Police hacking in the Netherlands

An examination of the necessity and proportionality of the investigatory power of police hacking

Master Thesis Law & Technology, Tilburg University
SNR 2046839

Florianne Kortmann
Thesis Supervisor: Dr. Maša Galič
Second Reader: Lucas Jones
Tilburg, August 2020

Table of Contents

Chapter I: Introduction

§1.1 Background

Networked technologies have resulted in new opportunities for crime.[1] So-called cyber-assisted crimes in which the criminal uses networked technology as a tool to facilitate a low-end crime (think of a murderer googling information on how to dispose of a body), and cyber-enabled crimes in which the criminal uses the network to commit existing crimes on a global scale (think of Ponzi or Pyramid selling schemes) are now a daily reality.[2] Moreover, cyber-dependent crimes, i.e. "true cybercrimes wholly mediated by networked technology" are increasingly committed in which the computer or computer network is the target of the crime (think of hacking, botnets, and DDoS attacks).[3]

The sui generis character of cybercrime - which this thesis characterizes as both cyber-enabled and cyber-dependent crime – directly challenges the characteristics of traditional crime that shape the traditional model of law enforcement.[4] Traditional crime is characterized by physical proximity of the perpetrator and the victim, a low amount of victims, physical constraints of the real-world, and clearly identified patterns regarding the perpetrator.[5] However, physical proximity is not required for cybercrime because the perpetrator can commit the crime from his computer on a global scale.[6] Moreover, the automation of cybercrimes results in many victims with little effort, and various crimes can be conducted simultaneously.[7] Furthermore, because criminals commit crimes online, they avoid the majority of physical constraints that are present in the real world as a result of which they may be more difficult to detect and identified.[8] Crimes are also discovered at a later moment because digital traces are more difficult to detect or have already been wiped out which results in law enforcement being confronted with a cold trail.[9] Even if digital traces are left behind, it is increasingly difficult to detect the perpetrator as law enforcement is unable to track the perpetrator's location because of the use of anonymization tools such as VPNs, fake identities, and torrent networks.[10] Finally, clear identified patterns regarding the perpetrator are not present because cybercrime is underreported or not noticed

[1] Bert-Jaap Koops, 'The Internet and its opportunities for cybercrime' (2010). Tilburg Law School Legal Studies *Research Paper Series* No, 09/2011, p. 735; Peter Grabosky, 'The Evolution of Cybercrime, 2004-2014' (2014). *RegNet Research Paper No. 2014/58*. p. 9-12;
[2] David Wall, *Cybercrime: The Transformation of Crime in the Information Age*. Vol. 4. Polity. 2007, p. 44-48.; David Wall, 'Hunting, Shooting and Phishing: New Cybercrime Challenges for Cybercanadians in the 21st Century' (2008). Eccles Centre for North American Studies, London, p. 16-20
David Wall 'Crime, security and information communication technologies: The changing cybersecurity threat landscape and implications for regulation and policing' in R. Brownsword, E. Scotford and K. Yeung (eds) *The Oxford Handbook on the Law and Regulation of Technology*, Oxford: Oxford University Press, 2017;
[3] ibid
[4] Susan Brenner. Clarke, L., 'Distributed Security: A New Model of Law Enforcement.' John Marshall Journal of Computer & Information Law, Forthcoming, p. 7
[5] ibid, p.5
[6] ibid, p.7
[7] Maryke Silalahi Nuth. 'Taking advantage of new technologies: For and against crime.' (2008). *Computer Law & Security Review*, *24*(5), 437-446, p. 438
[8] Brenner (n 4), p. 7
[9] ibid
[10] ibid

because of salami techniques (think of stealing 10 cents from millions of people).[11] These characteristics make cybercrime difficult to detect, prevent, and prosecute, and tackling cybercrime has thus become a daunting task for law enforcement.[12]

Fortunately, technological developments have not only transformed crime but law enforcement too. Already in 1993, the Dutch legislator implemented Computer Crime Act I which criminalized key forms of computer criminality and introduced new investigative powers for law enforcement to combat computer crime such as the internet tap, the decryption order, the production order, and the network search.[13] Next, Computer Crime Act II was proposed in 1998.[14] By then, information was increasingly being exchanged, stored, and edited electronically and crimes against the computer, network, system, and data occurred regularly.[15] Criminals also increasingly used the network to store or hide evidence which hampered criminal investigation.[16] The legislator, therefore, wished to better regulate the 'electronic highway' to protect the legitimate user and to provide law enforcement with improved means to enforce the law.[17] However, because of European developments regarding the Cybercrime Convention, Computer Crime Act II was only implemented in 2006, shortly after the Cybercrime Convention came into force in the Netherlands.[18] Computer Crime Act II criminalized distributed denial of service attacks and adapted the existing procedural provisions to better reflect the technological situation.[19] Finally, in 2013, Computer Crime Act III was proposed, and on March 1st, 2019, the Act was implemented.[20] Computer Crime Act III introduced the new investigatory power of police hacking, enabled the use of a teenager as bait to better be able to prosecute groomers, and introduced a new substantive provision criminalizing online dealing in computer data.[21]

§1.2 Problem Statement

The legislator has actively created new investigatory powers to empower law enforcement to keep up with cybercrime. Most recently, Computer Crime Act III came into force which introduced the investigatory power of lawful hacking into article 126nba of the Dutch Code of Criminal Procedure (hereafter: DCCP). This provision allows the designated police officer to hack an automated work in use by the suspect in order to determine certain aspects of the

[11] Koops 'The Internet and its' (n 1), p.740
[12] Brenner (n 4), p.7
[13] *Kamerstukken II* 1989/1990, 21 551, nr. 3, p. 25-30; Computer Crime Act I (Stb. 1993, nr. 33);
see also Bert-Jaap Koops, 'De dynamiek van cybercrimewetgeving in Europa en Nederland.' (2012) 38 *Justitiële Verkenningen* (1), p. 12-13; Bert-Jaap Koops & Schellekens, M. H. M. 'Computercriminaliteit II: de boeven zijn er - nu de wet weer.' (1999) *Nederlands Juristenblad*, 74(37), p.1
[14] ibid
[15] *Kamerstukken II*, 1998/1999, 26 671, nr. 3, p. 2.
[16] ibid
[17] ibid
[18] Computer Crime Act II (Stb. 2006, nr. 301); Convention on Cybercrime, Budapest, 23.XI.2001;
Koops, 'De dynamiek van cybercrimewetgeving' (n 14), p.12
[19] Koops & Schellekens (n 13), p. 13
[20] Computer Crime Act III (Stb, 2018, nr. 322)
[21] Ministry of Justice and Security. 'Nieuwe wet versterkt bestrijding cybercriminaliteit' (28 February 2020) <https://www.rijksoverheid.nl/actueel/nieuws/2019/02/28/nieuwe-wet-versterkt-bestrijding-computercriminaliteit> accessed 19 February 2020

computer or user[22], intercept confidential communications[23], conduct systematic observation[24], secure stored and future data[25], and render data inaccessible.[26] To clarify, an automated work is any computer or computer network that automatically processes computer data based on a computer program (think of computers, servers, modems, routers, smartphones, tablets, televisions, pacemakers, smart devices et. Cetera).[27]

The hacking provision was created in response to three technological barriers to criminal investigation: the encryption of electronic data, wireless networks, and cloud computing.[28] These developments are said to hamper the police's ability to locate and gain access to potential key evidence that is required to effectively prosecute and prevent cybercrime.[29] Encryption, for example, undermines the police's ability to read out or access collected data as it turns plain-text into unreadable code which can only be accessed with the correct private key or password.[30] Wireless networks facilitate broad access to the internet from various access points, thereby contributing to anonymity on the network and reducing the usefulness of an internet tap which must be placed on a specific access point.[31] Finally, cloud computing allows the storage of data on an external server outside one's network as a result of which data is spread across different locations which hampers the process of retrieving such data.[32] With hacking, law enforcement is said to at least partially overcome these barriers to the criminal investigation.[33]

While the hacking provision was introduced to assist the police in their investigatory duties, supposedly improving security as cybercrime will be reduced, it simultaneously provides the police with a set of far-reaching powers. Not only will the police make use of "manipulation of, and interferences with peoples' devices and software" but the subsequent surveillance will occur covertly as unauthorized access to one's device is gained in which nowadays, almost all information is stored.[34] To this end, the police's use of the hacking powers to intercept confidential communications, to conduct systematic observation, and to secure stored and future data are particularly problematic, as these hacking powers enable the police to subject the targeted individual to a form of covert surveillance that can be deemed highly intrusive. With these hacking powers, the police can remotely activate a microphone or keylogger to intercept confidential communications such as WhatsApp messages, texts, e-mails, and they may secure existing and future stored data such as data files, photos or videos by using a keylogger or search algorithm.[35] The police can also track the location of a suspect to conduct

[22] Article 126nba(1)(a) DCCP
[23] Article 126nba(1)(b) DCCP
[24] Article 126nba(1)(c) DCCP
[25] Article 126nba(1)(d) DCCP
[26] Article 126nba(1)(e) DCCP
[27] *Kamerstukken II* 2015/2016, 34 372, nr. 3, p. 86;
See also Article 80sexies Dutch Criminal Code for the definition of an automated work
[28] *Kamerstukken II* 2015/2016 (n 27), p.7-12
[29] ibid
[30] *Kamerstukken II* 2015/2016 (n 27), p. 7-10
[31] *Kamerstukken II* 2015/2016 (n 27), p. 10-11
[32] *Kamerstukken II* 2015/2016 (n 27), p. 11-12
[33] *Kamerstukken II* 2015/2016 (n 27), p. 7-10
[34] Privacy International, 'Government hacking' <https://privacyinternational.org/learning-topics/government-hacking> accessed 22 February 2020
[35] *Kamerstukken II* 2015/2016 (n 27), p.7-12

systematic observation as a result of which a more or less complete picture of one's private life can be established.[36] Because the data that is collected will reveal information about the private life of citizens, the use of these hacking powers by the police will inevitably interfere with the right to respect for private life enshrined in article 8 of the ECHR.[37] Such interference by the police can only be justified if it is in accordance with the law, and is necessary in a democratic society in the pursuit of a legitimate aim.[38] This latter condition is precisely where the problem lies, however, as various actors openly questioned the necessity and proportionality of the hacking provision.

