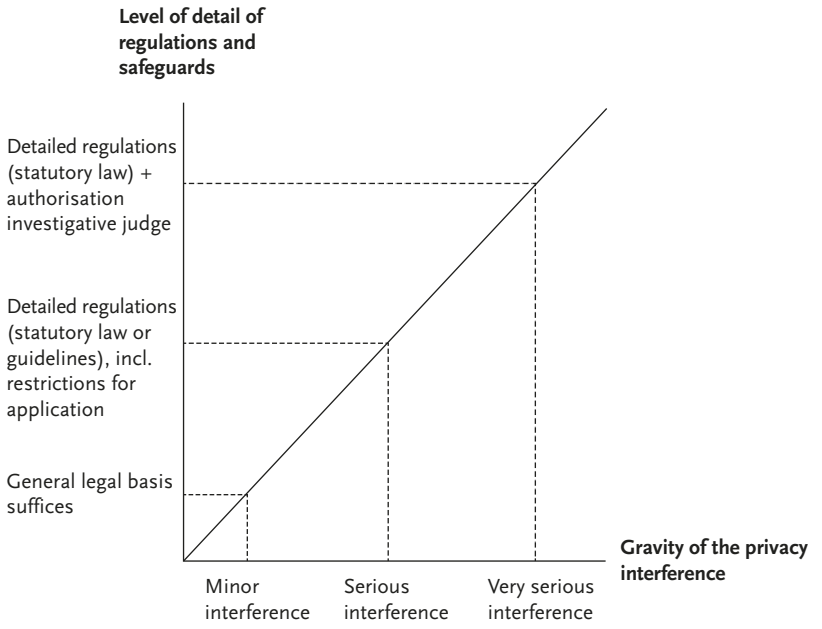

Figure 9.1 The scale of gravity for privacy interferences and the level of detail of regulations and safeguards[7]

Figure 9.1 illustrates the scale of gravity for privacy interferences. It shows how investigative methods that interfere more heavily in the right to private life generally require a more detailed legal basis in law, coupled with additional procedural safeguards to protect the right to private life of the individuals involved (see Gerards, 2011; Ölçer, 2008).[8] By requiring more detailed regulations and a higher level of procedural safeguards for investigative methods that interfere with the right to private life in a serious manner, the ECtHR aims to reduce the risk of abuse of governmental power.[9] The level of detail of the law and the procedural safeguards, that is, the 'quality of the law' that is required for regulating the investigative methods, thus depends on the gravity of the privacy interference that occurs when an investigative method is used.

7 Source: Oerlemans, 2017a, p. 91.

8 See also *P.G. and J.H. v. the United Kingdom*, para. 46.

9 See e.g., *Liberty and Others v. the United Kingdom*, para. 62; ECtHR 2 September 2010, ECLI:CE:ECHR:2010:0902JUD003562305, appl. No. 35623/05, para. 61 (*Uzun v. Germany*); and ECtHR 21 June 2011, ECLI:CE:ECHR:2011:0621JUD003019409, appl. no. 30194/09, para. 68 (*Shimovolos v. Russia*).

Consider the example of hacking by the police to gather evidence in criminal investigations. While the ECtHR has not yet decided on the issue of hacking as an investigatory power, it is likely to consider it a very serious interference with the right to private life (and possibly as an interference with the home and correspondence, as specific aspects of the right to respect for private life).[10] If so, the ECtHR will require a very detailed legal basis and significant safeguards in statutory law regulating hacking. This might include the condition to use the hacking power only in criminal investigations relating to very serious crimes, such as hacking vital IT infrastructures or in criminal investigations relating to violent crimes, such as murder. Furthermore, prior authorisation by an (investigatory) judge is likely to be required when hacking is employed. Prior authorisation by a judge or another independent authority functions as a safeguard because it reduces the risk that investigatory powers would be misused by governmental authorities. This makes it possible for the individuals involved in criminal investigations to foresee when and in what manner hacking as an investigative method may be used and which safeguards apply.

States will, of course, regulate investigative methods in different ways. In the Netherlands and other countries in continental Europe, criminal procedure law is regulated through 'law in the books'. Criminal procedure law is found first and foremost in Codes of Criminal Procedure (such as the Dutch Code of Criminal Procedure). Following the legality principle in criminal law, investigative methods that interfere with the right to privacy are regulated as 'investigative powers'. For very basic investigative methods, such as collecting information about a suspect in a criminal investigation by making use of the Google search engine for a limited amount of time, a general legal basis that stipulates that law enforcement authorities can conduct a criminal investigation will often suffice. Some states may introduce (more detailed) regulations in case law or guidelines (rather than statutory law), depending on different legal traditions (such as 'common law countries' like the United Kingdom), and because of cultural or historic reasons. Therefore, one cannot

10 See e.g., *Petri Sallinen and Others v. Finland*; ECtHR 16 October 2007, ECLI:CE:ECHR:2007:1016JUD007433601, appl. no. 74336/01 (*Wieser and Bicos Beteiligungen GmbH v. Austria*); ECtHR 3 July 2012, ECLI:CE:ECHR:2012:0703JUD003045706, appl. no. 30457/06 (*Robathin v. Austria*); ECtHR 14 March 2013, ECLI:CE:ECHR:2013:0314JUD002411708, appl. no. 24117/08 (*Bernh Larsen Holding AS and Others v. Norway*); ECtHR 30 September 2014, ECLI:CE:ECHR:2014:0930JUD000842905, appl. No. 8429/05 (*Prezhdarovi v. Bulgaria*); and ECtHR 17 December 2020, ECLI:CE:ECHR:2020:1217JUD000045918, appl. no. 459/18 (*Saber v. Norway*).

assume that when an investigative power sounds the same – such as, a 'computer search' – it has the same meaning and comes with the same safeguards in the law of different countries. For example, in the United States a 'search' can take place in a computer and can be conducted *remotely* (such as searching for data stored in the cloud); on the contrary, in the Netherlands, a 'search' can only take place in a physical place.[11]

9.2.2 Jurisdiction and cybercrime

The concept of 'jurisdiction' is particularly important in relation to criminal law, which is necessarily 'grounded' in notions of territoriality (Clough, 2015). The term jurisdiction describes the limits of the legal competence of a state or a different regulatory authority to make, apply and enforce rules of conduct upon persons (Lowe, 2006 in: Evans, 2006). The jurisdiction of a state can be split into (1) the capacity to make and apply law (the 'jurisdiction to prescribe' or 'prescriptive jurisdiction') and (2) the capacity to ensure compliance with such laws through executive, administrative, police or other non-judicial action (the 'jurisdiction to enforce' or 'enforcement jurisdiction').

Enforcement jurisdiction comes with a strict territorial limitation. The generally accepted view is that states can only investigate crimes on their own territory and according to their own rules, as a way of exercising their sovereign rights. This strict territorial limitation of enforcement jurisdiction was made explicit by the Permanent Court of International Justice as early as 1927.[12] This means that law enforcement officials cannot conduct a criminal investigation on foreign territory without ad hoc permission from a foreign state or a treaty with that state. Gathering evidence on the territory of another state without permission or consent derived from a treaty can, thus, lead to a conflict between the two states. The reason is that these extraterritorial investigatory activities can be perceived as an infringement of the territorial

11 In the United States, a remote search is regulated by Rule 52 of the United States Code of Criminal Procedural Law. In the Netherlands, a search can also take place remotely with a different special investigative power called a 'network search' or the 'power to gain remote access in computers' (i.e., hacking power), which are regulated by Art. 125j, 557 and Art. 126nba of the Dutch Code of Criminal Procedure.

12 PCIJ, SS Lotus, 1927, *PCIJ Reports*, Series A, No. 10 (*France v. Turkey*): 'The first and foremost restriction imposed by international law upon a State is that – failing existence of a permissive rule to the contrary – it may not exercise its power in any form in the territory of another State. In this sense jurisdiction is certainly territorial; it cannot be exercised by a State outside its territory except by virtue of a permissive rule derived from international custom or from a convention.'

sovereignty of the other state. This is so because it is the exclusive function of the state to conduct criminal investigations within its own territory (Schmitt, 2017).

As a consequence of territorial sovereignty, each state possesses its own set of local criminal laws that define what behaviours constitute 'cybercrimes'. These states also have local authorities who are responsible for investigating cybercrimes in accordance with their local procedural laws, which outline the investigative powers that can be applied collect evidence in criminal investigations within its own territory. Furthermore, these states have local authorities tasked with prosecuting cybercrimes, which are subsequently adjudicated in local courts. In contrast, it has become clear from earlier chapters that cybercrime is a thoroughly global phenomenon. Law enforcement officials oftentimes need to gather evidence on foreign territory and prosecute foreign individuals. Consequently, cybercrime investigations often extend beyond the territorial borders of the state (see UNODC, 2013). The differences in the regulation of cybercrimes and the regulation of investigative powers, often hamper criminal investigations that extend beyond the territorial borders of a state.

9.2.3 Mutual legal assistance

To collect evidence located abroad, states often rely on the formal mechanism of 'mutual legal assistance' to request and obtain evidence on foreign territory. Through this mechanism, states can agree on the conditions under which evidence can be gathered upon request on their territory by local law enforcement authorities, or even unilaterally by foreign law enforcement officials under the supervision of local law enforcement authorities. If a state is unwilling to cooperate with a legal assistance request to gather evidence, investigating authorities of the investigating state may simply be left empty-handed (Stigall, 2013).

The conditions in which mutual legal assistance is provided to other law enforcement authorities can be agreed upon in 'mutual legal assistance treaties' (MLATs). The process of mutual legal assistance, with the United States as an example of the receiving state of a mutual legal assistance request, is illustrated below in Figure 9.2.

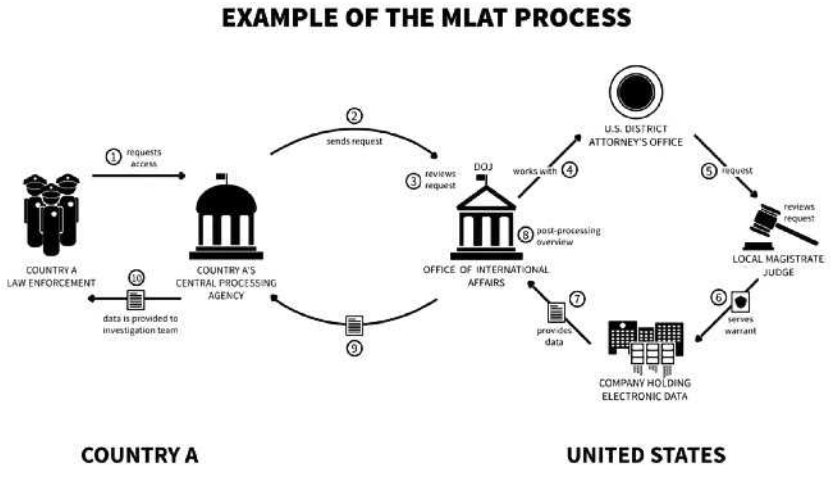

Figure 9.2 Mutual legal assistance treaty process[13]

The Convention on Cybercrime is the most important multilateral treaty when it comes to cross-border cybercrime investigations. The Convention is particularly important for the following three reasons.

(1) *Harmonisation of criminal substantive law with regard to cybercrime.* Harmonisation of criminal substantive law facilitates mutual legal assistance, because states criminalise harmful behaviours in a similar manner. This makes it easier for states to agree on mutual legal assistance to gather evidence from other states and to extradite individuals.

(2) *The obligation to introduce certain investigative powers in a domestic legal framework.* The regulation of investigative powers is important, because it provides practical tools for law enforcement authorities to investigate cybercrimes.

(3) *The creation of a system for swift international cooperation.* The Convention on Cybercrime obliges member states to create a contact point to ensure the provision of immediate mutual legal assistance for cybercrime investigations.[14] The contact point must be available 24 hours a day, 7 days a week. The contact point ensures that the assigned law enforcement authority within a member state is able to coordinate mutual legal assistance proceedings with foreign law

13 Source: Lin & Fidler, 2017, p. 3

14 See Art. 35 of the Convention on Cybercrime.

enforcement authorities. The aim is to make mutual legal assistance procedures in cybercrime investigations more efficient.

However, two states that are crucial to cybercrime investigations, Russia and China, did not ratify the Convention on Cybercrime (Kalecová, 2015; Kshetri, 2013; Taylor et al., 2010).[15] Therefore, these states (a) may have regulated cybercrimes in a completely different manner, (b) have not necessarily implemented all of the investigatory powers found in the Convention in their domestic legal frameworks, and (c) do not have a contact point that is obliged to cooperate with foreign law enforcement authorities that ratified the convention. This may therefore frustrate international cybercrime investigations.

All states can use traditional mutual legal assistance to collect evidence located abroad.[16] Within the EU, these traditional instruments were considered insufficient to effectively fight transnational crime, such as cybercrime. To make judicial cooperation in criminal matters simpler and more effective, the EU created legal instruments based on the principle of 'mutual recognition'. 'Mutual recognition of judicial decisions' means that each EU Member State will execute foreign decisions by other Member States as if they were their own.[17] In the realm of cybercrime investigations, this principle would ideally eliminate the need for procedural formalities, allowing for investigative orders with extraterritorial effect. This is not the case in reality, however, because the power to regulate criminal (procedural) law is a sensitive policy area and considered an essential component of the core sovereign powers of the state. Nonetheless, in 2009 many EU Member States gave up a part of their sovereignty by granting the European Commission the authority to propose regulations governing criminal (procedural) law in the Treaty of Lisbon.[18] Consequently, cybercrime was explicitly designated in Article 83 TFEU as a serious transnational criminal phenomenon falling within the EU's jurisdiction.