Firstly, it was stated that the government had not sufficiently motivated the necessity of the hacking provision as it was not clear how the hacking powers would assist the police in overcoming the challenges arising from these technological developments, and there were also no statistical figures presented on what is wrong with already existent powers.[39] Moreover, messages from the media and a WODC report indicated that existent powers such as the internet tap were not being optimally used because of a lack of knowledge and capacity.[40] Thus, it was argued that there could be no necessity for a new power that is highly intrusive as the focus should be on improving the effectivity of existing powers before concluding that these powers are insufficient.[41]

Furthermore, it was argued that the hacking powers were not properly restricted in their use and application as "hacking should only be possible in case of organized crime, terrorism, or life-threatening cases."[42] Moreover, the fact that the hacking provision contained five hacking powers was criticized as a large amount of special investigatory powers were combined into a single provision with every hacking power enabling an unlimited amount of functionalities.[43] It was further stated that because perpetrators often do not work from their computer, networks, or servers but instead use computers in use by third parties to commit crimes or to hide evidence, the hacking powers would interfere with the right to private life of third parties too.[44] Finally, it was noted that the hacking powers lacked sufficient safeguards and oversight mechanisms.[45]

It is crucial that the legislator adequately balances the need for new investigatory powers with the fundamental rights of citizens, in which any far-reaching power must be subjected to

---

[36] ibid
[37] European Convention on Human Rights as amended, Rome, 4.XI.1950, article 8
[38] ibid
[39] Bits of Freedom, 'Reactie op consultatie Wetsvoorstel Computercriminaliteit III', p. 10-11. *Attachment 651730* to *Kamerstukken II* 2015/2016, 34 372, nr. 3; p.10-11
Nederlandse Orde van Advocaten (Dutch Bar Association). 'Betreft: concept-wetsvoorstel tot verbetering van de opsporing en vervolging van computercriminaliteit (computercriminaliteit III)'. *Attachment 651732* to *Kamerstukken II* 2015/2016, 34 372, nr. 3, at §2.9
[40] Bits of Freedom (n 39), p. 11; see also article 126m DCCP
[41] ibid
[42] Jacob Kohnstamm; Dutch Data Protection Authority Representative, cited in Joost Schellevis and Nando Kasteleijn, 'Forse kritiek op hackbevoegdheid politie' *NOS* (11 February 2016) <https://nos.nl/artikel/2086191-forse-kritiek-op-hackbevoegdheid-politie.html> accessed 18 February 2020
[43] Bits of Freedom (n 39) p. 6
[44] Bits of Freedom (n 39), p. 3-5
[45] Nico Van Eijk; Professor information Law at University of Amsterdam, cited in J. Kraan 'Veel kritiek op voorgestelde hackbevoegdheid voor politie.' *NU* (11 February 2016) <https://www.nu.nl/internet/4213037/veel-kritiek-voorgestelde-hackbevoegdheid-politie.html> accessed 14 April 2020

scrutiny to avoid arbitrary treatment of citizens by the government. Because the necessity and proportionality of the hacking provision were openly questioned by various actors, and considering that these three hacking powers can be deemed highly intrusive and may only be justified if they are, inter alia, necessary in a democratic society in the pursuit of a legitimate aim, the objective of this thesis will be examining the necessity and proportionality of these three hacking powers in relation to the right to respect for private life as found in article 8 ECHR.

§1.3 Research question and sub-questions

Considering the above, this thesis will answer the following research question:
Can the new investigatory power to hack, introduced in article 126nba of the DCCP, be considered a necessary and proportionate tool for evidence gathering by the police to combat cybercrime, in particular when considering the right to respect for private life in article 8 ECHR?

To answer this question, the following sub-questions will be answered:

1. What is the legislator's rationale behind the creation of article 126nba of the DCCP and which concrete hacking powers does article 126nba(1) (sub-paras. b, c, and d) of the DCCP grant?
2. Under what conditions can the hacking powers be used and are there any alternative and less intrusive investigatory measures available to police to combat cybercrime?
3. How do the hacking powers of article 126nba(1)(sub-paras. b. c, and d) of the DCCP interfere with the right to respect for private life and what conditions must be fulfilled according to ECtHR case-law for a restrictive measure to be necessary and proportionate, particularly in the case of covert surveillance powers used by law enforcement?
4. Considering the various safeguards identified in sub-question 2, and the conditions for necessity and proportionality identified in sub-question 3, can the hacking powers of 126nba(1) (sub-paras. b, c, and d) of the DCCP be considered necessary and proportionate tools for evidence gathering by the police to combat cybercrime?

§1.4 Methodology

This thesis focuses on hacking by the Dutch police in order to intercept confidential communications[46], to conduct systematic observation[47], and to secure stored and future data.[48] As such, hacking to determine certain aspects of the computer or user[49] and to render data inaccessible[50] are excluded. These hacking powers are excluded because they do not result in highly intrusive secret surveillance of citizens. To illustrate, hacking to determine certain

[46] Article 126nba(1)(b) DCCP
[47] Article 126nba(1)(c) DCCP
[48] Article 126nba(1)(d) DCCP
[49] Article 126nba(1)(a) DCCP
[50] Article 126nba(1)(e) DCCP

aspects of the computer or user enables the police to conduct a digital sneak and peek search in which only certain aspects of the computer and users are determined while hacking to render data inaccessible concerns a single action which immediately reveals to the suspect that someone has interfered with his or her automated work. The jurisdiction of the Netherlands was chosen because the hacking powers were recently introduced into the DCCP and are potentially problematic. Additionally, relatively few countries know a provision of police hacking. Finally, it is important to note that this thesis considers each investigatory purpose for which hacking can be used to be a separate hacking power.

Having said that, this thesis is predominantly based on doctrinal legal research and desk research. To answer sub-question one and two, positive law (the DCCP, Computer Crime Act III, Decision Investigation in an Automatic Work), parliamentary documents, legal theory focused on the Dutch criminal system, academic literature, news articles, and blogs were analyzed through black-letter law analysis and critical evaluation. Moreover, answering sub-question three required a thorough analysis of European Court of Human Rights (hereafter: ECtHR) case-law regarding the scope of the right to respect for private life and the conditions of necessity and proportionality of secret surveillance powers conducted by law enforcement in relation to the right to respect for private life. Finally, sub-question four was answered by applying the findings of ECtHR case-law regarding what constitutes a necessary and proportionate covert surveillance power to the earlier identified legal framework surrounding the hacking power in order to evaluate the necessity and proportionality of the three hacking powers.

§1.5 Chapter overview

This thesis is structured as follows. After the introduction (1), the Dutch legislator's rationale behind the creation of the hacking provision will be explained as well as which concrete hacking powers article 126nba (1) (sub-paras. b, c, and d) of the DCCP grants to the police (2). The next chapter (3) will then discuss the legal framework surrounding the hacking powers by examining under what conditions the hacking powers can be used. This includes an identification of the legal safeguards and oversight mechanisms incorporated by the legislator against the arbitrary use of the hacking power by police. Moreover, it includes an analysis of whether there are any alternative and less intrusive investigatory measures available to the police compared to the hacking power. Next, it is discussed how the hacking powers interfere with the right to private life in article 8 of the ECHR, and what conditions must be fulfilled according to ECtHR case-law for a restrictive measure to be necessary and proportionate, particularly in the case of surveillance measures conducted by law enforcement (4). Hereafter, the insights of the previous chapters are combined to critically assess and evaluate whether the hacking powers can be considered necessary and proportionate tools for evidence gathering by the police to combat cybercrime (5). Lastly, a conclusion will be presented in which the findings are reflected upon, and suggestions for further research are proposed (6).

Chapter II: The rationale behind the hacking provision and the concrete hacking powers granted to the police

This chapter discusses the Dutch legislator's rationale behind the hacking provision as well as which concrete hacking powers article 126nba(1) (sub-paras. b, c, and d) of the DCCP grants. In the introduction, it was illustrated that the hacking provision was created in response to three technological barriers to criminal investigation: the encryption of electronic data, wireless networks, and cloud computing.[51] To grasp this, this chapter discusses these technological barriers after which light is shed on the legislator's rationale behind the hacking provision (**§**2.1). Hereafter, the three hacking powers granted by the hacking provision are portrayed, and it is illustrated how through the police's use of these hacking powers the problems related to these technological developments are at least partially overcome (**§**2.2). Finally, a conclusion is presented in which an answer to the first sub-question is provided (**§**2.3).