15 Allegedly, cyberattacks commonly originate from their territory.

16 See, for example, the European Convention on Mutual Assistance in Criminal Matters, OJ C 197, 12 July 2000.

17 See also Art. 67(3) and 82(1) of the Treaty on the Functioning of the European Union (TFEU).

18 Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, OJ C 306, 17 December 2007.

In practice, EU criminal law primarily focusses on establishing minimum standards and facilitating cooperation among its Member States, rather than dictating criminal procedural laws of its own. Through treaties, the EU can regulate the conditions under which investigative powers are to be exercised by Member States. Instituting common minimum standards for criminal procedure, to which all Members States have committed, cultivates trust in the legality and fairness in the legislation of other Member States. As such, it emphasises the importance of 'mutual trust' as a prerequisite for effective cooperation, whereby Member States must trust each other's criminal justice systems. This trust is founded on their shared commitment to the principles of freedom, democracy and respect for human rights, fundamental freedoms, and the rule of law.[19] For instance, adherence to the ECHR is mandatory for all EU Member States. Across Europe, case law relating to the ECHR has already introduced sufficient and proven minimum standards for criminal proceedings. The adoption, codification and amendment of fundamental rights and procedural safeguards in the Charter of Fundamental Rights of the EU (EU Charter) further bolsters trust in the legality and fairness in the legislation of other Member States (Ronsfeld, in Ambos & Rackow, 2023).

The EU has established several agencies to facilitate and strengthen efforts to combat transnational crime, including cybercrime, most notably Europol and Eurojust.[20] It is essential to understand that these agencies do not function as federal law enforcement authorities akin to the FBI in the U.S. (Ligeti & Giuffrida, 2023). Europol has no special investigatory powers.[21] However, in 2022 Europol was granted the authority to utilise data analysis techniques on large (bulk) datasets and transfer relevant information to Member States. Law enforcement authorities can subsequently use that information in criminal investigations (Tas, 2023).[22] An illustrative example of Europol's capabilities

19 See Council of ministers, *Programme of Measures to Implement the Principle of Mutual Recognition of Decisions in Criminal Matters*, OJ C 12/10, 15 January 2012, p. 11.

20 Council Act of 26 July 1995 drawing up the Convention based on Art. K.3 of the Treaty on European Union, on the establishment of a European Police Office (Europol Convention), OJ C316/01, 27 November 1995 and Council Decision of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime, OJ L 63/1, 6 March 2002.

21 See Art. 88 TFEU and FAQ, 'Is Europol a European FBI?', *europol.europa.eu*, 4 November 2016.

22 Regulation (EU) 2022/991 of the European Parliament and of the Council of 8 June 2022 amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role in research and innovation 2022 (OJ L).

emerged in the aftermath of the EncroChat operation (as detailed below), where Europol's expert team analysed over 115 million EncroChat messages and associated data received from the Joint Investigation Team (JIT) partners. Europol cross-checked and analysed the data, combined it with information available in its information systems and provided close to 700 actionable intelligence packages to countries worldwide.[23]

The most important EU instrument (called a 'Directive') to collect evidence in criminal proceedings is the European Investigation Order (EIO).[24] The EIO is a 'judicial' decision mandating the collection of evidence, whether pre-existing or to be acquired through investigative measures, from another Member State. Additionally, the EIO can encompass requests for securing or freezing evidence. While the EIO operates under the principle of mutual recognition, it does not entail blind or automatic acceptance and execution of the requested measure. Instead, as a rule, the grounds for refusal are restricted to a minimum (Bachmaier Winter, 2010). This means that the executing state is not empowered to assess the adequacy, necessity, or proportionality of the requested measure; it must in principle trust the judgement of the issuing state. Nevertheless, the measure is subject to specific requirements, conditions, and scrutiny. States retain the right to decline execution if the order contravenes their constitutional principles or if investigative measures exceed those permitted in comparable domestic proceedings (Bachmaier Winter, 2023).

In practice, the EIO assumes a significant importance in transnational cybercrime investigations. The EncroChat operation serves as a pertinent illustration, showcasing a contemporary application of EU legal assistance mechanisms.

23 Europol press release, 'Dismantling encrypted criminal EncroChat communications leads to over 6.500 arrests and close to EUR 900 million seized', *eurpol.europa.eu*, 23 June 2023.

24 Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, OJ L 130, 1 May 2014.

Case study: legal assistance in the EncroChat-operation

EncroChat was a communications service provider located in France. The company offered modified smartphones (also called 'cryptophones' or 'PGP phones') running EncroChat software. This software and the modified hardware provided users with a high level of security and enabled users to automatically encrypt their calls and messages. All network traffic was routed through servers located in Roubaix, France. In order to collect the information, the servers and EncroChat phones were hacked by French law enforcement authorities, operating in a Joint Investigation Team (JIT) with the Dutch law enforcement authorities and Europol. From 1 April 2020 to 20 June 2020, the French *Gendarmerie* collected over 120 million EncroChat messages sent from tens of thousands of mobile telephones (Oerlemans & van Toor, 2022). With the authorisation of the *tribunal correctionnel de Lille* (Criminal Court of Lille, France), a Trojan (a type of malware) was first uploaded to the server in the spring of 2020 and was, from there, installed on those mobile phones via a simulated update. Of a total of 66.134 subscribed users, 32.477 users in 122 countries are said to have been affected by that software, including approximately 4.600 users in Germany.[25]

France then informed other Member States of the operation. On 9 March 2020, representatives of the *Bundeskriminalamt* (the Federal Criminal Police Office in Germany; 'the BKA') and of the Frankfurt Public Prosecutor's Office, as well as representatives of the French, Dutch and United Kingdom authorities, participated in a videoconference organised by Eurojust. During that videoconference, the representatives of the French and Dutch authorities informed the representatives of the other Member States' authorities of their investigation of an encrypted mobile phone operating company and of their planned interception of data, including data from mobile phones located outside French territory. The representatives of the German authorities signalled their interest in the data of the German users. On 13 March 2020, the BKA announced that it was opening an investigation in respect of all unknown users of the EncroChat

25 CJEU 30 April 2024, C-670/22, ECLI:EU:C:2024:372, para. 20 (*EncroChat*).

service, on suspicion of engaging in organised trafficking in substantial quantities of narcotic drugs and of forming a criminal association. The BKA justified the opening of that investigation by explaining that the use of the EncroChat service in itself gave rise to a suspicion that serious criminal offences were being committed, in particular the organisation of drug trafficking.[26]

On 2 June 2020, the Frankfurt Public Prosecutor's Office requested authorisation from the French authorities, by way of an initial EIO, to use the data from the EncroChat service without restriction in criminal proceedings. This investigation order was recognised by the competent examining judge in Lille on 13 June 2020, and the transmission of the requested data was set in motion. In this case, the question was raised whether a public prosecutor could be considered as 'judicial authority' for the purpose of issuing an EIO, taking into account that some public prosecution authorities are not completely independent being subject to instructions from the executive branch. On 30 April 2024, the (Grand Chamber) of the Court of Justice of the European Union made clear that the German public prosecutor was competent to order the transmission of the (EncroChat) evidence, which was already in the possession of the competent authorities of the executing state (France).[27] The EU Court, however, made clear that a court before which an action against an EIO is brought must nevertheless be able to review compliance with the fundamental rights of the persons concerned.

Mutual legal assistance, which remains the norm outside of the EU, has two notable limitations. The first limitation is that mutual legal assistance is only available insofar as states are able to agree upon the conditions for extraterritorial evidence gathering. Consequently, law enforcement officials are completely dependent on the willingness of local law enforcement authorities to cooperate when no treaty can be negotiated. The second limitation is that mutual legal assistance is a very burdensome and time-consuming procedure, especially when it comes to cybercrime. On the one hand, mutual legal assistance procedures take too much time for the requested (local) law enforcement officials that are gathering the evidence. On the other hand, it takes too much time before the requesting (foreign)

26 Ibid., para. 21-22.
27 Ibid., para. 77.

law enforcement authority actually receives the evidence. In general, the time required is a matter of months, rather than days (UNODC, 2013).

Many law enforcement authorities consider mutual legal assistance mechanisms too slow and unable to meet the investigative and prosecutorial challenges of cybercrime investigations (Koops & Goodwin, 2014; UNODC, 2013). As an alternative, law enforcement authorities sometimes seek to apply digital investigations *unilaterally*, that is, without permission from the affected state or a treaty basis that would authorise the evidence-gathering activity. Strictly speaking, such unilateral investigations are not allowed. However, the intensity of the interference with sovereignty of the affected state is also dependent on the specific investigative method used.

States are not likely to engage in war over unilateral investigations by law enforcement authorities. Nonetheless, a state can – and often will – react to unilateral extraterritorial activities of law enforcement authorities that it does not deem permissible. At the very least, states can demand an apology, an acknowledgment of the wrongful act, or a commitment to discontinue those activities in the future (Koops & Goodwin, 2014). Foreign law enforcement authorities that engage in unauthorised extraterritorial evidence-gathering on foreign territory can also be prosecuted under local criminal laws of the affected state (usually with little practical effect, since the person charged will likely not be extradited to the foreign jurisdiction (Doyle, 2012)).[28] Furthermore, states increasingly use economic and political sanctions to show their discontent with the practice.

In the meantime, there are many developments with regard to mutual legal assistance treaties, especially with regard to data production orders to gather evidence from Internet Service Providers (hereinafter ISPs) (see Section 9.3.1). These developments, as well as the possible unilateral application of digital investigative methods will be discussed throughout this chapter.

9.3 IP addresses as digital leads

An IP address is a unique number assigned to every device on a network, which allows the devices to communicate with each other. As such, it can be

28 See, e.g., J. Leyden, 'Russians accuse FBI agent of hacking', *The Register*, 16 August 2002.

an important digital lead in cybercrime investigations. To make this clear, let us consider a short scenario:

Case study: IP addresses from an internet forum

After an international police operation (coordinated by Europol), Dutch law enforcement authorities receive a high number of IP addresses from Europol.[29] According to Europol, the IP addresses originate from an online forum where child sexual abuse material (CSAM) was exchanged. A copy of the server with corresponding messages and material is also available. User data from these accounts on the internet forum, include IP addresses that can be traced back to internet service providers in various EU Member States. In this case, Europol forwards the IP addresses that can be linked to the Netherlands to the Dutch police. Dutch law enforcement officials must then link the IP addresses to suspects in the Netherlands so that it can be proved that they were active on the forum. How does that work?

Step 1:
First of all, a search in the so-called 'WHOIS-database' can be used to find out which ISP issued the IP address. If the IP address belongs to a Dutch ISP, there is a chance that the suspect is also Dutch.

Step 2:
In the Netherlands (as well as in most other European countries), investigating officers can demand the data about the subscriber (usually the person who pays for the internet connection) from the ISP through a data production order. This way, a name and address can be gathered, thus potentially revealing the address where the suspect lives.

Step 3:
By searching the suspect's residence, which requires an authorisation from a public prosecutor and a warrant from an investigatory judge, evidence about the crime can be gathered. Investigating officers will then search for data carriers, such as computers and hard drives, which

29 See e.g. the judgment of the Court of Zwolle-Lelystad of 1 June 2010, ECLI:NL:RBZLY:2010:BM9626.

may have been used to store and distribute CSAM. These devices will be seized.

Step 4:
Investigating officers look for CSAM or other evidence of the crime (such as, messages sent or nicknames used) on the seized data carriers and connected networks.

Step 5:
Oftentimes, witness statements from the occupants of the (neighbouring) premises are taken. And, if found, the suspect may be arrested and questioned.

In the above scenario, there is a good chance that the suspect will be identified, and proof will be found that the suspect possessed or exchanged CSAM via the online forum. Nevertheless, it is important to realise that the above scenario is an ideal scenario from an investigative perspective. In practice, cybercriminals often use anonymisation techniques, such as a VPN (virtual private network) connection, to hide their IP address. Section 9.4.1 discusses these techniques in more detail.

In this description of the investigatory process for a digital trace of an IP address, various investigatory powers have been mentioned. We briefly discuss these investigatory powers in the following subsections.

9.3.1 Data production and preservation orders

Data production orders are extremely important in cybercrime investigations. As already mentioned, relevant data, such as subscriber data and logging data pertaining to the activities of the subscriber, can be gathered from ISPs. Other electronic communication service providers, such as Google or Microsoft, may also have data that is relevant for law enforcement authorities. Data production orders enable law enforcement authorities to collect not only subscriber information and traffic data but also content data, such as stored documents or the contents of e-mails. Different types of communications can be gathered using different types of data production orders that are sent by law enforcement authorities. The data is then collected in order to gather evidence in a criminal investigation.