§2.1 Rationale behind the hacking provision

§2.1.1 Technological barriers to criminal investigation

The first technological development that causes problems for criminal investigation is the encryption of electronic data.[52] Encryption is the technological process of converting readable data (plain-text) into an unreadable code (ciphertext) that can only be decrypted with the correct private key or password.[53] Both data in transit (data that is currently being processed or transferred by an automated work) and stored data (data stored on an automatic work) can be encrypted.[54] In the case of encryption of data in transit, one can think of communication software or services such as Skype, WhatsApp, VPN, Gmail, and Twitter that encrypt communications by default.[55] However, data in transit may also be manually encrypted, for example via the plug-in Pretty Good Privacy (e-mail), via The Onion Routing (internet traffic) or by making use of the encryption option that Facebook and Hotmail provide.[56] For stored data, one can think of smartphones that increasingly have full disk encryption integrated into their operating software by default, and encryption programs offered on the internet for free such as TrueCrypt and BoxCryptor that automatically encrypt data before it is saved on the automated work, with the former program also enabling the possibility of encrypting the entire hard drive.[57]

---

[51] *Kamerstukken II* 2015/2016 (n 27), p. 7-12
[52] *Kamerstukken II* 2015/2016 (n 27), p. 7-10
[53] James A. Lewis, Zheng, D.E., Carter, W.A. *The effect of encryption on lawful access to communications and data* (2017), Rowman & Littlefield. p,1.
[54] *Kamerstukken II* 1998/1999 (n 27), p.3
[55] *Kamerstukken II* 2015/2016 (n 27), p. 8
[56] ibid
[57] Joseph Gildred 'How to encrypt your data for cloud storage' *Cloudwards* (18 May 2018) <https://www.cloudwards.net/how-to-encrypt-your-data-for-cloud-storage/#Zero-Knowledge-Cloud-Storage> accessed 12 May 2020;
See also *Kamerstukken II* 2015/2016 (n 27), p. 8

Through encryption, data confidentiality is ensured as unauthorized access to the content of data is prevented, thereby providing enormous benefits for data security and privacy.[58] While it is in the general interest to encourage the use of strong encryption techniques, it also forms a barrier to criminal investigation because criminals remain undetected as the police's ability to understand or gain access to encrypted data is hampered.[59] When telecommunications are intercepted via phone, e-mail, or internet tap, for example, the intercepted data will only show cyphertext.[60] Similarly, when the police wish to access or secure data stored in an automated work during a search of a place or during a network search, the police do not possess the correct private key or password required to obtain access to the encrypted data.[61]

The second technological barrier to criminal investigation concerns the use of public wireless networks by criminals.[62] The widespread availability of public wireless networks in restaurants, trains, hotels, and other spaces impedes the ability of the police to effectively intercept telecommunications through an internet tap, particularly when the suspect makes use of (different) hotspots.[63] A suspect may, for example, move from one network to another as a result of which an internet tap must be placed on the different access points to obtain the complete communication data, while different networks and service providers may also be involved.[64] The legislator notes that this proves impossible in practice, and even if an internet tap can be successfully placed on the various hotspots, the communication may be encrypted.[65] Moreover, the router upholds connections with a wide variety of automated works because of the hotspot, as a result of which it may be difficult to determine which data flow pertains to which automated work and user.[66] Consequently, data from persons in whom the police are not interested are also intercepted, thereby undermining the principle of proportionality which entails that the use of this power should be limited to the interception of the communication of the suspect only in order to respect the right to private life of third parties.[67] In short, wireless networks contribute to anonymity of the suspect on the network and hamper the police's access to potential evidence.

The final technological barrier to criminal investigation is cloud computing.[68] Cloud computing can be defined as the "ability to access a pool of computing resources owned and maintained by a third party via the Internet."[69] Whereas before, data could only be stored in the hard drive of a computer located in a private place or within the own network, one now increasingly makes use of web-based applications that enable the storage of data on an external server outside one's

[58] Ivan Škorvánek, Koops, B.J. Newell, B.C., Roberts, A.J. 'My Computer is My Castle: New Privacy Frameworks to Regulate Police Hacking' (2019) *Brigham Young University Law Review*, forthcoming. p. 2-3
[59] *Kamerstukken II* 2015/2016 (n 27), p. 7-12
[60] *Kamerstukken II* 2015/2016 (n 27), p. 9; See also article 126m DCCP
[61] *Kamerstukken II* 2015/2016 (n 27), p. 8; See also article 125i and 125j DCCP
[62] *Kamerstukken II* 2015/2016 (n 27), p 10
[63] Article 126m DCCP; *Kamerstukken II* 2015/2016 (n 27), p 10
[64] ibid
[65] ibid
[66] ibid
[67] ibid
[68] *Kamerstukken II* 2015/2016 (n 27), p. 11
[69] Rachna Arora, Parashar, A. 'Secure user Data in Cloud Computing using Encryption Algorithms' (2013) *International Journal of Engineering Research and Applications Vol 3 Issue 4*, pp. 1922-1926, p. 1922

network.[70] Well-known cloud computing providers such as Google and Hotmail offer a wide variety of integrated applications to their users, including data storage services (think of Google Drive, OneDrive).[71] When these services are used, the data is automatically saved on an external server which is often located in foreign territories.[72] Data files may also be saved in various pieces, as a result of which they may be spread across various servers which could be present in various countries.[73] Finally, because of the automatic process and the fact that data may be located across various servers, not even the service provider may be able to determine the location of the server on which the data is stored.[74] The problem of cloud computing is thus twofold. On the one hand, it relates to the difficulty of the police to determine the location of such data once stored on the external server (anonymity). On the other hand, it relates to the difficulty to retrieve the located data because of its diffuse location in which data may be spread across various countries.

§2.1.2 Lacuna in present investigatory powers

According to the legislator, present investigatory powers are inadequate to tackle the problems arising as a result of encryption, wireless networks, and cloud computing because they are based on the idea that suspects and data can always be located as well as that data can always be decrypted and that data stored elsewhere can always be retrieved.[75] As seen, however, this notion is directly challenged by the three technological developments as they enable the suspect to remain anonymous on the network and hamper the ability of the police to gain access to data. A gap in present investigatory power is said to be present and this is problematic because the police's ability to gain access to electronic data for the purpose of detecting and prosecuting cybercrime is hampered, if not made impossible.[76]

Whether the present investigatory powers are indeed inadequate to combat the problems arising from these three technological developments and cause a lacuna in present investigatory powers to effectively combat cybercrime will be critically assessed in Chapter 3 (§3.2).

§2.1.3 Pressing needs and the hacking provision as a solution

Considering the three technological barriers to criminal investigation, the legislator identifies the following pressing needs. Firstly, there is a need for the police to be able to retrieve the keys or passwords of encryption programs or services so that they can decrypt and subsequently access the data.[77] Secondly, there is a pressing need to intercept communications either before they are encrypted (before the communication is sent) or after they have been decrypted by the software of the automated work (after the communication is received).[78] Thirdly, there is a

[70] Škorvánek, Koops, Newell, Roberts (n 58), p. 3
[71] *Kamerstukken II* 2015/2016 (n 27), p 11
[72] ibid
[73] ibid
[74] ibid
[75] *Kamerstukken II* 2015/2016 (n 27), p. 6-15
[76] ibid
[77] *Kamerstukken II* 2015/2016 (n 27), p. 9
[78] *Kamerstukken II* 2015/2016 (n 27), p. 9-10

pressing need to be able to access an automated work to identify the device or user to enable a more targeted investigation afterward.[79] Finally, there is a pressing need for the police to access data stored in the Cloud without the involvement of the suspect or service provider.[80]

The hacking provision was created to fill this presumed gap in investigatory powers, thereby overcoming the problems and subsequent pressing needs arising from these three technological developments and empowering the police to effectively prevent and prosecute cybercrime.[81]

§2.2 Concrete hacking powers granted to the police

The previous section discussed the legislator's rationale behind the creation of the hacking provision. This section portrays three hacking powers granted to the police by the hacking provision and examines to what extent these hacking powers help the police overcome the previously identified problems arising from the three technological developments.

§*2.2.1 Hacking techniques to gain access to an automated work*

Article 126nba of the DCCP grants the police the power to remotely access an automated work in use by the suspect. Because unauthorized access to an automated work is gained, this can be considered hacking.[82] Access to the automated work can be obtained in three ways, although this is not exhaustive. Firstly, access may be obtained through social engineering (think of phishing) or artificial intelligence (think of AI software used to guess passwords) in which the login details of the suspect are used. [83] Secondly, access may be obtained through remotely infecting the computer with malware.[84] A person may be deceived to open a certain file attached in an email after which a malware (trojan or rootkit) is automatically installed.[85] The malware could also be installed in the case the police have physical access to an automated work, or by tricking the suspect into plugging an infected USB stick in the automated work.[86] Finally, existing vulnerabilities of an automated work can be exploited in which mistakes or software leaks are used to take control of devices or networks.[87] Once access is gained, the hacking powers can be used, three out of five which are discussed below.

§*2.2.2 Hacking to record and intercept communications*

The police may hack an automated work to record and intercept confidential communications.[88] The unauthorized access could be obtained by sending a phishing email in which the suspect receives an email from a 'legitimate body'. After clicking on the file in the email, a trojan is

[79] *Kamerstukken II* 2015/2016 (n 27), p. 11
[80] *Kamerstukken II* 2015/2016 (n 27), p. 12
[81] *Kamerstukken II* 2015/2016 (n 27), p. 6-15
[82] Hacking. (n.d.) In Lexico. <https://www.lexico.com/definition/hacking> accessed 9 April, 2020
[83] *Kamerstukken II* 2015/2016 (n 27), p. 34
[84] *Kamerstukken II* 2015/2016 (n 27), p. 34
[85] ibid
[86] Škorvánek, Koops, Newell, Roberts (n 58), p.8
[87] *Kamerstukken II* 2015/2016 (n 27), p. 34
[88] Article 126nba(1)(b) DCCP

secretly installed which can execute any program it is designed for (method 2).[89] The malware could also be placed by exploiting a web browser's vulnerability (think of sending a phishing email containing a link to a website). Once the suspect visits the infected website, the malware is automatically launched (a combination of methods 2 and 3).[90]

With this power, the police can execute a keylogger program via the installed malware which enables the recording of keystrokes and mouse clicks as a result of which electronic communications may be intercepted such as e-mail, internet browsing, texts, and chats.[91] Moreover, malware that enables the police to remotely activate the microphone or camera of an automated work can be used, so that voice over internet protocol (think of WhatsApp and Skype calls) and other oral communications can be eavesdropped or otherwise recorded.[92] By using this hacking power, the problem of encryption can be circumvented as confidential communications can be intercepted before they are encrypted. Moreover, communications can be recorded even if the location or the identity of a person is unknown which overcomes anonymity.

§*2.2.3 Hacking to conduct systematic observation*

The police may also hack to conduct systematic observation in which the location of a person or automated work is followed over a longer period.[93] Because people carry their phones with them wherever they go, the location data that is obtained will give a more or less complete picture of the suspect's life.[94] The location data may be obtained by sending a phishing email to the suspect who opens the email on his phone after which malware is installed on the automated work which enables the police to take over the device, and to remotely activate the GPS or WIFI signal and initiate transmission of location data to the provider (method 2).[95] Another option could be remotely activating the camera function of the automated work via malware which enables visual observation of environmental characteristics.[96]

This hacking power proves useful when the suspect manages to evade an observation team, or when the suspect makes use of a GPS jammer as a result of which location data cannot be obtained.[97] Since this power enables the police to determine the location of the automated work, it also frees the path to conduct different investigatory activities.[98] The police could, for example, arrest a suspect even when the home location is unknown.[99] However, it is unclear how this hacking power overcomes any of the problems and subsequent pressing needs previously identified.

---

[89] Škorvánek, Koops, Newell, Roberts (n 58), p.9
[90] ibid
[91] *Kamerstukken II* 2015/2016 (n 27), p.23-25
[92] ibid
[93] Article 126nba(1)(c) DCCP
[94] *Kamerstukken II* 2015/2016 (n 27), p. 26
[95] *Kamerstukken II* 2015/2016 (n 27), p. 26-27
[96] ibid
[97] *Kamerstukken II* 2015/2016 (n 27), p. 25-26
[98] ibid
[99] ibid

§*2.2.4 Hacking to secure existing and future stored data*

Finally, the police may hack to secure existing data stored on the automated work and to secure data that enters the automated work after access has been obtained.[100] Because the police may also capture future data, this enables a form of remote monitoring of computer use, and hacking for this purpose can be considered the most comprehensive and intrusive functionality.[101]

The police can, for example, install malware via phishing which executes a program that repeats a search after a certain amount of time, thereby capturing newly stored data.[102] Moreover, real-time surveillance may occur through the execution of a keylogger program that transmits real-time information to the police regarding what the user is typing or clicking on.[103] Consequently, the content of data files can be secured before they become encrypted, and keys and passwords may be obtained through which access to the encrypted hard disks and stored data files can be acquired.[104] Finally, there is also the possibility of triggering screen casting functionalities in which screenshots can be made over a period of time.[105] Consequently, the internet use of the suspect can be monitored and the content of stored e-mails that were not exchanged can be secured.[106] Not surprisingly then, this hacking power can be considered the "virtually equivalent of an invisible police officer looking over your shoulder at whatever you do with your computer."[107]

With this hacking power, the police can circumvent encryption, as data can be secured before it is stored on the computer or cloud server. Moreover, it allows remote access to encrypted stored data files or decrypted stored communications without the involvement of the provider or suspect as decryption keys and login details can be obtained. Such details can also be used to gain access to a cloud account as a result of which access may be obtained to data that is stored elsewhere. Through this, the problems of encryption and cloud computing are, therefore, overcome.

§2.3 Conclusion

This chapter found that the Dutch legislator's rationale behind the creation of the hacking provision was filling a gap in present investigatory powers caused by three technological barriers to criminal investigation: encryption, wireless networks, and cloud computing. These technological developments render present investigatory powers ineffective because they cause anonymity of suspects on the network and hamper the ability of the police to collect, access, or retrieve electronic data provided it can be located. Consequently, the police's ability to gain access to electronic data for the purpose of detecting and prosecuting cybercrime is undermined, if not made impossible. This gap in present investigatory powers forms an obstacle to the

[100] Article 126nba(1)(d) DCCP
[101] ibid
[102] Škorvánek, Koops, Newell, Roberts (n 58), p.11
[103] *Kamerstukken II* 2015/2016 (n 27), p. 20-21
[104] ibid
[105] Škorvánek, Koops, Newell, Roberts (n), p.11
[106] *Kamerstukken II* 2015/2016 (n 27), p. 21
[107] Škorvánek, Koops, Newell, Roberts (n 58), p.11

effectiveness and success of criminal investigations into serious cybercrime. The hacking provision was created to supposedly fill this gap, thereby empowering police to effectively prevent and prosecute cybercrime.

Moreover, it was established that the concrete hacking powers granted to the police are hacking an automated work to record and intercept communications by activating a keylogger or microphone, hacking to enable systematic observation by activating a GPS or WIFI signal, and hacking to secure stored and future data by installing a keylogger or search algorithm. Finally, it was established that through the use of the first two hacking powers, the problems arising from encryption and cloud computing are overcome.

Chapter III: The legal framework

This chapter explores under what conditions the three hacking powers can be used, and whether there are any alternative and less intrusive investigatory measures available to the police to combat cybercrime. Firstly, the conditions of use, safeguards, and oversight mechanisms surrounding the hacking powers are identified (**§**3.1). Hereafter, a critical examination of whether there are any subsidiary investigatory measures available to the police to effectively combat cybercrime follows (**§**3.2). Finally, a conclusion is presented in which an answer to the second sub-question is provided (**§**3.3).

§3.1 Conditions of use, safeguards and oversight mechanisms

§*3.1.1 Conditions of use in article 126nba(1) of the DCCP*

The hacking provision can be found in article 126nba of the DCCP and was placed in Title IVA of the DCCP because of its covert and intrusive character.[108] Title IVA of the DCCP contains special investigatory powers that are risky for the integrity of the criminal investigation or that may infringe on one's fundamental rights in a more than a limited way.[109] The powers placed in this Title are subject to strict conditions that are discussed below.[110]

The first condition is that hacking by activating a microphone or keylogger to intercept confidential communications and hacking by activating a GPS signal or video camera function to conduct systematic observation may only be ordered by the public prosecutor in case of suspicion of a pre-trial detention crime which seriously breaches the legal order.[111] Pre-trial detention crimes are felonies that carry minimum imprisonment of four years such as rape and theft, but may also include designated felonies that carry imprisonment of fewer than four years such as money laundering or minor assault.[112] Whether these felonies result in a serious breach of the legal order depends on the nature of the crime or the relation to other crimes that have been committed by the suspect.[113] The nature of the crime is not only determined by the description of the fact in the law but it is also based on the severity of the facts and circumstances under which the crime has been committed.[114] Felonies such as murder, drug- and human trafficking, and financial felonies such as carousel fraud[115], for example, are crimes that automatically result in a severe breach of the legal order because of their violent character, scope, and consequences for society.[116] Still, less severe crimes may also result in a serious breach of the legal order, for example, when these felonies are committed alongside another

[108] *Kamerstukken II* 2015/2016 (n 27), p. 28
[109] *Instruction Investigatory Powers* (Stc. 2011, nr. 3240 as amended by Stc. 2012, nr. 10486), p. 1-2
[110] ibid
[111] Article 126nba(1)(b) and Article 126nba(1)(c) DCCP
[112] See Article 67(1) DCCP; See also Škorvánek, Koops, Newell, Roberts (n 58), p.18;
[113] Article 126nba(1) DCCP
[114] *Kamerstukken II* 1996/1997, 25 403, nr 3, p. 24-25
[115] With carousel fraud, *Party A* imports goods tax free from *Party B* who is located in another country. *Party A* then resells these goods to domestic buyers and collects tax from these buyers. Once the goods are sold, *Party A* disappears and does not provide the government the tax that has been charged.
[116] *Kamerstukken II* 1996/1997 (n 114), p. 24-25

crime.[117] Here, one can think of smaller fraud in combination with bribing government officials or the committing of a home burglary and subsequent phone theft after midnight.[118]

When the purpose of hacking is securing stored and future data, the hacking may only be ordered in the case of felonies which carry minimum imprisonment of eight years, and in the case of specifically designated felonies mentioned in the government decree *Decision Investigation in an automated work* (hereafter: Decision Investigation).[119] These designated felonies are cybercrimes such as the execution of a botnet or online child pornography in which there is a clear societal interest to end such crimes and to prosecute the perpetrator because these crimes seriously disrupt the legal order.[120]

From all of the above, it follows that the legislator restricts the scope of application of the hacking powers to serious (cyber)crime. By adding the safeguard that the felony must result in a severe breach of the legal order, the hacking powers are subjected to an aggravated condition of use. To illustrate, when a pre-trial detention crime such as forgery[121] is committed by a teenager faking an ID card, this may not necessarily result in a severe breach of the legal order, and the ordering of hacking will not be allowed. Nevertheless, this ground still appears to be rather broad, something that will be further discussed in §5.2.1.