Subscriber data includes the subscriber's identity, postal or physical address, telephone and other access number and billing and payment information, available on the basis of the service agreement or arrangement.[30] IP addresses and subscriber information data are generally not considered as particularly privacy sensitive and can usually be gathered by law enforcement authorities without a warrant from an examining judge.[31]

In contrast, 'traffic data' is (nowadays) considered highly privacy sensitive information. Traffic data (also called *metadata*) can reveal the following information about a communication: its origin, destination, route, time, date, size, duration, and type of underlying service.[32] Traffic data therefore enables law enforcement officers to learn about (a) the devices used by a suspect, (b) the internet services that a suspect is using at a specific time, and (c) the location data of a suspect's device. The Court of Justice of the European Union considers traffic information particularly sensitive and requires prior authorisation of an examining judge or an independent institution to collect traffic data with a data production order.[33]

Finally, 'content data' can be defined as 'data with regard to the meaning or message conveyed by the communication, other than traffic data'.[34] This includes private messages that can be sent using electronic communication services and documents stored at electronic communication service providers. Content data is traditionally considered as the most privacy sensitive data, thus requiring stringent safeguards when law enforcement authorities want to gather them. States often require specific investigatory powers combined with appropriate safeguards, such as prior authorisation by an examining judge to obtain the information.

30 See Art. 18 Convention on Cybercrime.

31 See, e.g., ECtHR 30 January 2020, ECLI:CE:ECHR:2020:0130JUD005000112, appl. no. 50001/12, para. 92 and 94 (*Breyer v. Germany*) and CJEU 6 October 2020, C-511/18, C-512/18 and C-520/18, ECLI:EU:C:2020:791 (*La Quadrature du Net et al. v. Premier ministre et al.*) and CJEU 30 April 2024, C-470/21, ECLI:EU:C:2024:370 (*La Quadrature du Net and Others*). However, a serious interference does takes place when IP addresses are used to 'track an internet user's complete clickstream' and, therefore, their online activity enable a 'detailed profile' of the user to be produced. See also ECtHR 24 April 2018, ECLI:CE:ECHR:2018:0424JUD006235714, appl. no. 62357/14, para. 129-130 (*Benedik v. Slovenia*), in which a warrant was required for obtaining dynamic IP addresses.

32 Art. 1(d) Convention on Cybercrime.

33 CJEU 2 March 2021, C-746/18, ECLI:EU:C:2021:152 (*H.K. v. Prokuratuur*).

34 Explanatory Report to the Convention on Cybercrime (2001), para. 209.

As already mentioned, data production orders are a very important tool in cybercrime investigations. For this reason, the Convention on Cybercrime specifically obliges states that have ratified the Convention ('contracting parties') to implement legislation empowering law enforcement authorities to issue data production orders to electronic communications service providers. Importantly, Article 15 of the Convention on Cybercrime requires that all of these investigatory powers are established and exercised in a way that provides for adequate protection of human rights and liberties, as can be found in the ECHR and other national or international human rights instruments. As such, Article 15 essentially integrates the case law of the ECtHR into the Convention on Cybercrime (Hildebrandt, 2020). This means that the investigatory powers need to provide for sufficient conditions and limitations, such as judicial supervision, grounds justifying application, and limitation of the scope and the duration of the power (e.g. applied to an individual case, rather than to indiscriminate groups of subscribers).

Article 18 of the Convention on Cybercrime requires contracting parties to establish powers for law enforcement authorities, enabling them to compel service providers offering services in their territory to provide subscriber data. The scope of this power is limited, since law enforcement can only request access to subscriber data, but not to traffic or content data. The power is also limited to the extent that the provider actually maintains subscriber data; some providers might namely store more and others less data on subscribers. Nevertheless, it is an important power, as subscriber data is said to be the most often sought data in criminal investigations (Cybercrime Convention Committee, 2017), and plays a key role in establishing the identity of the suspect (as seen in Step 2 of the above scenario).

On 17 November 2021, the Second Additional Protocol to the Convention on Cybercrime was adopted. In this context, the additional protocol creates a legal basis for direct searches of domain name information from domain name registration service providers, using the WHOIS-database (see Step 1 of the above scenario). Furthermore, Article 7 creates the legal basis for direct requests of subscriber data to foreign internet service providers. This represents a departure from the traditional principle in international law whereby states decide whether to authorise searches within their territories, rather than companies. The new rules can contribute to criminal investigations by speeding up and simplifying the identification of internet users, based on identifying information, such as an IP address, or locating internet users or computers based on network traffic data.

Besides the production order, the 'preservation order' is also an important investigatory power. Article 16 of the Convention on Cybercrime establishes an obligation for states to ensure that law enforcement authorities are able to request the 'expedited preservation of specified stored computer data' in connection with a specific criminal investigation. The purpose of this power is to preserve data, which are vulnerable to loss and modification. This provision applies to any type of stored computer data (i.e. subscriber, traffic and content), but it bears particular importance for traffic data, which are usually retained for only a short period of time by service providers.[35] Stored traffic data are critical for determining the source or destination of a past communication, which can be necessary for identifying persons who have, for instance, distributed CSAM or malware. Oftentimes, however, more than one service provider is involved in the transmission of a communication, so that no single provider possesses enough of the crucial traffic data to be able to determine the actual source or destination of the communication. The following article, Article 17 of the Convention, thus ensures that expeditious preservation of traffic data can be achieved among all of the service providers involved (in theory).

Article 32(b) of the Convention on Cybercrime provides for the possibility of law enforcement authorities to access (any type of) computer data stored in another country, when lawful and voluntary consent is obtained from the 'person' who has the lawful authority to disclose the data. This includes accessing or receiving computer data from extraterritorial service providers, such as cloud operators, on the basis of their voluntary cooperation (UNODC, 2013).[36] However, Article 32(b) is drafted in permissive terms, stating that contracting parties 'may' undertake such actions, rather than imposing an obligation to introduce such a power in national law (seen by the use of the term 'shall'). As such, states may nevertheless prevent other states from accessing data stored in their territory based on voluntary cooperation from service providers.

In practice, online service providers indeed commonly *voluntarily* disclose information to foreign law enforcement authorities, at least under certain conditions. For instance, Microsoft states on its website that it voluntarily discloses customers' non-content data (i.e. subscriber but also traffic data) with foreign government agencies, requiring only a subpoena or its local

35 See Explanatory Report to the Convention on Cybercrime (2001), para. 27.
36 See also Explanatory Report to the Convention on Cybercrime (2001), para. 294.

equivalent, that is, a production order without prior judicial oversight.[37] Microsoft also voluntarily discloses content-data, but requires a warrant, court order, or its local equivalent for such disclosure.[38]

Case study: Microsoft v. Ireland

In 2014, Microsoft fought a data production order from U.S. law enforcement authorities (therefore, based on U.S. law) to obtain stored content data on servers at Microsoft's subsidiary in Ireland.[39] Microsoft had already handed over subscriber and traffic data to U.S. law enforcement authorities, but it refused to execute the data production order with regard to content data.

Microsoft was of the opinion that the information being sought should have been obtained using mutual legal assistance as stipulated in Irish law, stating that Irish law and EU directives apply to 'Hotmail and Outlook.com accounts hosted in Ireland'.[40] The U.S. Department of Justice argued that under the U.S. Stored Communications Act, the location of the records is irrelevant.

The U.S. Court of Appeals concluded that the Stored Communications Act does not have extraterritorial reach.[41] The content data is located on Microsoft's data centre servers in Ireland. Therefore, using the location of the stored data as a localisation principle, the judges concluded that a U.S. warrant under the Stored Communications Act cannot force Microsoft to send the data from Ireland to the United States.[42]

37 Microsoft (2020), 'Law Enforcement Requests Report'.

38 Ibid. For a broader overview of cooperation of service providers with foreign law enforcement, see Cybercrime Convention Committee (2017).

39 See B. Smith, 'We're Fighting the Feds Over Your Email', *The Wall Street Journal* (opinion), 29 July 2014.

40 See 'Frequently Asked Questions', Microsoft Transparency report (2014).

41 U.S. Court of Appeals District Court of Connecticut, (2nd circuit), In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation, *Microsoft Corporation v. United States of America*, 14 July 2016, p. 42.

42 U.S. Court of Appeals District Court of Connecticut, (2nd circuit), In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation, *Microsoft Corporation v. United States of America*, 14 July 2016, p. 39.

Mutual legal assistance and data production orders

As a response to the Microsoft Ireland case, the United States adopted the Clarifying Lawful Overseas Use of Data Act (hereinafter: 'CLOUD Act') in 2018.[43] There are two key elements of the CLOUD Act: (1) provisions on access to data by U.S. authorities that are stored abroad, and (2) provisions to create executive agreements for access to data by other states that are stored in the U.S.

The first part of the CLOUD Act amends the Stored Communications Act, simply giving the statute extraterritorial reach. Consequently, U.S. companies like Microsoft are mandated to provide data to U.S. law enforcement authorities, when they have issued a data production order, even if the data is located outside of the United States. Therefore, U.S. courts can compel the production of such data, despite objections of the service provider, even if it conflicts with the laws of another jurisdiction.

The second part of the CLOUD Act permits foreign states that have robust protections for privacy and civil liberties to enter into executive agreements with the United States for the purpose of obtaining access to data stored in the United States. Unlike with the MLAT process, such an agreement would allow partner states to request data stored by a service provider in the United States without a review of the foreign data production order by a U.S. federal official or court. And *vice versa*: the agreement also requires the partner state to remove legal barriers that would prevent the U.S. government from issuing orders to service providers within their borders. A CLOUD Act executive agreement thus permits data to be requested by foreign law enforcement based solely on their domestic legal procedure. This process is illustrated in Figure 9.3 below.

43 EPIC (2018) 'The CLOUD Act'.

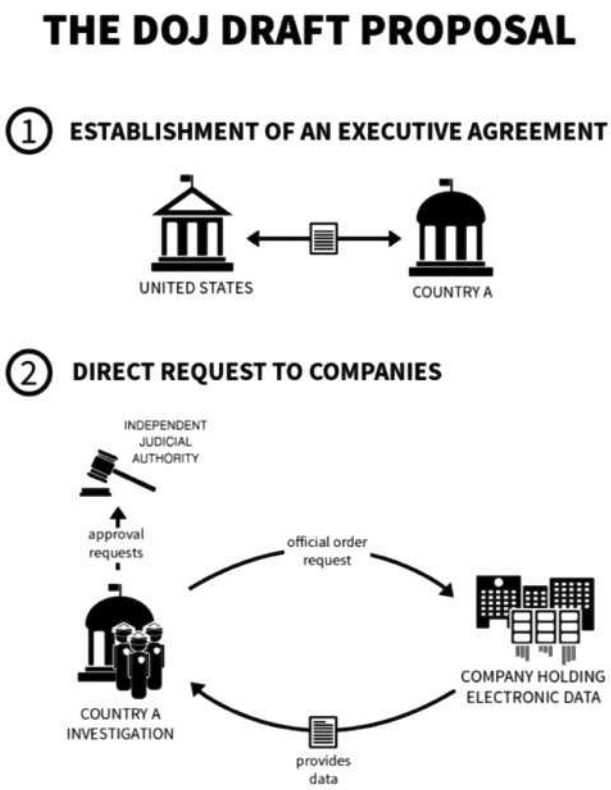

Diagram 2 Diagram of DOJ Cross-Border Data Access Proposal

Figure 9.3 Process of data production orders under an executive agreement[44]

On the one hand, such an executive agreement establishes a much quicker and more efficient process for transborder data access than the MLAT process. On the other hand, it has been criticised for allowing foreign governments to access user data, records and even real-time communications with lowered procedural safeguards in place.[45] In 2019, the United States and the UK were the first countries to enter into such an executive agreement.[46] It can be said that this agreement was only possible due to the very close

44 Lin & Fidler, 2017, p. 6.

45 C. Fischer, 'The CLOUD Act: A dangerous expansion of police snooping on cross-border data', *Electronic Frontier Foundation* (8 February 2018).

46 U.S. Department of Justice, 'U.S. and UK sign landmark cross-border data access agreement to combat criminals and terrorists online' (3 October 2019).

political and legal ties between the two countries (Christakis & Terpan, 2021).[47]

At the EU-level, another important development took place in 2023, when the EU adopted the 'e-Evidence package', consisting of a Regulation and a Directive.[48] Like the Second Additional Protocol to the Cybercrime Convention, the e-Evidence package aims to simplify and speed up access to data in the hands of foreign ISPs. Unlike the Protocol, however, the package applies to all types of stored data: subscriber and other types of data requested for the sole purpose of identifying the user, traffic data and content data. The e-Evidence package was deemed necessary because electronic service providers face a fragmented system of data retrieval schemes and gathering this form of digital evidence from electronic service providers under the current mutual legal assistance system – including the European Investigation Order – was considered (too) time-consuming (Ligeti & Robinson, 2021).

The e-Evidence Regulation establishes a European Production and a European Preservation Order, enabling EU law enforcement agencies to compel ISPs in another EU Member State to produce and preserve data, which may serve as evidence in criminal proceedings. This development has been called revolutionary as it sidesteps the traditional approach to jurisdiction stemming from international law, according to which the jurisdiction to enforce laws (enabling law enforcement to open and conduct investigations) ends with the physical borders of the state. Based on the e-Evidence Regulation, a law enforcement agency in one EU Member State can issue an order for the production of data to an ISP in another Member State *directly*: (1) regardless of where the data sought are physically stored (even if that storage is in a data centre abroad) and (2) without the involvement of the competent authorities of the Member State to which the order has been sent

47 For a discussion on the possibility of an EU-U.S. executive agreement based on the Cloud Act.

48 Regulation (EU) 2023/1543 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings (OJ L 191, 28 July 2023) and Directive (EU) 2023/1544 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings (OJ L 191, 28 July 2023). The Regulation and Directive will enter into force in 2026.