The second and third conditions of use are that only the public prosecutor may order the hacking, and only when the investigation urgently requires it.[122] Whether an investigation urgently requires the ordering of the hacking is based on a proportionality and subsidiarity test.[123] The proportionality test requires that the interest that is served with the hacking is in balance with the extent of the intrusion to the right to private life.[124] The subsidiarity test requires that there are no less intrusive measures available to the police that can serve the same interest or end-goal.[125] To illustrate, when communications can be eavesdropped on by tapping a wire, hacking an automated work by remotely activating the microphone to eavesdrop on these communications may not be ordered, because the intended goal can be reached through the use of a less intrusive means. Through this test, an important safeguard is added as the hacking powers will only be ordered if it is truly necessary.

The fourth condition is that the hacking may only be ordered to conduct five predefined investigatory activities which are exhaustively mentioned.[126] As previously mentioned, this thesis focuses on three which are intercepting confidential communications by activating a microphone or keylogger, conducting systematic observation by activating one's GPS signal or

[117] Article 126nba(1) DCCP; See also Procurator General's Office of the Dutch Supreme Court 17 December 2013, ECLI:NL:PHR:2013:2696; Procurator General's Office of the Dutch Supreme Court 30 September 2014, ECLI:NL:PHR:2014:2162
[118] *Kamerstukken II* 1996/1997 (n 114), p. 24-25;
Procurator General's Office of the Dutch Supreme Court 30 September 2014, ECLI:NL:PHR:2014:2162, at 5
[119] Article 126nba(1)(d) DCCP; Decision Investigation in an Automated Work (Stb. 2018, nr. 340)
Dutch: *Besluit onderzoek in een geautomatiseerd werk*
[120] *Kamerstukken II* 2015/2016 (n 27), p. 29
[121] Article 225(1) DCCP
[122] Article 126nba(1) DCCP
[123] *Kamerstukken II* 2015/2016 (n 27), p. 53-54
[124] ibid
[125] ibid
[126] See article 126nba(1)(a-e) DCCP

camera, and securing stored and future data on a computer by using screen-casting functionalities, keyloggers or an algorithm.[127] By limiting the hacking to five powers, a safeguard is added as the public prosecutor can adequately assess the necessity of the use of these powers in a concrete case.[128] Also, it avoids the police from hacking a device and using an unlimited amount of functionalities to secure an unlimited amount of data without a legal basis.

Finally, only computerized works in use by the suspect may be hacked.[129] This does not only incorporate the suspect's computer but any computerized work that the suspect uses more or less regularly (more than just once or twice).[130] This is problematic, however, because the automated works of friends, co-inhabitants, and relatives or other third parties may also be hacked.[131]

§3.1.2 Further safeguards and oversight mechanisms

Once the public prosecutor has assessed whether the conditions mentioned in the previous section are fulfilled, he must notify the Central Examination Committee (hereafter: CEC) – an internal advisory body consisting of members of the police and the public prosecution body – of his intent to issue the hacking order.[132] The CEC examines whether the intent to issue the hacking order complies with rules and legislation, case-law, proportionality and subsidiarity, and balances the effectivity of the hacking and its potential drawbacks with the public interest that the hacking serves in an individual case.[133] After this assessment, it issues advice to the Council of Procurator's Generals - the Board of the Public Prosecutor's Office – who grants or denies permission for the hacking order to the public prosecutor.[134] By requiring an assessment by the CEC and prior permission of the Board, a form of internal oversight is added, and this is a unique safeguard because this process only applies to a very limited amount of investigatory powers.[135]

Moreover, the public prosecutor must obtain prior authorization from the investigative judge.[136] The investigative judge assesses the legality, proportionality, and subsidiarity of the hacking order before granting or denying the authorization.[137] To enable the investigative judge to conduct an adequate assessment, the hacking order must contain information regarding the suspected crime, the identified suspect, the targeted automated work, the facts and circumstances from which it follows that the hacking is urgently required, the nature and function of technical tool used, the investigatory activity, what part of the device is targeted, the category of data collected, and the intended period for which the hacking is ordered.[138] The

[127] See article 126nba(1)(b)(c)(d) DCCP
[128] *Kamerstukken II* 2015/2016 (n 27), p. 53
[129] Article 126nba(1) DCCP
[130] Škorvánek, Koops, Newell, Roberts (n 58), p.19
[131] ibid
[132] *Kamerstukken II* 2015/2016 (n 27), p. 37-38
[133] ibid
[134] ibid
[135] See article 5.1 of *Instruction Investigatory Powers* (n 109)
[136] Article 126nba(4) DCCP
[137] *Kamerstukken II* 2015/2016 (n 27), p. 30, p. 37-38
[138] Article 126nba(2) DCCP

authorization is also subject to these information requirements and must contain the period for which the authorization is valid.[139] Because the hacking order of the public prosecutor is subject to prior oversight by an independent judge, an additional safeguard is incorporated.

When the police investigate by activating a computer's microphone to eavesdrop on communications, by using a keylogger to secure telecommunications, or by activating the GPS signal to track one's location, the hacking involves the use of special investigatory activities that are separately regulated in the DCCP.[140] Because these powers are separately regulated, the conditions of use to which these individual powers are subject apply too. Consequently, a separate order of the public prosecutor is required.[141] Moreover, a separate authorization of the investigative judge must be obtained when the hacking concerns the use of a microphone or the recording of keystrokes to intercept communications.[142]

The hacking order may be issued for a maximum period of four weeks, after which the order can be prolonged for blocks of four weeks indefinitely.[143] When the order requires amendment, supplementation, extension, or termination, written authorization from the investigatory judge must again be obtained.[144] As such, the investigative judge executes oversight even after the hacking order has been issued as it must approve an extension or change.

During the police's hacking, oversight is conducted by the Inspectorate of Justice and Security who ensures that the hacking is executed in compliance with the legal requirements of the DCCP and Decision Investigation.[145] Oversight is conducted on, inter alia, the authorization of the police, the police's expertise and knowledge, logging obligations, and the destroying of data.[146] However, because the Inspectorate executes oversight under the authority of the Minister of Justice and Security, this cannot be deemed independent oversight.[147]

Once the hacking has ended, the public prosecutor must notify the person(s) concerned about the exercise of the hacking.[148] If the person concerned feels that his fundamental rights have been breached, he can bring his complaint before the criminal court.[149] The notification obligation further ensures that the person concerned will be aware of the hacking and subsequent surveillance activity and is ensured a right to redress.[150] This is an important safeguard because hacking is a covert power and not every investigation results in a criminal

[139] Article 126nba(4) DCCP
[140] See article 126l and article 126m DCCP (intercepting communications), article 126g DCCP (systematic observation)
[141] See article 126l(1), article 126m(1), and article 126g(1) DCCP.
[142] See article 126l(4) and article 126m(5) DCCP
[143] Article 126nba(3) DCCP
[144] Article 126nba(5) DCCP
[145] See article 126nba(7) DCCP and article 65 Police Act 2012 (Stb. 2012, nr. 315)
[146] ibid
[147] See article 65(1)(2) Police Act 2012
[148] *Kamerstukken II* 2015/2016 (n 27), p. 40; See also Article 126bb(1) DCCP
[149] Article 552a DCCP
[150] *Kamerstukken II* 2015/2016 (n 27), p. 40

indictment in which ex-post oversight by a judge can be conducted. However, it appears that the notification obligation is not always strictly followed in practice.[151]

§*3.1.3 Decision Investigation in an automated work*

Decision Investigation, a governmental decree, further regulates the execution of the hacking.[152] It follows that the hacking and subsequent investigatory activities may only be executed by police officers appointed by the chief of police which are part of the technical team.[153] These police officers have specialized knowledge in the field of communication and information technology.[154]

Once the relevant surveillance has been conducted and data has been obtained, the investigative officers of the tactical team will analyze the data.[155] The investigative officers that are part of the technical team cannot be part of the tactical team involved in the analysis of the evidence.[156] This functional separation is a key safeguard that prevents tunnel view and ensures the objectivity of the investigation.[157]

During the hacking, all relevant data is logged (think of activities conducted to execute the order, access to a technological tool, the data that is transferred to the technological infrastructure, the functioning of the technological infrastructure) by the technical team.[158] The tactical investigative officers must similarly report any investigatory activities conducted.[159] Through logging, the integrity and reliability of the data are ensured as any irregularity will be determined.[160]

Finally, the technological tool must be designed in a way that it is limited to executing the investigatory functionalities as specified in the hacking order.[161] The technological tool must also be approved by a supervisory body.[162]