(except for a few very limited situations).[49] An important limitation of these data production orders is that traffic and content data may only be requested for offences punishable by a maximum term of imprisonment of at least three years in the issuing country or for specific cyber- and terrorism-related offences.[50]

The production of data therefore takes place without an assessment of the validity and legitimacy of the orders by competent authorities of the enforcing state (for example, verifying whether the order has been issued by a competent authority or whether the double jeopardy requirement has been met). This has led some scholars to designate the Regulation as a 'quantum leap of mutual trust' (Tosza, 2023). Without the need to conduct any such check, ISPs need to transmit the data within ten days from the receipt of the order and, in cases of emergency, within eight hours.

For this new system to work, there needs to be at least one addressee to which the newly created European Production and Preservation Orders can be submitted. This is accomplished through the e-Evidence Directive, which establishes an obligation for ISPs 'offering services' in the EU to appoint a legal representative for the purpose of gathering evidence in criminal proceedings in an EU member state. The ISPs falling under the scope include not only electronic communications services, but also other information society services, such as storage or processing services and internet domain name or IP numbering services. Importantly, an ISP is not required to be physically present in the EU (for instance by having headquarters or data centres in the EU). What matters is the 'virtual presence' of the ISP in the EU. This virtual presence is established if there is a 'substantial connection based on specific factual criteria' to an EU Member State, for instance a significant number of users in one or more Member States, or the targeting of activities towards one or more Member States (for example, by using the language of that state or through advertising). This means that any ISP established anywhere in the world potentially falls under the scope of the Regulation and Directive.

49 The authorities of the state to which the order has been sent ('the enforcing state') are only notified when traffic and content data are being sought. However, this obligation does not apply in cases that are purely 'national'. That will be the case where the offence has been committed or is likely to be committed in the issuing state and where the person whose data are being requested resides in the issuing state (Art. 8 (2) e-Evidence Regulation). The assessment, whether the case is national or not, is made by the issuing state.

50 See Art. 5(4) and recital 40-41 e-Evidence Regulation.

While certainly simplified and with the potential to be incredibly fast, this new system for data production leads to concerns for the protection of fundamental rights and principles, including the right to respect for private life, the protection of personal data and the right to effective judicial protection. In this new system, ISPs have become the main guardians of individuals' rights and freedoms, a task usually reserved for public authorities with features of accountability, impartiality, and independence. Unlike public authorities, ISPs are private actors primarily motivated by their business interests and accountable to their owners and stakeholders, rather than protection of persons' rights and freedoms (Mitsilegas, 2018; Tosza, 2024). This issue of conflicting interests is magnified by the fact that ISPs may refuse to produce data only in very limited cases, mainly involving orders that are incomplete, contain manifest errors or do not contain sufficient information to execute it, or because the production of data is *de facto* impossible. A refusal to comply with the order may result in a fine of up to 2% of the total worldwide annual turnover to the ISP. Moreover, even when ISPs would want to act for the greater good, the task of ensuring persons' rights and freedoms may prove too difficult a task for smaller ISPs, with a small number of employees and a lack of relevant legal knowledge.

9.3.2 Seizing and analysing data on computers

In many cybercrime investigations, data carriers play a particularly important role, as they may contain evidence of the offence committed. Digital forensic investigations may be conducted on data carriers, such as laptops, PCs, smartphones and USB sticks. Traditionally, an exact copy of a hard disc (or another source) is made at the beginning of a forensic investigation, after which the copy (i.e. an 'image') is examined for evidence. Nowadays, *live forensics* is preferred, whereby, for example, the random-access memory (RAM) of computers is also secured and an investigation can be extended to computer networks (discussed in Section 9.3.3). This makes it possible, among other things, to determine which users have logged into the computer or an account recently (Casey, 2011).

Forensic software makes it possible to organise different types of files and to analyse each file. Deleted files can also often be recovered. Moreover, developments in digital forensics are rapid. For example, new types of devices with new operating systems need to be investigated all the time. The exponential growth of the amount and types of data thus requires that forensic techniques continue to develop (Henseler, 2017). Software can

help make these investigations more effective and efficient, for instance, by automating the analysis of unstructured data and by discovering patterns and links between huge amounts of data (i.e. data mining).

Case study: Hansken

The Netherlands Forensic Institute (NFI) has developed an innovative system for searching data. This platform, called 'Hansken', allows large amounts of different types of data to be quickly and thoroughly analysed in a controlled environment, in which every step is logged. Datasets can be searched quickly in order to establish links between various attributes, such as user names, nicknames, telephone numbers and e-mail addresses. This enables investigating officers and analysts to work more quickly and effectively (van Beek et al., 2015). The software is used for investigations into serious drug crime and murder cases in the Netherlands and has provided important evidence in several cases. One of the first public examples of Hansken's use was in the case against Naoufal 'Noffel' F., who was suspected of ordering the murder of another person through an extra-secure mobile phone (Schermer & Oerlemans, 2020).[51]

Numerous Dutch suspects involved in criminal cases in the past years were communicating with so-called 'PGP phones', also known as 'crypto phones', designed to facilitate secure, encrypted communication using the Pretty Good Privacy (PGP) protocol. Following several police operations, over a billion (!) messages exchanged through various crypto phones have been meticulously stored by Dutch law enforcement agencies.[52] These 'bulk datasets' can then be analysed by Hansken, employing dozens of forensic tools available on its platform. For example, the system enables the use of keyword searches and AI techniques like object recognition and machine translation, to

51 Court of Amsterdam 19 April 2018, ECLI:NL:RBAMS:2018:2504.

52 H. van Gelder, 'Politie beschikt over 1 miljard "criminele" chats en de teller loopt door: "Goud in handen"' ['Police has over 1 billion "criminal" chats and it keeps counting: "pure gold"'], *AD.nl* 13 April 2023. See also J.J. Oerlemans, 'Overzicht cryptophone-operaties', *jjoerlemans.com*, 19 November 2023.

analyse the content and metadata of these messages.[53] Often, these messages serve as crucial evidence in criminal proceedings, potentially revealing incriminating details. Substantiating the connection between suspects and their mobile phones requires meticulous analysis, linking nicknames and metadata of messages to individuals. Moreover, evidence from additional sources frequently supplements criminal investigations.

Some legal scholars argue that the landscape of investigative procedures has undergone a profound transformation due to the meticulous analysis of secured crypto messages. From these data sets, new investigations are initiated, heralding the advent of what is called 'data-driven investigations' (Hirsch Ballin & Oerlemans, 2023; Galič et al., 2024). The rules and regulations that apply in this regard – and are becoming increasingly important – are not only found in the Code of Criminal Procedure but also in the Police Data Act (based on the EU Data Protection Law Enforcement Directive).[54] It is for reasons such as these that legal authors in the Netherlands advocate for greater attention to compliance with and oversight of these rules in criminal cases (Fedorova et al., 2022; Hirsch Ballin & Oerlemans, 2023; Schermer & Galič, 2022; Stevens et al., 2021).

The above example illustrates that digital evidence on data carriers does not play a role only in investigations into cyber-dependent crimes, which are wholly mediated by technology and cannot be committed without the use of computer networks (e.g., a ddos attack). Increasingly, digital evidence also plays a role in traditional criminal cases, such as murder investigations, where the use of computers and the internet play a supporting role ('cyber-assisted crimes').

53 C. van der Meer & M. Willebrands, 'Duizenden foto's sneller doorzoeken dankzij slim algoritme' ['Thanks to a smart algoritm, it is possible to analyse thousands of pictures faster'], *Magazines Forensisch Instituut*, 27 January 2021.

54 Directive (EU) 2016/680 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, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4 May 2016.

Furthermore, the role of digital evidence in criminal cases shows it is sometimes more important to know with *whom* someone has been communicating and *where* someone has been, than to know *what* has been communicated (Henseler & De Poot, 2020). For this purpose, traffic data rather than content data needs to be gathered. Think of, for example, location data found in the metadata of photos, GPS signals, Wi-Fi and Bluetooth connections. The importance of such data can be seen in case law as well. For instance, smartphone location data play an important role in an increasing number of murder cases. As such, digital evidence not only helps to answer the question 'who did it', by finding out which user was hiding behind an e-mail address, user account or telephone number, but can also map users' activities (what), place (where) and time (when) (Henseler & De Poot, 2020).[55]

However, countries may face a range of challenges when it comes to the extension of 'traditional' search and seizure powers – which were developed with tangible objects in mind – to intangible data. For this reason, Article 19 of the Convention on Cybercrime requires contracting states to adopt the power to conduct search and seizure of stored computer data. Stored computer data are data which are already located on the device; in contrast to data which are still in transmission, and for which interception powers will need to be employed (see Section 9.5.2 to 9.5.3).

Just as in regard to production and preservation orders, the power to search and seize needs to be established and exercised in line with human rights and liberties, including those found in the ECHR. Seizing a computer and analysing the information stored on it constitutes a serious privacy interference. The ECtHR has explicitly noted that the search of a place and the seizure of computers amount to a serious interference with private life, home and correspondence.[56] Considering the gravity of the privacy interference, particularly detailed regulations with specific procedural

55 See, e.g., Court of Zeeland-West-Brabant 28 June 2016, ECLI:NL:RBZWB:2016:3865 (manslaughter in traffic) and Court Midden-Nederland 17 December 2013, ECLI:NL:RBMNE:2013:7258 (murder), where Bluetooth data from roadside sensors played an important evidentiary role in the criminal cases. See also Court of Zeeland-West-Brabant 14 February 2019, ECLI:NL:RBZWB:2019:575 on the use of data on Wi-Fi connections, and Court of Noord-Holland Court 11 July 2019, ECLI:NL:RBNNE:2019:2986 on a murder case where the suspect was located based on location data from Google's smartphone operating system.

56 See e.g., *Petri Sallinen and Others v. Finland*, *Wieser and Bicos Beteiligungen GmbH v. Austria*, *Robathin v. Austria*, *Bernh Larsen Holding AS and Others v. Norway* and *Prezhdarovi v. Bulgaria*.

safeguards will be required for this investigative method (Hirsch Ballin & Galič, 2021).[57] It is thus 'essential to have clear, detailed rules on the subject'.[58] This includes a meaningful judicial scrutiny of the search and seizure of computers, such as a warrant of an examining judge, and the limitation of the scope of the search-and-seizure operation to relevant information.[59]

Article 19 – and the Convention on Cybercrime in general – do not provide for the possibility of transborder search and seizure. Due to the connectivity of computer systems, a lot of data might not be stored on the actual computer being searched, but it may be 'readily accessible' from that computer. For instance, data might be stored in the suspect's cloud storage account, access to which might not require a password when conducted from the already accessed computer. Article 19(2) of the Convention thus allows law enforcement authorities to extend the search from the already accessed computer to connected networks, but only when these are located on its territory. This power is called a 'network search' and is discussed in Section 9.3.3 below.

9.3.3 Network computer searches

With the investigative power of a 'network search' (a type of 'remote search'), it is possible to extend an existing search into a suspect's computer to other computers (such as laptops, PCs, media players and hard discs) that are connected to an internal network (intranet) and to analyse the data on them. The network search can also be used, for example, to remotely search a company's mail server in a data centre (such as Microsoft's) during the search of an office building. Lastly, a network search may also enable law enforcement officials to remotely access accounts of suspects after their devices have been seized (see, e.g., Conings & Oerlemans, 2013; Koops Committee, 2018). For instance, the police can access the suspect's data stored in his or her cloud account, which is accessible from the computer or smartphone that has been seized.

For many years, the general strategy of law enforcement agencies has been to apprehend cybercriminals while they are logged in to their computers. The reason for this is simple: if the computer remains turned on during the search, connected networks (and therefore accounts) can be searched from

57 *Saber v. Norway*, para. 50 and *Petri Sallinen and Others v. Finland*, paras 82 and 90.
58 Ibid.
59 See *Prezhdarovi v. Bulgaria*, para. 49 and *Robathin v. Austria*, para. 48.

those computers.[60] It is likely that the search of data on an interconnected computer, such as a server in a data centre, will become increasingly important. This is so because data is increasingly stored remotely on a computer, since it is cheaper to store and process data in a data centre instead of a computer (Koops Committee, 2018).

In practice, it is sometimes impractical and undesirable to carry out a network search at the physical location, where the search takes place. Searching and the examining data carriers, which take a long time, can cause considerable inconvenience, especially in homes with many housemates (such as in student housing) or in the case of an office search. Luckily, this is not always necessary, because forensic software enables law enforcement to copy the data on connected computers and examine it later at the police station.[61]

Jurisdictional issues

However, network searches can lead to jurisdictional issues, since it is not always possible to know (at least, at the time of the search), where exactly the computer or data that are being accessed are physically located. When the territorial restriction of enforcement jurisdiction and international law are fully respected, law enforcement officials cannot gain access to computer systems on foreign territory.

This interpretation of the law severely restricts the possibilities of law enforcement for using network searches to gather evidence from interconnected computers, since many online services make use of cloud computing and distribute their storage and processing activities among data centres all over the world. Unfortunately, no treaty basis exists, which would allow states to gain transborder access to computers. The Convention on Cybercrime allows for transborder access only when the data is publicly available to anyone, or permission is obtained from the individual who has rightful access to that information (i.e. the suspect).[62]

60 See, e.g., Security.nl, 'Utrechtse student krijgt 192 dagen cel voor verkoop malware' ['192 days jailtime after selling malware by student from Utrecht'], 20 March 2020. The article tells us how a student from Utrecht University was arrested during class, while working on his laptop. The suspect surrendered his login data to the police who then searched his accounts.

61 See Court of Rotterdam 22 February 2019, ECLI:NL:RBROT:2019:2712. See also 'Rechter: OM mag inloggen in Telegram accounts van verdachten' ['Judge: Public Prosecution Office is authorised to log into Telegram accounts of suspect'], *NU.nl*, 10 April 2019.

62 See Art. 32(a)(b) of the Convention on Cybercrime.

In practice, transborder network searches are often applied unilaterally using login data acquired from the suspect in a criminal investigation by law enforcement authorities of the state the suspect resides in. Many authors have suggested that in this situation, the interference with territorial sovereignty that occurs is not severe, but that the legal certainty of the suspect is endangered (see Koops & Goodwin, 2014; Conings, 2014; Oerlemans, 2019).

9.4 The challenge of anonymity

The problem of anonymity in cybercrime investigations is well-documented (see, among others, Bernaards et al., 2012; Brenner, 2010; Oerlemans, 2017a; UNODC, 2013). Section 9.3 explained and illustrated how even in an ideal situation – where a suspect uses a fixed internet connection from home – a lot of effort is needed to gather evidence based on an IP address as a digital lead. In addition, the use of pseudonyms (nicknames) and virtual payment services also allows individuals to remain anonymous to some extent. However, many criminals make mistakes in their operational security ('opsec') by, for example, consistently using the same language, phrases or quotes that can be linked to the person. Law enforcement authorities take advantage of cyber criminals' mistakes or mutual distrust when using investigative methods (van de Sandt, 2019).

In this section we first discuss three important anonymisation techniques commonly used by cybercriminals, namely proxy-services, VPN-services and Tor (Section 9.4.1). Afterwards we discuss how open-source investigations (Section 9.4.2) and online undercover powers (Section 9.4.3) can be used to gather evidence, despite the use of these anonymisation techniques.

9.4.1 Anonymisation techniques

A proxy-service acts as an intermediate step before a computer connects to another computer via the internet, such as a web server to visit a website. Proxy-services forward the traffic to the other computer, thereby changing the IP address of the connecting computer. The public IP address used by the internet user changes to the IP address of the proxy-service server used (see also Hagy, 2007). Cybercriminals also hack computers in order to use them as a proxy-service (Bernaards et al., 2012).

With the use of VPN-services, traffic is also routed through various servers and encrypted. Encryption provides internet users with additional security against third parties who want to read the content of network traffic, for example, to steal passwords or financial data, or law enforcement authorities who want to know what is communicated. Figure 9.4 illustrates the use of proxy- and VPN-services in a home.

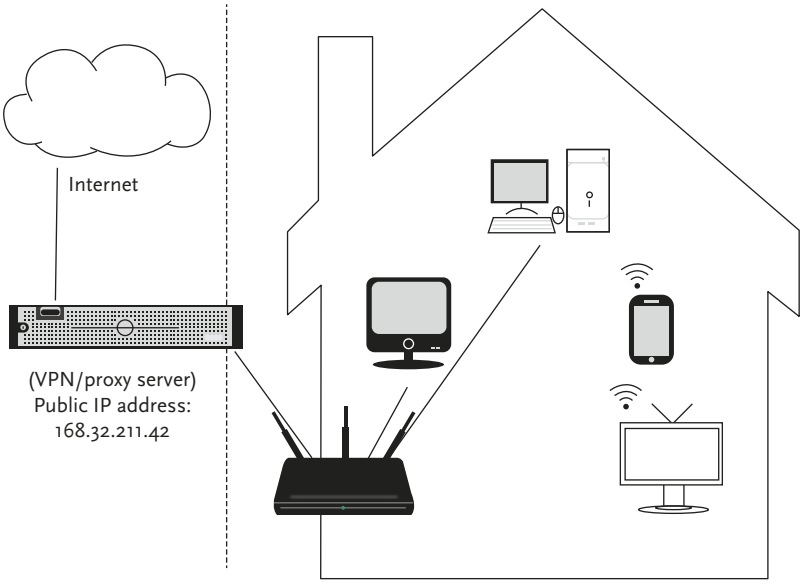

Figure 9.4 Visualisation of a proxy- and VPN-service[63]

VPN-services are commercial services. This means that individuals or organisations need to register and pay for the use of the services. VPN-services usually keep track of who connects to their services and at what time. As such, investigative authorities can demand log data (that is, traffic data) and subscriber data in order to identify a suspect (Casey, 2011; see also Section 9.3.1). However, in many cases cybercriminals will provide as little data as possible for purposes of registration or will simply provide information from a fake identity. Payment with prepaid cards or virtual money also offers a high-level of anonymity in the process of registration. This means that data acquired by data production orders will not always be useful for law enforcement agencies. In fact, the business model of some VPN-service providers is to cooperate as little as possible with requests for

63 Source: Oerlemans, 2017a, p. 39.

data from investigatory bodies. Despite the legal power to demand data, it is therefore possible that investigative bodies nevertheless remain empty-handed.

The Tor system sends internet traffic past at least three servers and encrypts network traffic (see further: Section 4.2 of Chapter 4). The intermediate Tor servers do not record any data, so that only the IP address of the last Tor server (also called 'Tor exit node' or 'Tor exit relay') is visible. Similar to a proxy- or VPN-service, this conceals the originating IP address of the internet user's network. It is therefore not possible to issue a data production order to acquire subscriber data about the users of this service, since there is no central authority in the Tor system. However, law enforcement authorities may be able to deanonymize users or Tor servers using hacking techniques (see Section 9.5.3).

9.4.2 Open-source investigations

If an investigation on the basis of an IP address fails, there may be other digital leads that investigating authorities can follow. In particular, there may be digital traces left behind by persons using the internet, which can be collected by gathering publicly available data on the internet.

Just like other persons, cybercriminals are active on social media. When this is the case, investigating officers can follow the 'digital breadcrumbs' of people's identities on the internet to find out more about the suspect, the victim and the suspect's environment, or to gather more information about the criminal offence itself. The collection of data from open sources is also called 'open-source intelligence' (OSINT) (Akhgar et al., 2017). 'Open-source information' can be defined as 'information that anyone can lawfully obtain by request, purchase, or observation, for instance information that is publicly available online'.[64] Most cybercriminals strictly separate their real identity from their criminal identity by employing a nickname. However, many criminals make mistakes in their *operational security* ('opsec') for instance, by using the same language, expressions or quotes that can be used to link their criminal to their official identity. It can also happen that cybercriminals betray each other by publishing personal data about one another ('doxing'). Investigating authorities can thus make use of cybercriminals' mistakes or mutual distrust when applying investigative methods (van de Sandt, 2019).

64 See the National Open Source Enterprise, Intelligence Community Directive 301, July 2006 for this definition.

In open-source intelligence techniques, a distinction can be made between 'manual collection' and 'automated collection' of data (Oerlemans & Koops, 2012). Manual collection of publicly available online data involves collecting data that are available, when search terms are entered into search engines such as Google. Other examples include searches in online telephone directories, online discussion forums and publicly available information on social media services, even when registration is required. While these searches might sound too basic to be fruitful, entering nicknames of suspected hackers in Google has actually led to the identification of suspects in cybercrime cases.[65] Similarly, the e-mail address of the notorious online drug baron Ross Ulbricht, which was found in an advertisement of the notorious darknet market 'Silk Road', provided an important lead for the FBI at the time.[66]

Open-source intelligence can also be (partly) automated by using software. Commercial tools such as 'SpiderFoot' and 'Maltego', enable law enforcement authorities to enter a search term and automatically collect data from many different (open) data sources at once and then visualise the data. In addition, software called 'crawlers' and 'scrapers' automatically collect all available information based on certain parameters, such as a particular website, the name of the suspect or criminal organisation, a certain weapon, certain drugs sold on the internet or the metadata of a certain image.[67] An investigator can retrieve all available information that the program has collected through a type of search program. By doing so, connections or links between the information can be made. For example, a person who uses different nicknames but always uses the same encryption key to send messages (such as PGP keys on darknet markets) or uses the same bitcoin address to transfer money (Oerlemans & van Wegberg, 2019). Despite the presumed widespread use of open-source research as an investigative method by law enforcement authorities, journalists and NGOs (such as 'Bellingcat'), there is hardly any case law available on the subject.

Collecting private (or personal) data from open sources interferes with the right to private life and the right to protection of personal data (two

65 See e.g., G. Cutlack, 'Police caught an anonymous hacker by googling his IRC name', *Gizmodo*, 12 December 2012.

66 See K. Zetter, 'How the feds took down the silk road drug wonderland', *Wired*, 18 November 2015.

67 A crawler indexes information, such as URLs. Scrapers also download and store data, such as the content of web pages.

closely connected but distinct human rights) (e.g., Edwards & Urquhart, 2016). For this reason, many states have detailed regulations concerning the legal grounds that are necessary for the processing of personal data by law enforcement authorities.[68] For example, in the case of *Segerstedt-Wiberg*, the ECtHR decided that the storage of public information (a photo in a newspaper) in the police register of the Swedish police indeed constituted interference in the private lives of the individuals involved. The ECtHR emphasised that the fact that the data was public did not negate the interference, since the information had been systematically collected and stored in files held by the authorities.[69] The gravity of such interference is generally considered relatively low, because people can be said to have a lower 'expectation of privacy of the data' that is publicly available.[70] Nevertheless, the ECtHR has oftentimes found a violation of the right to private life in such cases, confirming that even minor privacy intrusions require a legal basis, which indicates with sufficient clarity the scope and manner of exercising the power (Galič, 2019).[71] In the Netherlands, the Dutch oversight body on intelligence and security services cautioned that open-source research has evolved beyond merely 'looking up' phone books or conducting internet searches with search engines. With the advent of 'automated OSINT', hundreds of sources from various origins can be accessed simultaneously, including commercially available location data, data from advertisements and data from leaked datasets. This entails a more serious privacy breach than previously envisioned by lawmakers.[72] And yet, open-source investigations are usually conducted by law enforcement officials without clear or stringent

68 On the European Union level this is regulated in the Law Enforcement Directive (EU) 2016/680 of 27 April 2016.

69 ECtHR 6 June 2006, ECLI:CE:ECHR:2006:0606JUD006233200, appl. no. 62332/00, para. 72 (*Segerstedt-Wiberg and others v. Sweden*). See also *Rotaru v. Romania*, para. 43.

70 See by analogy case law on CCTV-footage; *P.G. and J.H. v. the United Kingdom*, para. 57 and ECtHR 17 July 2003, ECLI:CE:ECHR:2003:0717JUD006373700, appl. no. 63737/00, para. 38 (*Perry v. The United Kingdom*).

71 See, e.g., ECtHR 8 February 2018, ECLI:CE:ECHR:2018:0208JUD003144612, appl. no. 31446/12 (*Ben Faiza v. France*), ECtHR 28 January 2003, ECLI:CE:ECHR:2003:0128JUD004464798, appl. no. 44647/98 (*Peck v. the United Kingdom*), ECtHR 16 February 2000, ECLI:CE:ECHR:2000:0216JUD002779895, appl. no. 27798/95 (*Amann v. Switzerland*); ECtHR 18 October 2016, ECLI:CE:ECHR:2016:1018JUD006183810, appl. no. 61838/10 (*Vukota-Bojić v. Switzerland*) and *Rotaru v. Romania*.

72 Review Committee on the Intelligence and Security Services, 'Automated OSINT: tools and sources for open source investigation', CTIVD report no. 74 (2022). See also T. Wetzling & C. Dietrich, 'Disproportionate use of commercially and publicly

regulation in criminal procedure law (although data protection regulations do apply) (Lodder et al., 2015).

The Convention on Cybercrime explicitly provides for a treaty basis for the cross-border unilateral application of open-source investigations. The treaty basis is provided in Article 32(a) of the convention, which reads as follows:

> 'A party may, without the authorisation of another Party: (a) access publicly available (open source) stored computer data, regardless of where the data is located geographically.'

Contracting parties thus agree that cross-border unilateral access to publicly available data – which is technically stored in computers that may be located on foreign territory – is permitted, without the need for legal assistance to acquire the evidence.[73] In other words, states that have ratified this convention agree that such evidence-gathering activity does not interfere with their territorial sovereignty (see Koops, 2013b). It can also be argued that cross-border unilateral collection of publicly available online data that is stored in a computer located on the territory of a foreign state that has *not* ratified the Convention is not allowed without permission and may violate the territorial sovereignty of the affected state. Yet, this approach would ignore the fact that cross-border unilateral gathering of publicly available online information has been tacitly tolerated by states for almost two decades (see Seitz, 2005, p. 38). Under this assumption, Article 32(a) of the Convention on Cybercrime should be viewed as a codification of an existing practice.[74]

9.4.3 *Online undercover operations*

Online undercover operations offer valuable possibilities for law enforcement authorities. The internet is not only a boundless medium for criminals to conduct criminal activities with (relative) anonymity; it also offers opportunities for law enforcement to fight crime. Investigating officers can communicate just as anonymously as others on the internet, without running any (immediate) physical risk and without having to leave their office (Oerlemans, 2018).