§3.2 Alternative and less intrusive measures

Having examined the legal framework surrounding the hacking powers, this section will assess whether there are alternative and less intrusive investigatory powers available to the police that can overcome the problems arising for the criminal investigation. As Chapter 2 (§2.1) indicated, these problems directly relate to the suspect's anonymity on the network and the inability of the police to locate, collect/retrieve electronic, and access data. Importantly, the aim of this section

---

[151] A. Beijer, R.J. Bokhorst., M. Boone, C.H. Brants, J.M.W. Lindeman. 'De Wet bijzondere opsporingsbevoegdheden-eindevaluatie.' (2004) *WODC-reeks onderzoek en beleid, 222.*
Spapens, T., Siesling, M., & Feijter, E. D. *Brandstof voor de opsporing* (2011). Boom Juridische uitgevers.
[152] Decision Investigation in an Automated Work (n 119); Article 126nba(8)(a)(b) DCCP
[153] *Kamerstukken II* 2015/2016 (n 27), p. 30; Decision Investigation in an Automated Work (n 119), p. 13
[154] ibid
[155] See article 24(1) and article 29(1) Decision Investigation in an Automated Work (n 119)
[156] ibid
[157] *Kamerstukken II* 2015/2016 (n 27), p. 31
[158] Article 5 Decision Investigation in an Automated Work (n 119); see also Decision, p. 17
[159] See article 152 DCCP
[160] Article 6 Decision Investigation in an Automated Work (n 119)
[161] Article 8 Decision Investigation in an Automated Work (n 119)
[162] Article 14-20 Decision Investigation in an Automated Work (n 119); Article 126nba(6) DCCP

is not to discuss all means to collect evidence. Instead, only those investigatory powers that can be used to directly address the previously discussed problems are discussed, after which their viability is critically assessed.

§3.2.1 Production order

The production order is a broad investigatory power. On the one hand, it enables the police to request *subscriber data*[163] and *traffic data*[164] from the electronic communication provider (think of the internet provider, social media provider, cloud provider). Through subscribers and traffic data, the police can identify the suspect and his automated work (think of a name, address, location, MAC-number, IP address).[165] On the other hand, *data other than subscriber and traffic data that is not content data* may be requested from anyone that has access to such data (think of a company, service provider, or third persons).[166] Here, one can think of payment details (credit card details, PayPal account) that could offer the police further information about the suspect.[167] Finally, the police may use the production order to request online service providers to submit *content data* such as voicemail and email (communications) or stored data that is located on an external server.[168] The production order counters anonymity on the network and paves the way to conduct further investigatory activities that require knowledge of the identity or location of the suspect.[169] Moreover, it solves the problem of criminals storing data on a cloud server because the provider may be requested to submit the data.

However, when the suspect connects to a hotspot or uses anonymization techniques such as TOR, the production order no longer proves effective. Public hotspots impede the police's ability to obtain information about the suspect because the requested subscribers' data will only provide clues about the owner of the hotspot, whereas the traffic data will belong to all the devices that used the hotspot, thereby making it difficult to pinpoint what data belongs to which user or automated work.[170] Moreover, TOR encrypts and anonymizes the internet traffic as a result of which data flows are not visible and cannot be traced back to a specific device or user.[171] While the anonymity caused by hotspots may be overcome by placing CCTV cameras at public hotspots to potentially identify the suspect, this is more intrusive than using the hacking powers and cannot be considered an alternative. A solution for TOR could meanwhile be collecting publicly available data on the Dark Web to identify the suspect.[172] However, in

[163] See article 126na: Subscriber data that may be requested are the name, address, city, postal code, number (this also includes email addresses and IP address) and the type of service that is provided
[164] See article 126n: Traffic data that may be requested are time, duration, used computer, services purchased and location data
[165] Article 126n and 126na DCCP
[166] Article 126nd DCCP
[167] Jan-Jaap Oerlemans 'Normering van digitale opsporingsmethoden.' (2017) *Research paper van de Faculteit Militaire Wetenschappen Nederlandse Defensie Academie*. p. 47
[168] Article 126ng(2) DCCP
[169] Think of article 125i (searching a place to secure data in a computer) article 125j DCCP (network search) article 126l DCCP (recording of communications), article 126m (intercepting telecommunications) for example.
[170] Chris Hoffman. 'Why you shouldn't host an open Wifi-Network without a password.' howtogeek (26 September 2016) <https://www.howtogeek.com/132925/htg-explains-why-you-shouldnt-host-an-open-wi-fi-network/> accessed 5 April 2020; *Kamerstukken II* 2015/2016 (n 27), p. 10-11
[171] *Kamerstukken II* 2015/2016 (n 27), p. 8
[172] Oerlemans 'Normering van digitale opsporingmethoden' (n 167), p. 17-18

the absence of any clues on the Dark Web, it appears that anonymity cannot be overcome and hacking may be the only solution.

Another problem is that data storage and communication providers are increasingly located abroad and the relevant data is often spread across various servers located in various countries.[173] Consequently, it may be difficult to pinpoint the location of the data (or provider) which is problematic, because in order to request such data, the location of the server on which the data is stored must be determined, something which is not always possible.[174]

Provided that the location can be determined, the police could directly request subscribers data from the foreign provider based on the Cybercrime Convention but in the case of content data, the service provider must provide its consent, whereas transparency reports and practical experience indicate that it is difficult to retrieve such data.[175] Another option could be a request for legal assistance to the national authority of the country in which the data is located.[176] The authority will assess the request and either deny or grant permission based on the local requirements.[177] However, this process takes a long time and only concerns stored data, whereas information regarding data in transit may also be relevant.[178] When the service provider does not provide its consent to produce traffic or content data, when the request for legal assistance is rejected, or when it is accepted but only concerns stored data whereas information concerning data in transit is also crucial, the police, therefore, does not have a reliable means to retrieve all relevant data.

Two alternatives to secure such data remain. On the one hand, a network search could be conducted, however, this does not prove fruitful as it may only be conducted in the Netherlands, while the police will often encounter encrypted data.[179] On the other hand, improving international cooperation and the pace and efficiency in which evidence is shared could be an option. Currently, negotiations regarding cross-border access to electronic evidence for judicial cooperation in criminal matters are occurring between the EU and the United States[180], and within the EU there exists a proposal for a regulation on European Production and Preservation Orders for electronic evidence in criminal matters.[181] If these negotiations and legislative proposals result in legislation that improves the efficiency of cross-border exchange of

[173] *Kamerstukken II* 2015/2016 (n 27), p. 11-12
[174] ibid
[175] Article 18b Cybercrime Convention (subscriber data); Article 32b Cybercrime Convention (content data)
Kamerstukken II 2015/2016 (n 27), p. 8-9
[176] *Kamerstukken II* 2015/2016 (n 27), p. 8-9
[177] ibid
[178] ibid
[179] *Kamerstukken II* 2015/2016 (n 27), p.12
[180] Recommendation and Annex to Recommendation for a council decision authorising the opening of negotiations in view of an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters COM(2019) 70 final, p.1;
[181] Proposal for a regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters COM (2018) 225 final;
See also Recommendation for a council decision authorizing the participation in negotiations on a second Additional Protocol to the Council of Europe Convention on Cybercrime COM (2019) 71 final

evidence, this may be an adequate alternative. For now, however, the hacking powers appear to be the only solution to ensure access to data stored on an external server.

§*3.2.2 Decryption order addressed to the internet or communication provider*

The police often encounter encrypted data when searching an automated work[182], when conducting an internet tap to intercept communications[183] or when requesting data via a production order.[184] These investigatory powers can only be used efficiently if the collected data can be decrypted. Decryption can be achieved via a decryption order that can be directed at anyone who can be reasonably expected to have the means or knowledge to decrypt the data.[185] In the case of stored encrypted data, one can think of directing the decryption order at the provider of the encryption program, whereas in the case of communications, the order could be directed at the internet or communication provider.[186]

However, achieving decryption may not always be easy. Firstly, the decryption order cannot be directed to the suspect because of the principle of self-incrimination, while the suspect will often be the only person to possess the correct key or password.[187] Secondly, while the decryption order could be directed at the provider, the provider may not be able to decrypt the data because the data has been separately encrypted by connected services (think of WhatsApp, TrueCrypt, Apple, Gmail) who have added an additional layer of security.[188] While a decryption order may be directed at these connected services, many service providers are located abroad (think of Facebook, Microsoft, Apple) and cannot be ordered to comply with the decryption order because they do not fall under Dutch jurisdiction.[189] Additionally, the providers may not fall under the definition of a public communication provider as a result of which they do not have to comply with the decryption order (think of Whatsapp, Skype).[190] Finally, even if the providers are willing to cooperate, achieving decryption may be impossible, especially when the latest encryption techniques are employed.[191] WhatsApp, for example, makes use of the unrecoverable encryption technique *end-to-end encryption* with '*perfect forward secrecy'* in which only the sender and the receiver of the message possess the correct private key because once the communication session ends, the public key is automatically discarded as a result of which not even provider can decrypt the message.[192] When the police, therefore, requests the

[182] Article 125i DCCP to search data located on a computer in a physical place, article 125j DCCP to search data located on a computer or a server elsewhere
[183] Article 126l and article 126m DCCP
[184] Article 126n and further DCCP
[185] The decryption order is based on article 125k(2) DCCP when the data was collected via a search of a place (article 125i DCCP) or network search (article 125j DCCP). When the encrypted data concerns data that was intercepted via an internet or email tap (article 126m DCCP), the legal basis for the decryption order will be article 126m(6) DCCP. Finally, in case of the production order, a decryption order can be based on article 126nh(1) DCCP.
[186] Oerlemans 'Normering van digitale opsporingmethoden' (n 167), p. 45-48
[187] *Kamerstukken II* 2015/2016 (n 27), p.8-9; see also article 125k(3) and article 126m(7) DCCP; Article 126nh(2) DCCP
[188] *Kamerstukken II* 2015/2016 (n 27), p.8-10
[189] ibid
[190] ibid
[191] ibid
[192] Lewis, Zheng & Carter (n 53), p, 5

provider to decrypt the message, this is technically impossible.[193] Similar observations can be made in case of encrypted data stored on an automated work. Open-source programs such as TrueCrypt and BoxCryptor use unbreakable encryption techniques and can, therefore, only be accessed with the correct password that is in the possession of the suspect[194] whereas Apple has stated that it cannot break the encryption techniques used for Apple devices that run iOS 11 or higher.[195] Considering this, the decryption order does not appear to be an alternative to the hacking powers as decryption cannot always be achieved.