---

available data: Europe's next frontier for intelligence reform?', *Stiftung der Neue Verantwortung*, November 2022.

73 See Explanatory Report to the Convention on Cybercrime (2001), para. 293.

74 See also the report by the Ad-hoc Subgroup on Transborder Access and Jurisdiction of the Convention on Cybercrime 2013, p. 10.

For example, law enforcement officials can buy an illegal good or service from an online marketplace in order to gather evidence in a criminal investigation. Investigating authorities can then check who is sending the package containing the goods or data. If the suspect does the shipping himself, they may be unwittingly disclosing identifying data. For instance, a package containing drugs may contain fingerprints or DNA material (e.g., by licking a stamp) on the basis of which further investigations may take place. The purchase of goods or data via the internet is sometimes preceded by online communication. During this communication, it may be possible to obtain identifying data from a suspect, such as a name, telephone number and/or e-mail address. These data, in turn, provide opportunities for further investigative activities, such as requesting data from ISPs.

However, when a suspect offers illegal goods or data on the internet and an investigating officer subsequently buys the offered goods or data, this might be regarded as incitement (also called 'entrapment') – that is, luring a person to commit a crime that they would have otherwise been unlikely or unwilling to commit. Investigatory activities in undercover operations must therefore be carefully recorded so that it can be verified during trial that there has been no incitement and that the right to a fair trial in Article 6 ECHR has not been violated.[75] When determining whether law enforcement authorities interfered in the investigation in an active manner that led the suspect to commit the offence, the ECtHR takes into consideration four factors: (1) the reasons underlying the undercover operation; (2) the behaviour of the law enforcement authorities; (3) the existence of a reasonable suspicion that the suspect was involved in criminal behaviours; and (4) the predisposition to the crime of a suspect (Ölçer, 2014).[76]

The internet also allows law enforcement authorities to interact with suspects and those around them while using an undercover identity. These interactions can take place on chat channels, online discussion or trade forums, or by becoming 'friends' with the suspect or his friends on social media and then communicating with them. It is also possible that an officer

75 In the case of *Teixeira de Castro v. Portugal*, the ECtHR held that the right to a fair trial would be violated when law enforcement officials 'do not confine themselves to investigating criminal activity in an essentially passive manner, but exercise an influence such as to incite the commission of the offense' (ECtHR 9 June 1998, ECLI:CE:ECHR:1998:0609JUD002582994, no. 44/1997/828/1034, para. 38 (*Teixeira de Castro v. Portugal*)).

76 See also ECtHR 4 November 2010, ECLI:CE:ECHR:2010:1104JUD001875706, appl. no. 18757/06, *EHRC* 2011/9 (*Bannikova v. Russia*).

takes over another person's account and then communicates with the suspect under someone else's identity (e.g., an acquaintance of the suspect).

Such undercover interactions have a significant limitation: an investigating officer can usually only interact with one suspect at a time. This poses the question: what does this mean for crimes, such as CSAM and webcam child sex tourism? It is said that every day, hundreds of thousands of men around the world surf the internet, seeking for boys and girls to engage in webcam sex.[77] For this reason, law enforcement authorities in cooperation with private actors have begun to develop automated chatbots to interact with suspects online. These chatbots are no longer operated by a human, but by a fully or partially autonomous artificial intelligence that can engage in meaningful conversations with suspects. Unlike human operators, the use of such technology is in theory infinitely scalable. An illustrative example of such a development can be seen in the case of Sweetie.

Case study: Sweetie

Webcam child sex tourism is a rapidly growing new form of online child sexual exploitation. In this case, men from wealthier parts of the world pay money to children in developing countries, such as the Philippines, to perform sexually explicit acts in front of a webcam.

In 2013, the Dutch children's rights organisation Terre des Hommes launched the Sweetie project.[78] Sweetie is a virtual ten-year-old Filipino girl (i.e., an avatar) with a very lifelike appearance, which is used to identify and expose offenders in chatrooms and online forums. The Sweetie avatar was initially operated by an agent of the organisation, whose goal was to gather information on individuals who contacted Sweetie and solicited webcam sex from her. In order to avoid incitement, the operators would wait for individuals to initiate a conversation with Sweetie in a sexually suggestive way. Researchers were able to identify the individuals communicating with Sweetie, using only the information voluntarily provided to the avatar and by gathering publicly available information on the internet, such as Facebook or Yahoo accounts (Guyt, 2019). The gathered information

77 See Terre des Hommes, 'Sweetie, our weapon against child webcam sex'.
78 Ibid.

was subsequently handed over to the authorities, who could then launch investigations in their respective country. The Sweetie project has led to several arrests and convictions in countries such as Australia, Belgium, Denmark, the Netherlands, Poland, and the UK (Schermer et al., 2019).

However, existing criminal laws in many countries have trouble coping with these new investigative possibilities. One notable limitation of the Sweetie project is the question whether undercover investigations can be performed by non-human agents, such as chatbots. At the moment, a human being seems to be a necessary element of undercover investigations in many criminal procedure codes around the world (Açar, 2017). For this reason, some countries, such as the Netherlands, have already amended their criminal procedure codes to allow for the gathering of evidence in undercover operations by chatbots and other technologies (Oerlemans, 2017b).

One step further is to *infiltrate* a criminal organisation in order to gather evidence, which happened in the so-called 'Hansa operation' in 2017.

Case study: the Hansa operation

The Hansa operation is an excellent example of infiltration as an investigative power in a digital context. At the beginning of 2017, Hansa Market was a popular darknet market, focussed mainly on drug sales. The largest and most popular darknet market, however, was 'AlphaBay'. AlphaBay offered not only drugs, but also other illegal goods, such as firearms.[79] At one point, AlphaBay was ten times the size of the notorious 'Silk Road' darknet market. At the beginning of 2017, however, U.S. law enforcement authorities made AlphaBay inaccessible. U.S. authorities did not hold an extensive press conference after the 'take down' of AlphaBay. Instead, they intentionally left the darknet market users confused as to what had happened. The idea was that many

79 See FBI press release, 'Darknet Takedown. Authorities Shutter Online Criminal Market AlphaBay', 20 July 2017.

buyers and sellers would simply move from AlphaBay to the Hansa Market.

This enabled the Dutch High Tech Crime Team to launch 'Operation Bayonet' in coordination with Europol. As expected, many buyers and sellers indeed moved to the other popular darknet market: the Hansa Market. Such migration of users to other markets or services is known as the *waterbed effect* (van Wegberg & Verburgh, 2018). The number of visitors to the Hansa Market increased from 1,000 to 8,000 per day.[80]

The Dutch police gained and then maintained control of Hansa Market for about a month. To achieve this, the contents of the Hansa Market servers were copied and transferred from Lithuania to a data centre in the Netherlands. Acting as 'administrators' of the market, the Dutch police essentially ran the drug market under the direction of the public prosecution and in cooperation with foreign investigation agencies. During this takeover, more than 27,000 transactions in total took place and a wealth of information was collected, including identifying information of 20,000 users and 10,000 home addresses. This data was provided to Europol, which further distributed it to investigating authorities in other countries. Communications between the darknet staff and customers were also mapped. This information may provide incriminating evidence for further prosecution.[81]

Besides taking down another darknet market, the operation had the secondary aim of disrupting cyber-enabled crime. The operation namely made it clear to darknet market users that they were not anonymous and that the police can and does track their criminal activities on such markets. Well-known Dutch vendors were also named and shamed by the Dutch police (see Figure 9.5).

80 See also press release Public Prosecutor's Office, 'Ondergrondse Hansa Market overgenomen en neergehaald' ['Underground Hansa Market taken over and taken down'], 20 July 2017.

81 See, e.g., A. Greenberg, 'Operation bayonet: Inside the sting that hijacked an entire dark web drug market', *Wired*, 3 August 2018.

Figure 9.5 Screenshot shown during Hansa operation

As a result of the Hansa operation, many offenders had to say goodbye to their longstanding nickname. Such nicknames are of high value, since they are used to build up a certain reputation. Similarly, as with regular marketplaces, buyers prefer to buy from an established and well-reviewed seller, who can be recognised by their nickname. After the Bayonet operation, criminals had to start from scratch, which can be seen as a disruptive effect (van Wegberg and Verburgh, 2018)

In the Netherlands, on 3 July 2019, one of the sellers on the Hansa Market was sentenced to five years imprisonment by the Court of Rotterdam for laundering bitcoins worth more than €800,000 and for delivering more than 22,000 drug orders together with others.[82] In this judgment, the Rotterdam court considered whether a situation of incitement had occurred. The court employed the usual test of whether the sellers and buyers had been lured by the investigation team to commit offences other than those that they had already intended to commit. It decided that the admission of new sellers and the offering of a discount to persons who already had the intention to trade in narcotics on this hidden website were part of normal operations of a

82 The drugs were hidden in special 3D-printed packages such as make-up boxes. Two co-defendants were also convicted, see Court of Rotterdam 4 July 2019, ECLI:NL:RBROT:2019:6049 and ECLI:NL:RBROT:2019:6050.

darknet market. As such, the court concluded that the takeover of the Hansa Market by the Dutch police cannot be qualified as incitement.[83]

From an international law perspective, questions arise whether extraterritorial online undercover operations can be applied unilaterally. Different investigative methods may interfere with state sovereignty with different levels of severity. For instance, when online pseudo-purchases and online infiltration operations are applied, undercover agents commit authorised crimes. These investigative methods may be regarded as a violation of the affected state's territorial sovereignty, when no permission is provided by the affected state to conduct the (often minor) crime on its territory (see O'Floinn & Ormerod, 2011).

At the beginning of an online investigation, it may be impossible to ask a state for permission. For example, when an operation is conducted on the darkweb, it is not clear *where* an online undercover operation takes place, so that it is unclear which states should be asked for permission. Online interactions with individuals may be regarded as less intrusive investigative methods, since they only involve law enforcement officers interacting with individuals in an undercover capacity. States may find this type of online undercover operations (in which the officer does not commit any authorised crimes), which are undertaken on their territory without their permission, as more acceptable. However, the individuals involved may regard these online interactions as more privacy intrusive than, for example, online pseudo-purchases by law enforcement officers (Oerlemans, 2017a).

Case study: David Schrooten alias 'Fortezza'

The case of David Schrooten is an illustrative example of the various legal problems that arise when foreign law enforcement authorities conduct an online undercover operation on foreign territory. In 2012, the U.S. Secret Service suspected David Schrooten, a Dutch national, of credit card fraud that involved U.S. victims (Schrooten & Vuijst, 2016).

83 See also Court of Rotterdam 3 July 2019, ECLI:NL:RBROT:2019:5339, *Computerrecht* 2019/178, with annotation by J.J. Oerlemans.

According to Schrooten's defence counsel, the U.S. Secret Service had assumed the online identity of a suspect who had been apprehended in the United States and had subsequently used his online account to interact with David (who was in the Netherlands) in an undercover capacity via the internet. This example aptly illustrates that the power of law enforcement officials to take over a person's online identity is a unique and valuable feature of online undercover operations.

U.S. Secret Service agents then purchased credit card numbers from Schrooten, who used the nickname 'Fortezza' on the internet. Under Dutch law, this activity requires the use of a special investigative power or permission of the Dutch state. In the United States, however, undercover operations such as this one do not require special investigative powers. Instead, they are regulated in guidelines and do not require authorisation of a public prosecutor or a judge. In this case, U.S. law enforcement officials then maintained contact with Schrooten. At one point in the investigation, the suspect flew to Romania to visit his girlfriend. When he arrived there, Schrooten was arrested at the airport by Romanian authorities and extradited to the United States. Schrooten was subsequently incarcerated in a U.S. prison for twelve years after a plea bargain agreement with a U.S. public prosecutor.[84] He eventually returned to the Netherlands to serve the remainder of his sentence in a Dutch prison.[85] The conversion of his sentence to the (much lower) Dutch sentence for the crimes committed meant that he was released soon after his return to the Netherlands.

This case led to controversy in the Netherlands, partially due to Schrooten's bad living conditions in the U.S. prison and the manner in which U.S. law enforcement officials obtained custody of him. The question also arose, whether U.S. law enforcement officials had engaged in evidence-gathering activities on Dutch territory and lured David into committing the crimes in order to prosecute him, thereby infringing upon Dutch sovereignty. In response to parliamentary questions, the Dutch Minister of Security and Justice explained that the

84 See H. Lensink & F. Vuijst, 'Geen krediet voor David S.' ['No lenience for David S.'], *Vrij Nederland*, 15 April 2013.

85 See H. Lensink, 'Minister wil terugkeer hacker David S. bespoedigen' ['Minister of Justice seeks to speed up return of David S.'], *Vrij Nederland*, 15 April 2013.

Netherlands was aware of U.S. law enforcement authorities' interest in David at the time, but not of any investigative activities that these authorities were undertaken on Dutch territory.[86]

Of course, it is possible that U.S. law enforcement officials were not aware of David's identity and location at the time the undercover investigation took place. His nickname, 'Fortezza', in itself did not indicate where he was located. Following their online undercover interactions with the suspect, U.S. law enforcement authorities might have simply decided to seize the opportunity and request Romania to extradite him once it became clear that he would land at a Romanian airport. However, it is also plausible that U.S. law enforcement officials already knew Schrooten's identity and could have requested the Netherlands to prosecute or extradite him. Schrooten himself argued that U.S. law enforcement authorities were aware of his location and identity. He claimed that the Secret Service knew his location from subscriber data that it obtained from online service providers and derived his identity from financial transactions that he conducted with the Western Union money transmitting service (Schrooten & Vuijst, 2016). It also appears that Russian hackers had previously exposed his identity in online forums, information which may also have noticed by U.S. law enforcement authorities.[87]

Regardless of which of these two versions of the extraterritorial evidence-gathering activities is true, the case of David Schrooten illustrates how online undercover investigative methods are used in practice and may lead to issues with regard to both the territorial sovereignty of states and the legal certainty of the individual involved. The case shows how U.S. law enforcement officials actually conducted an online undercover operation that involved a Dutch citizen without either requesting prior permission from the Netherlands to conduct the operation or having authorisation derived

86 See answers to the parliamentary questions of parliamentary member van Bommel by the State Secretary of Security and Justice regarding the extradition by Romania of Dutch hacker David S. to the United States on 1 August 2012.

87 See B. Krebs, 'Feds arrest "kurupt" carding kingpin?', KrebsonSecurity blog, 12 June 2012.

from a treaty.[88] This also means that U.S. laws were applied. U.S. laws for undercover investigative methods are not accessible, nor foreseeable for Dutch citizens. Therefore, such practices endanger the legal certainty of the individuals involved. This case also shows how the cross-border unilateral application of online undercover investigative methods can lead to political tensions between states.

It should be noted that there are no legal assistance treaties specifically regulating online undercover operations. At the time of writing, there are also no proposals or public plans to regulate online undercover operations within the EU. Therefore, we suspect that in the future, unilateral online operations will continue to take place in practice and create tension among states.

9.5 The challenge of encryption

In order to prevent unauthorised persons from gaining knowledge of information, encryption is essential. For this purpose, cryptography can be used. Cryptography makes data unreadable by means of a mathematical algorithm.[89] With the use of a decryption key, data can be made readable again. As such, cryptography is an essential technique for confidential communication with others (Arnbak, 2015). To some extent, encryption is already a part of the devices that we use every day.[90] For example, mobile phones and laptops employ standard encryption to store information securely ('encryption by default') and many websites nowadays enable the SSL-protocol, which makes visiting websites more secure (visible as 'https://' instead of 'http://').

Yet, the use of cryptography also has a downside. It creates problems for law enforcement both for the interception of telecommunications ('data in transit') as well as for the analysis of stored data on computers ('data in storage'). Since the early 1990s, law enforcement agencies have expressed the expectation that the use of cryptography by criminals (i.e. 'going dark') will render law enforcement ineffective. For this reason, law enforcement has been trying to limit the public's access to cryptography ever since the 1990s, what has been called the 'cryptowars' (Jarvis, 2020). During the first

88 This may again be explained by the argument that U.S. law enforcement officials were not aware of David's identity and location.

89 In other words, the data is converted into 'cipher text'.

90 The data is converted to 'plain text'.

cryptowar in the mid-1990s, law enforcement authorities proposed measures such as requiring a licence for the use of cryptography and making the crypto keys available to the government ('key escrow') for the benefit of national security and investigation (Koops, 1999). Variants of these proposals have been implemented in a few countries, but did not gain global traction (Koops & Oerlemans, 2019).

In the meantime, encryption has become a commonplace occurrence in investigations. This is due in large part to encrypted mobile phones, which are seized in investigative investigations. Contemporary mobile phones almost always have some form of encryption on them, such as a password, pin code, fingerprint- or 'Face ID'-technology. Other forms of encryption faced by investigators include encrypted chat services, other encrypted devices (e.g., laptops and PC's), encrypted e-mail services and cryptophones. According to a recent study of the problem of encryption faced by Dutch law enforcement agencies, encryption is most often encountered in organised (drug) crime, cybercrime and CSAM investigations (Jansen et al., 2023).

Since 2014, representatives of law enforcement authorities have again begun arguing for a legal obligation to give enforcement agencies access to unencrypted information. This prompted the so-called *second* – and on-going – cryptowar. This cryptowar is characterised by the fact that governments generally no longer call for the abolition or prohibition of certain type of cryptography. Instead, the idea is that a 'back door' should be built into systems in some way or another, in order to enable law enforcement to reverse the encryption of data. An important objection to this idea is that this would make the IT infrastructure inherently insecure, because actors other than well-intentioned democratic government bodies could abuse such backdoors. Think of spies by foreign governments ('state actors') or technically savvy criminals (Bellovin et al., 2013). For the time being, electronic communication service providers (particularly in the United States), such as Facebook and Apple, are not obliged to decrypt communication traffic for investigating authorities. Nevertheless, as end-to-end encrypted communications through WhatsApp, Telegram and other over-the-top-services (OTTs) continue to diminish the value of interception of communications, many European states are still fostering the idea of introducing obligatory backdoors in their legislation.[91]

91 See also the 'Going dark' initiative of the Swedish Presidency of the Council, which in 2023 proposed to create a High-Level Expert group on data retention to strike a new 'balance between the right to privacy and the right to security', including a discussion

These ideas will now have to overcome the serious limitation of the recent ECtHR judgment in *Podchasov v. Russia* (2024). In this case, Russian authorities ordered Telegram to decrypt their communications protected by end-to-end encryption.[92] The ECtHR ruled that a statutory requirement to decrypt end-to-end encrypted (E2EE) communications is not proportional to the legitimate aims of fighting crime and protecting national security and is therefore in violation of Article 8 ECHR. Two considerations led the Court to this conclusion. First, the Court highlighted that enabling decryption of E2EE communications for specific individuals necessitates creating a backdoor, which would be accessible not only to law enforcement but also to malicious actors, therefore weakening the security of communications for all users. It would also make it technically possible to perform routine, general and indiscriminate surveillance of personal electronic communications.[93] Second, referring among others to a joint statement by Europol and the European Agency for Cybersecurity, the Court pointed out that there exist encryption-preserving alternatives to access encrypted communications, such as undercover (infiltration) operations and police hacking.[94]

In the following section we will briefly discuss two types of encryption: (1) encryption in storage and (2) encryption in transit. We will also discuss investigative methods that can be used to gather evidence in criminal investigations, despite the challenges encryption poses to criminal investigations.

9.5.1 *Encryption in storage*

The power to seize a device (such as an iPhone) generally also includes the power to access (i.e., to search) stored data and – as far as possible – to reverse its security.[95] However, encryption of data can thwart such attempts. Data encryption in storage can namely encrypt the whole device, a hard disc, or individual files. Not only is free encryption software available online, it is also a standard option on mobile phones, laptops, hard drives and USB sticks. This type of default encryption is very strong, and investigative authorities

on backdoors. See Statewatch.org, '"Going dark": will the next assault on privacy take place behind closed doors?', 19 April 2023.

92 ECtHR 13 February 2024, appl. no. 33696/19, ECLI:CE:ECHR:2024:0213JUD 003369619 (*Podchasov v. Russia*).

93 Ibid, para. 77.

94 Ibid., paras 78 and 33.

95 See also *Parliamentary Papers II* 2015/16, 34372, no. 3, pp. 7-8.

reportedly have great difficulty in 'cracking' the files, that is, making the content stored on computers readable again (Europol, 2015a; Mevis et al., 2016).

It is important to note that law enforcement authorities are sometimes nevertheless able to decrypt the data, either because the suspect has written down the passwords (and law enforcement manages to find them), they provide the unencrypted data voluntarily, or the suspect uses biometric security which law enforcement authorities can 'crack' (e.g. placing a thumb on an iPhone to unlock it). In some cases, it is also possible to demand a backup copy of a phone or hard disc from a company.[96] However, in practice, it is not always possible to acquire the necessary data, particularly if the company is located abroad. In that case, requests for legal assistance are necessary, which can lead to considerable delays. Without a legal assistance treaty, it is also possible that investigative authorities will be left empty-handed, if the company decides not to cooperate (see Section 9.2.2).

Decryption order

The question whether suspects can be forced to hand over their decryption keys is a continuing debate. In fact, paragraph 4 of Article 19 of the Convention on Cybercrime includes the power to compel a person to submit a password in order to access the computer system or to decrypt content. In practice, this provision is most often directed at system administrators of ICT networks. In fact, reference to the safeguards of the rule of law in paragraph 5 of the provision implies that this order cannot be directed at the suspect itself, as this could violate the privilege against self-incrimination ('nemo tenetur'). The privilege against self-incrimination guards against unwarranted compulsion by authorities and the obtaining of evidence through methods of coercion or oppression in defiance of the will of the accused.[97] The privilege against self-incrimination is thus closely connected to the right to remain silent and the freedom of explanation, fundamental rights which are derived from the right to a fair trial in Article 6 ECHR (van Toor, 2019).

This is connected to the fact that when the suspect is ordered to hand over a password or a pin code, they need to make a 'mental effort'. While passwords and pin codes exist independently of the will of the suspect, they generally

96 See also P. Rosenzweig, 'iPhones, the FBI, and going dark', *Lawfareblog.com*, 4 August 2015.

97 ECtHR 5 November 2002, ECLI:CE:ECHR:2002:1105JUD004853999, appl. no. 48539/99, para. 51 (*Allan v. the United Kingdom*).

cannot be obtained independently of the will of the suspect (unlike physical evidence). In other words, obtaining passwords or codes depends on the willingness and capability of the suspect to first remember them and then hand them over to the investigating officers. As such, ordering the suspect to 'hand over' such material might interfere with the freedom of the suspected person to choose whether to speak or to remain silent when questioned by the police. Such a legal obligation might thus be at odds with the right against self-incrimination. Nevertheless, this privilege is not an absolute right; depending on the public interest at stake, the existence of effective procedural safeguards and the nature and degree of compulsion, interference may be justified (Hildebrandt, 2020).[98]

On the contrary, the forced provision of a fingerprint to unlock a smartphone is often permitted, insofar as it meets the proportionality and subsidiarity principle.[99] The reason why this form of forced decryption is allowed is that a fingerprint (just like the unlocking via a facial scan) is biometric data existing independently of the will of the suspect, which does not require any mental effort to undo the encryption.

9.5.2 Encryption in transit

In the case of interception of communications (also called 'wiretapping'), the encryption of data again renders the content unreadable for law enforcement authorities. In the past ten years, this has mainly proved a problem with regard to the sending of private messages through popular apps, such as WhatsApp (Bellovin et al., 2013).

Using the special investigative power of wiretapping, law enforcement agencies can intercept data and then read or eavesdrop on them. Given the serious breach of privacy that this incurs, this power usually requires an order from a public prosecutor and a warrant from an examining judge.[100] In a standard situation, a provider of public telecommunication services must a wiretap. These providers are often legally obligated to cooperate

98 See ECtHR 11 July 2006, ECLI:CE:ECHR:2006:0711JUD005481000, appl. no. 54810/00 (*Jalloh v. Germany*).

99 See, e.g., Dutch Supreme Court 9 February 2021, ECLI:NL:HR:2021:202, *Computerrecht* 2021/63, with annotation by D.A.G. van Toor & T. Beekhuis (*Decryption order*).

100 See ECtHR 4 December 2015, ECLI:CE:ECHR:2015:1204JUD004714306, appl. no. 47143/06, para. 257-267 (*Roman Zakharov/Russia*).

with a wiretap order and to set up a wiretap infrastructure for that purpose. A wiretap is placed on a specific telephone number (or other identifying number of a telephone, such as an IMEI number). The entire conversation is then recorded, including traffic data (e.g. location data), and sent to the police. The situation is different with apps commonly used for communication over the internet, such as WhatsApp, which are referred to as Over The Top (OTT) services. These are not (at least, as of yet) regarded as providers of public telecommunications networks or services that must facilitate wiretapping. These (mostly U.S.) services are therefore not obligated to cooperate with a wiretap order, leaving law enforcement authorities unable to eavesdrop conversations over these OTT services in criminal investigations.

Note that, despite the problem of encryption, wiretapping telecommunications data can still provide useful information to investigating authorities. Although the content of the data cannot be read, various types of traffic data can still be analysed, such as which number (was) called at which time and from which location (Oerlemans, 2012).

9.5.3 Hacking as an investigative method

The use of hacking as an investigative method enables law enforcement authorities to covertly and remotely gain access to a computer used by a suspect. By breaking in 'at the source', investigators can intercept and read out communications before the encryption is activated (e.g., logging keystrokes of the message as it is being written), or after it has been reversed.

After access is acquired, law enforcement authorities can use different functionalities of hacking software to gather evidence. For example, keystrokes can be recorded to acquire login names, passwords, URLs and the content of messages. It is also possible to turn on a microphone in order to eavesdrop and record a conversation. Just like the malware used by cybercriminals, hacking software used by law enforcement enables them to take screenshots (to see what is on a suspect's computer), activate a camera (to identify the user of the computer) and activate GPS functionality (to locate the device).