§*3.2.3 Decryption order addressed to the suspect*

If the provider cannot decrypt the data, why not create a new investigatory power that allows the police to direct the decryption order to the suspect and in which noncooperation is penalized?[196] The idea to direct the decryption order to the suspect was originally part of the proposal for Computer Crime Act III but was disregarded by the legislator because the power would violate the right to not incriminate oneself.[197] Because the decryption order to the suspect would interfere with two key human rights (it would also violate the right to respect for private life), it is more intrusive than the hacking powers and cannot be considered an alternative.

§*3.2.4 Interception of communications by placing a technical tool inside a private place*

If decryption of data cannot be achieved, the investigatory power to intercept confidential communications through placing a technical tool inside a private place may be an option.[198] A bug could be placed on a keyboard or mouse of an automated work to register keystrokes or mouse-clicks, but it may also include the attaching of an eavesdropping device such as a microphone in a private place (living room, car).[199] Because keystrokes and mouse-clicks are registered, the police will know what the suspect is typing or clicking on.[200] Real-life communications can also be secured because through the placing of a microphone these communications may be intercepted.[201]

By using this investigatory power, the police can circumvent the encryption of (tele)communications because the communications are intercepted before they are sent (encrypted). If messages also contain passwords, these passwords are also intercepted which can later be used to access encrypted stored data on the automated work. Therefore, this investigatory power has similar functionality as hacking to intercept communications and to secure stored and future data and would appear to be a viable alternative.

---

[193] ibid
[194] Gildred (n 57)
[195] Kharpal, A. 'Apple vs. FBI: All you need to know.' CNBC (29 March 2016) <https://www.cnbc.com/2016/03/29/apple-vs-fbi-all-you-need-to-know.html> accessed 13 May 2020
[196] Bert-Jaap Koops. *Het decryptiebevel en het nemo-teneturbeginsel*. (2012). Boom Lemma., p. 174
[197] *Kamerstukken II* 2015/2016 (n 27), p. 6; see also article 6 ECHR
[198] Article 126l DCCP
[199] *Kamerstukken II* 1996/1997 (n 114), p. 35
[200] ibid
[201] ibid

The problem is that this power requires the placing of a physical technical tool inside a private place, whereas, in the case of hacking, malware is remotely installed on the computer which means that physical entry of a private place is not required.[202] Hacking can, therefore, be considered less intrusive. Moreover, when a bug is found, the suspect can easily discard it, while he simultaneously becomes aware of the fact that he is being surveilled which may result in the suspect destroying potential evidence.[203] A final shortcoming is that for the use of this power the location of the private place of the suspect must be known, which may not always be the case because of anonymization techniques, while it may also be difficult to determine at what location the bug should be placed.

§3.3 Conclusion

This chapter revealed that hacking may only be ordered in case of pre-trial detention crimes and specifically designated felonies that seriously breach the legal order, or in case of felonies with a minimum imprisonment of eight years. Moreover, only the public prosecutor may order the hacking, and only if the investigation urgently requires it. Furthermore, hacking may only be ordered for five investigatory activities, and only an automated work in use by the suspect may be hacked. Further safeguards and oversight mechanisms were also incorporated: the hacking order is subject to prior authorization of the investigative judge and the Board, and the hacking may only be ordered after prior examination by the CEC. During the hacking, oversight is exercised by the Inspectorate of Justice and Security. Further, once the hacking ends, the suspect must be notified, and ex-post oversight by the court is performed. Finally, Decision Investigation prescribes a functional separation of the tactical and technical team, logging obligations, and further operational requirements regarding the technical tool used to access the automated work and the subsequent data processing.

Moreover, it was established that there are no alternative and less intrusive investigatory measures available to the police to combat cybercrime because the investigatory powers that can be used are either more intrusive or cannot overcome the problems caused by the three technological developments.

[202] Article 126l(2) DCCP; See also *Kamerstukken II* 2015/2016 (n 27), p. 12-13
[203] ibid

Chapter IV: The right to respect for private life

This chapter explores how the three hacking powers interfere with the right to respect for private life in Article 8 ECtHR, and what conditions must be fulfilled according to ECtHR case-law for such powers to be necessary and proportionate. Firstly, the scope of the right to respect for private life is considered in relation to the use of these hacking powers (**§**4.1). Hereafter, the conditions that must be fulfilled for covert surveillance measures to be necessary and proportionate are discussed (**§**4.2). Finally, a conclusion is presented in which an answer to the third sub-question is provided (**§**4.3)

§4.1 Hacking and the right to respect for private life

The right to respect for private life is a qualified right that is enshrined in Article 8 of the ECHR which reads as follows:

> **ARTICLE 8 Right to respect for private and family life**
>
> 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

Whereas the first paragraph states that everyone has the right to respect for private life, the second paragraph contains a derogation clause that prescribes that an interference with the right to respect for private life by a public authority may nevertheless be justified provided that the interference is in accordance with the law and is necessary in a democratic society in the pursuit of one (or more) of the legitimate aims mentioned in the second paragraph. The right to respect for private life is thus not absolute - something that will further be discussed in §4.2.

To invoke the protection of the right to respect for private life, it must first be determined whether the hacking of an automated work by the police for investigation purposes falls within the scope of the right to respect for private life.[204] So far, the ECtHR has incorporated a wide range of topics within the scope of private life that can best be categorized in three broad categories: (i) privacy (think of surveillance and subsequent data collection, data protection, reputation rights), (ii) a person's physical, psychological and moral integrity (think of reproductive rights, environmental issues, sexual orientation), and (iii) identity and autonomy (think of the right to personal development, right to a name, gender identity).[205]

[204] Kilkelly, U. 'The right to respect for private and family life. *A Guide to the Implementation of Article 8*,' (2003) 200310-11. p.10.
[205] Council of Europe. 'Guide on Article 8 of the Convention – Right to respect for private and family life'. (31 December, 2019). p. 21

However, the ECtHR has not yet included the hacking of an automated work for investigation purposes within the scope of the right to private life.[206] Still, hacking may engage the concept of private life through its functionalities and subsequent data collection and storage as indicated by the ECtHR case-law below.

In *Copland v. the United Kingdom*, the ECtHR observed that the recording and interception of telephone conversations, e-mail, and personal internet use fall in the scope of private life and that the collection and subsequent storing of such data relating to one's private life constitutes an interference with these rights, irrespective of whether this data is used or disclosed.[207] When through hacking the microphone of an automated work is remotely activated to intercept conversations, or when through hacking a keylogger is activated to intercept or secure telecommunications this will, therefore, be covered by the notion of private life and constitute an interference thereof.[208]

From *Uzun v. Germany*, it further follows that GPS surveillance by the police is covered by the notion of private life and constitutes an interference thereof as location data is systematically collected, stored, and processed which reveals key information about the suspect's whereabouts and movements.[209] Likewise, in *Ben Faiza v. France*, the ECtHR determined that the installation of a geolocation device in a car and the subsequent request of cell tower pings by the police constituted an interference with the right to respect for private life.[210] When through the hacking of an automated work, a suspect's GPS or WIFI signal is remotely activated to collect and store location data to enable systematic observation, this will likely constitute an interference with the right to respect for private life.

Finally, in *Trabajo Rueda v. Spain*, the ECtHR notes that when the police access personal files stored on a computer via a search and seize power, this constitutes an interference with the right to respect for private life.[211] Although the search and seize power is generally an overt power, it seems logical that hacking in which access is covertly gained to data stored in an automated work via a remote search also falls within the scope of the right to respect for private life and will constitute an interference thereof. Important to distinguish, however, is that hacking may also concern a remote search that includes the securing of future data- data that enters the automated work after access has been obtained and is, therefore, more intrusive.