Hacking as an investigative method is deemed controversial in many countries, including the Netherlands where the method is already in use and regulated as an investigative power. There are several reasons for this, and we will discuss two key reasons in the following text.

The first question that arises is whether hacking powers can be regarded as proportionate, particularly since hacking leads to a severe interference with privacy. Hacking breaches the confidentiality, integrity and availability of data on computers. After access is gained, other investigative powers can be applied, such as wiretapping, searching and copying information and even making data inaccessible (see Škorvánek et al., 2019). In addition, the hacking power need not be limited to the suspect's laptops, PCs and smartphones. In the Netherlands, for instance, the investigative authorities can hack any computer that is 'used by the suspect', which can include computers by friends and family. Furthermore, the power can also be used to penetrate all automated works in many different types of criminal investigations. Devices such as smart meters, lamps, pacemakers and smart cars can also be hacked.[101] Recent law enforcement operations have shown that law enforcement authorities nowadays engage in large scale hacking and interception. In the EncroChat and SkyECC operations, law enforcement authorities intercepted approximately 120 million and 500 million messages in France (Oerlemans & Royer, 2023; Oerlemans & van Toor, 2022). It is expected that the ECtHR will find such large-scale hacking and interception permissible only when 'end-to-end safeguards' are in place, including a warrant to exercise the investigation power, the application of data protection principles in the collection and analysis phase, as well as independent and effective oversight (Fedorova et al., 2022; Galič, 2022, Oerlemans & Royer, 2023).[102]

The second point of criticism focusses on the use of vulnerabilities in the application of the power. The idea is that exploiting (previously) unknown vulnerabilities (so-called 'zero days') through hacking creates more insecurity rather than security for society. The reasoning behind this is that investigating authorities have an interest in preserving unknown vulnerabilities in devices so that they can keep on exploiting them. Since these vulnerabilities are not known to the manufacturer of the hardware or software, the security problem is not solved and the devices remain insecure. These unknown vulnerabilities can therefore also be exploited by malicious parties until the security problem

101 In the Netherlands, the legislative history indicates that hacking into a pacemaker or car is, in principle, deemed disproportionate, because of the great risks to the safety of individuals that occur when hacking into these devices. See *Parliamentary Papers II* 2016/17, 34372, no. 6, p. 32 and p. 53.

102 Similar to the minimum safeguards required for bulk interception by intelligence and security services as explained in ECtHR 25 May 2021, appl. nos. 58170/13, 62322/14 and 24960/15), ECLI:CE:ECHR:2021:0525JUD005817013, para 330 (*Big Brother Watch/The United Kingdom*).

is resolved. In the Netherlands, the police have an obligation to report unknown vulnerabilities, which they have become aware of in the course of applying the hacking power.[103] Only in the event of a 'compelling investigative interest' and after an approval from a public prosecutor, may an investigatory judge postpone the reporting of the unknown vulnerability (Koops & Oerlemans, 2019). In practice, notification of unknown vulnerabilities by law enforcement authorities almost never takes place. Reports also show that Dutch law enforcement authorities almost exclusively use commercially available hacking tools and mostly targeting mobile phones in serious crime (that is, not cybercrime investigations) (van Uden et al., 2022).

Following incidents within the European Union, in which commercial spyware was (illegally) used to spy on fellow politicians and journalists, the European Parliament urged EU Member States to respect ECtHR judgments and restore judicial independence and oversight bodies.[104] They also argued that spyware should only be used in Member States where allegations of spyware abuse have been thoroughly investigated and where export control rules have been enforced. The European Parliament also wants EU rules on the use of spyware by law enforcement, which should only be authorised in exceptional cases for a pre-defined purpose and a limited time. Furthermore, they argue that data falling under lawyer-client privilege or belonging to politicians, doctors or the media should be shielded from surveillance, unless there is evidence of criminal activity. Lastly, they propose mandatory notifications for targeted people and for non-targeted people whose data were accessed as part of someone else's surveillance, independent oversight after it has happened, and a common legal definition of the use of national security as grounds for surveillance.[105] So far, these recommendations by the European Parliament on spyware have not been proposed by the European Commission.

Clearly, hacking as an investigative method is also applied to circumvent the challenge of anonymity in cybercrime investigations. Similar to dealing with the problem of encryption, law enforcement can de-anonymise computer

103 *Parliamentary Papers II* 2016/17, 30372, no. 14.

104 European Parliament recommendation of 15 June 2023 to the Council and the Commission following the investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware.

105 Ibid.

users by gaining access to the source of the device they are using. The following case study provides a good example for this.

Case study: 'Operation Pacifier'

In the past, the FBI has regularly used special software in order to capture the IP address and other identifying data of computer users. Operation Pacifier was deployed to unmask visitors and distributors of CSAM on the darkweb forum 'Playpen'. Playpen has been labelled by the media as 'the most notorious darknet child pornography site'.[106] It was a forum that was only accessible via Tor and was online in the period of 2014-2015. CSAM, including materials of young children (under 12-years-old), was exchanged between members on the forum.

The Playpen forum received a lot of media attention because the FBI de-anonymised visitors of the forum in 2015. According to investigative journalists, this was possible because the FBI had temporarily taken over the website and, using special software, recorded identifying information of visitors to the website, such as IP addresses, MAC addresses and other technical information from the visitors' computers. As a result of the operation, 870 people have been arrested or convicted by May 2017, of whom 368 are from the European Union. In addition, 259 abused children have been identified or removed from their victimising situations.[107]

According to media reports, the FBI transferred the identifying information of EU visitors to Europol. Europol then carried out its coordinating role and forwarded the data to the various national investigation authorities within the European Union. The principle of trust (enshrined in international law) allows the prosecution to be confident that the evidence has been lawfully gathered by foreign authorities.

106 C. Farivar, 'Creator of infamous Playpen website sentenced to 30 years in prison', *Ars Technica*, 5 May 2017.

107 J. Cox, 'FBI's Mass Hack Hit 50 Computers in Austria. Revelations that the "Operation Pacifier" child porn investigation extended to Austria too shows the extent of the FBI's reach overseas', *Motherboard,* 28 July 2016.

As with network searches (discussed in Section 9.3.3), the unilateral application of hacking as an investigative method (another type of remote search) may incur an infringement on the territorial restriction of enforcement jurisdiction. In their extensive analysis regarding the law applicable to 'transborder access to computer systems', Koops and Goodwin (2014, p. 61) summarise the current view in international law as follows:

> 'The most solid view on what international law permits is that accessing data that are, or later turn out to be, stored on a server located in the territory of another state constitutes a breach of the territorial integrity of that state and thus constitutes a wrongful act (...) except where sovereign consent has been formally given.'

The territorial restriction of enforcement jurisdiction in the context of hacking as an investigative method can lead to a situation in which law enforcement officials are not able to gather evidence related to an individual who is located in their own state, because the individual uses an online service provider that stores or processes data on foreign territory. Yet, when a criminal utilises anonymisation techniques, such as proxy-services, VPN-services, and Tor, it may not be possible to identify the user of the computer or to locate the computer used by the suspect. For this reason, some national authorities, including Dutch, Belgian and U.S. authorities, have created an exception that hacking as an investigative method may be applied unilaterally, when the location of the targeted computer cannot reasonably be determined.

However, it oftentimes remains unclear what level of duty of care law enforcement needs to employ in its attempt to determine the location of the computer. Some countries, like the Netherlands, require law enforcement authorities to take additional factors into consideration when determining whether unilateral action is allowed. These factors include: (a) the seriousness of the crime, (b) the degree of the involvement of the Netherlands (either by Dutch victims or the use of IT infrastructure located in the Netherlands), (c) the nature of the investigative techniques (e.g. remotely disabling data is deemed more intrusive than remote copying), and (d) the risks for the integrity of the computers involved.[108]

108 See further the Dutch *Staatscourant*, 2019, 10277.

9.6 Disrupting cybercrime

The identification and prosecution of suspects of cybercrime is complex due to the challenges of anonymity, encryption, and jurisdiction. Successful detection and prosecution of cybercrime suspects is often not possible. When the detection or prosecution of cybercriminals is not feasible, the disruption of criminal processes is regarded as an alternative or complementary method to reduce harm to citizens and businesses. This approach focusses, for example, on the criminal revenue models behind the various types of cybercrime (van den Eeden et al., 2021). It is also called the 'broad approach' in fighting cybercrime, because it takes into account stopping the crime, stopping perpetrators or otherwise protecting the interests of victims, alongside the 'traditional' investigation and prosecution of cybercriminals (Bonnes & Divendal, 2024). With disruption, concrete barriers are placed in the crime script of offenders (as explained in Chapter 3 and 4).

In this book, several examples of these mitigation strategies and interventions have already been mentioned. These include removing ('taking down') illegal content, warning participants in a cybercriminal chat group of the illegality of their actions by posting a message, knock-and-talk actions, as well as by means of targeted advertisements to target groups, disabling a cybercriminal infrastructure (such as a botnet), and notifying or helping victims of cybercrime through websites such as nomoreransom.org.

From a legal perspective, it is unclear to what extent special investigative powers may be used when the goal is not prosecution for the crime, but rather ending a crime or disrupting cybercrime. In the Netherlands, this discussion has started only recently (Hirsch Ballin & Oerlemans, 2023; van den Eeden et al., 2021). A part of the problem is that police operations pursuing a broad approach to fighting cybercrime, is that this does not always lead to a criminal case. This is problematic, because in criminal cases the judge reviews the legality of compliance with the Code of Criminal Procedure during a criminal trial (Bonnes & Divendal, 2024; Oerlemans & van Wegberg, 2019; van den Eeden et al., 2021). If there is no trial, then there is also no such review. This constitutes an oversight problem or 'oversight gap' of compliance with laws and regulations, including the Police Data Act (Fedorova et al., 2022; Hirsch Ballin & Oerlemans, 2023; Schermer, 2022; Schermer & Galič, 2022; Stevens et al., 2021). Hirsch Ballin and Oerlemans (2023) argue that these disruptive actions are possible as part of a broad approach in fighting against cybercrime, but only in addition to the goal of the

traditional criminal investigation to prosecute individuals and bring them to justice. Despite this debate and suggestions, we do not expect any changes in the legal framework to address these issues in the following years.

9.7 To conclude

In this chapter, we discussed various digital investigation methods based on the challenges of jurisdiction, anonymity and encryption in cybercrime cases. Of course, there are many other problems that can be identified that are of a more organisational and practical nature. Research shows, for example, that the general level of knowledge about digital investigations needs to be improved within the Dutch police organisation (Boekhoorn, 2020; Ruiter et al., 2023).

The vast potential of digital evidence, coupled with the application of digital investigation methods, remains underutilised in many criminal investigations, despite their potential relevance in most criminal cases. This chapter provides numerous examples that extend beyond the realm of cybercrime investigations, touching on serious offenses such as murder and drug trafficking, in which computers and the internet are incidental to the crime (cyber-assisted crime). Law enforcement authorities are continually challenged to adapt to the ever-evolving and inventive tactics employed by cyber offenders, whether for monetary gain or to evade detection by law enforcement authorities (van de Sandt, 2019). Consequently, law enforcement authorities must continue to innovate and enhance their expertise to ensure the successful execution of digital investigations.

Moving forward, law enforcement authorities will persist in their efforts to combat and investigate cybercriminal organisations, also by collaboration in internationally coordinated operations. The role of multi- and interdisciplinary research is instrumental in monitoring these operations and the evolving cybercrime landscape. It is through this research that the necessity for legal, technical, or organisational modifications within the law enforcement domain can be effectively demonstrated, with respect for fundamental rights.

9.8 Discussion questions

1. To what extent are the mentioned digital investigation methods for cybercrime investigations relevant for conventional criminal cases?
2. What do you think of the statement: 'digital forensic investigation is a necessary tool for every investigation into a serious crime'?
3. Suppose you had to estimate the percentage of investigations into cybercrime that were successful in terms of sentencing or judgment. What would your estimate be after reading this chapter?
4. To what extent is judicial oversight necessary in undercover operations?
5. Does processing location data always constitute a serious privacy interference or does it become privacy intrusive only after an extended period of time?
6. Should we determine the level of privacy interference in relation to different (digital) investigatory powers *in abstracto*; that is, in relation to a type of power, rather than in relation to a concrete case in which a power was used?
7. Why do transborder online undercover operations challenge legal certainty of the individuals involved in these operations?
8. Do you think that the possibility to send data protection orders to companies instead of governments is the way forward when it comes to transborder investigations? Should the EU try to establish an 'executive agreement' with the United States?
9. Considering all of the criticism of a hacking power for law enforcement authorities, do you think it is desirable to use it as an investigation power? Do we have alternatives?
10. What do you think of the statement: 'the territorial restriction of enforcement jurisdiction is no longer applicable to internet investigations'?
11. Should the use of zero-day exploits by law enforcement authorities be regulated?
12. Are changes in the law necessary to accommodate a 'broad approach' in fighting cybercrime?

9.9 Key concepts

- Anonymity
- Cloud computing
- Data protection order

- Digital evidence
- Disrupting cybercrime
- Encryption
- Hacking power
- Infiltration
- Investigative powers
- Jurisdiction
- Legal assistance treaty
- Legality principle
- Network search
- Open-source investigations
- Privacy
- Search and seizure
- Undercover
- Vulnerability (unknown)
- Zero-day exploit