As these hacking powers are used, data is inevitably collected, stored, and subsequently processed by the police. It follows from *Leander v. Sweden* that the storage of data relating to the private life of an individual into a police file constitutes an interference with the right to respect for private life.[212] The ECtHR also affirmed this in *Amann v. Switzerland* and added

[206] Bert-Jaap Koops, Newell, B. C., Timan, T., Škorvanek, I., Chokrevski, T., & Galič, M. (2016). A typology of privacy. *U. Pa. J. Int'l L.*, *38*, 483, p. 518-520
[207] *Copland v. the United Kingdom* App no 62617/00 (ECtHR 3 April 2007) §41-44
[208] See also *Klass and others v. Germany* App no 5029/71 (ECtHR, 6 September 1978) §41; *Malone v. the United Kingdom* App no 8691/79 (ECtHR, 2 August 1984) §64, §84; *Halford v. the United Kingdom* App no 20605/92 (ECtHR, 25 June 1997) §44; *Amann v. Switzerland* App no 27798/95 (ECtHR, 16 February 2000) §44
[209] *Uzun v. Germany* App no 35623/05 (ECtHR, 2 September 2010) §49-53
[210] *Ben Faiza v. France* App no 31446/12 (ECtHR, 8 February 2018) §53-55, §66-68
[211] *Trabajo Rueda v. Spain* App no 32600/12 (ECtHR 30 May 2017) §32
[212] *Leander v. Sweden* App no 9248/81 (ECtHR, 26 March 1987) §48

that the subsequent use of data does not influence that finding.[213] Moreover, the ECtHR finds in *P.G. and J.H. v. the United Kingdom* and *Peck v. the United Kingdom* that the systematic collection and storage of data into a permanent record may give rise to private life considerations even when the data was collected from a public place or when the data is collected in a non-intrusive or overt way.[214]

The previous chapters indicated that when the police hack an automated work, private data such as conversations, e-mails, texts, stored data files, and location data are inevitably collected and subsequently transferred to an infrastructure (police file) by the technical police team. Applying these findings, the collection and storage of these private data will constitute an interference with the right to respect for private life.

ECtHR case-law further indicates that when data relating to the private life of an individual also concerns personal data (data that can lead to the identification of the suspect), a separate interference may be found if this data is further processed, irrespective of whether the data is disclosed to a third party.[215] Video footage, voice recordings, location data, police files, for example, enable the identification of the suspect, and since these data are processed by members of the tactical police team who will analyze this data for evidence, each processing activity constitutes a separate interference.

Finally, there also appears to be a movement to recognize the right to protect the confidentiality and integrity of computer systems as a new personality right that would fall in the scope of private life.[216] In Germany, for example, the Constitutional Court stated that since computers play a crucial role in personal development because they create new opportunities and threats for people, the right to personal development also incorporates the right to respect of confidentiality and integrity of computer systems.[217] Moreover, the Dutch legislator has stated that hacking an automated work will result in interference with the right to protect the integrity of a computer system, thereby acknowledging the existence of this right.[218] Arguably, an automated work stores and transmits more information than any other object. Through hacking, access to this data is covertly gained, and considering the protection that the ECtHR has granted to citizens in the case of police surveillance and data collection, storage, and processing, the creation of a new right seems to be a necessary step in ensuring optimal protection of citizens.

In short, although there is as yet no ECtHR case-law on whether hacking a computer to conduct investigation falls within the scope of the right to private life, existing case-law on police surveillance and subsequent data collection, storage and processing, and international developments in Germany and The Netherlands indicate that hacking to conduct investigation

---

[213] *Amann v. Switzerland* App (n 208) §69
[214] *P.G. and J.H. v. the United Kingdom* App no 44787/98 (ECtHR, 25 September 2001) §57-59
Peck v. the United Kingdom App no 44647/98 (ECtHR, 28 January 2003) §57-59;
[215] *S. and Marper v. The United Kingdom* App no 30562/04, 30566/04 (ECtHR 4 December 2008) § 103
See also *P.G. and J.H. v. the United Kingdom (n 214)* §59-60; *Copland v. the United Kingdom* (n 207) §42-44; *Leander v. Sweden* (n 212) §48
[216] Koops, Newell, Timan, Škorvanek, Chokrevski, & Galič (n 206), p. 518-520
[217] BVerfGE [Federal Constitutional Court] 27 February 2008, 1 BvR 370/07, ECLI:DE:BVerfG:2008:rs20080227.1bvr037007 (Ger.).§166 - 206.
[218] *Kamerstukken II* 2015/2016 (n 27), p. 52

will likely fall within the scope of the right to respect for private life and constitute an interference thereof.

§4.2 When is a restrictive measure necessary and proportionate?

The second paragraph of Article 8 of the ECHR states that an interference with the right to respect for private life may be justified if this is in accordance with the law (legality requirement) and if it is necessary in a democratic society in the pursuit of a legitimate aim (necessity requirement).[219] This section focuses on the necessity requirement and discusses what conditions must be fulfilled according to ECtHR case-law for a restrictive measure to be necessary and proportionate, particularly in the case of covert surveillance powers conducted by law enforcement. While the focus will be on police surveillance, ECtHR case-law regarding surveillance conducted by intelligence services will also be considered, because surveillance may also be conducted by special anti-terrorism task forces, semi-military police forces, and intelligence services of the police that represent a blurred line between regular police work and that of intelligence services. With that being said, it will be specified in the reference when surveillance is conducted by these special type of police or intelligence services. Finally, the legality requirement will only be considered where relevant in relation to the necessity requirement.

§*4.2.1 Necessity requirement*

ECtHR case-law shows that for an interference to be necessary in a democratic society, it must correspond to a pressing social need and be proportionate to the legitimate aim pursued.[220] A pressing social need exists when the restrictive measure is accompanied by a social interest that is so compelling that it gives the public authority no choice but to interfere with a fundamental right.[221] To this end, the public authority must bring forward relevant and sufficient arguments that prove the necessity of the measure.[222] Whether an interference is proportionate to the legitimate aim pursued is based on the facts and circumstances of an individual case in which the benefits of the application of the restrictive measure are reasonably balanced against the seriousness of the intrusion.[223]

Further, it follows from *Klass and others v. Germany* that powers of secret surveillance can only be allowed if they are *strictly* necessary to safeguard democratic institutions.[224] In *Szabó and Vissy v. Hungary* it is elucidated that the covert surveillance powers must be strictly necessary, both, as a general consideration, to safeguard democratic institutions, and as a

[219] Article 8(2) ECHR
[220] *Handyside v. the United Kingdom* App no 5493/72 (ECtHR, 7 December 1976) §48-49; *Sunday Times v. the United Kingdom* App no 6538/74 (ECtHR, 26 April 1979) §67; *Silver and others v. the United Kingdom* App no 5947/72; 6205/73; 7052/75; 7061/75; 7107/75; 7113/75; 7136/75 (ECtHR, 25 March 1983) §97.
[221] J.H. Gerards, *EVRM – Algemene leerstukken* (2011) The Hague: Sdu Uitgevers, p. 145;
[222] *Sunday Times v. the United Kingdom* (n 220) §62
[223] Jan-Jaap Oerlemans. *Investigating Cybercrime* (2017) Amsterdam University Press, p. 76-77
[224] *Klass and others v. Germany* App no 5029/71 (ECtHR, 6 September 1978) §42 **[in abstracto claim mass surveillance by the intelligence service]**

particular consideration, to obtain vital intelligence in an individual operation.[225] Finally, it follows from *Volokhy v. Ukraine* that the strict necessity test also applies in the context of covert police surveillance for criminal investigation purposes.[226]

Thus, in the case of police hacking, the public authority must conduct a general necessity test in which it is assessed whether the hacking powers correspond to a pressing social need and are proportionate to the legitimate aim pursued, and a particular necessity test in which it is assessed whether the particular hacking is necessary to obtain vital evidence. The particular necessity test appears to add an extra condition as it prescribes a subsidiarity test. That is, if vital evidence can be obtained in a less intrusive way and the same objective can be achieved, the hacking is not necessary and may not be ordered.

§*4.2.2 Margin of appreciation*

Klass and others shows that under *exceptional conditions* legislation granting secret surveillance powers to a public authority may be necessary to safeguard democratic institutions in the interest of national security or the prevention of disorder and crime.[227] To this end, Contracting States have a certain margin of appreciation regarding the imposition of the secret surveillance powers but this margin is not unlimited.[228] Because secret surveillance powers can destroy democracy under the cloak of defending it, there must be adequate and effective guarantees against abuse.[229] Oerlemans states in this regard that the more serious the privacy interference is, the more procedural safeguards will be required to avoid abuse of power by a public authority.[230] Since police hacking is a form of covert surveillance that will inevitably represent a serious interference with the right to respect for private life, the presence of adequate and effective guarantees against abuse will be crucial when assessing whether the interference is proportionate to the legitimate aim pursued. The margin of appreciation doctrine thus provides a framework to assess the proportionality of the hacking powers.[231]

§*4.2.3 Minimum safeguards*

The ECtHR state in *Klass and others* that whether there are adequate and effective measures against abuse depends on the circumstances of the case and is assessed by, inter alia, the nature, scope, and the duration of measures, the grounds required for ordering them, the authorities legible to authorize, conduct and supervise them, and the remedies provided for by national law.[232] Moreover, the ECtHR in *Weber and Saravia v. Germany* developed minimum

---

[225] *Szabó and Vissy v. Hungary* App no 37138 /14 (ECtHR, 12 January 2016) §72-73 **[mass surveillance by the anti-terrorism police task force]**
[226] *Volokhy v. Ukraine* App no 23543/02 (ECtHR, 2 November 2006) §43
[227] *Klass and others v. Germany* (n 208) §48; *Malone v. the United Kingdom* (n 208) § 81
[228] *Silver and others v. the United Kingdom* (n 220) §97; *Handyside v. the United Kingdom* (n 220) §49; *Klass and others v. Germany* (n 208) §48-50
[229] ibid §49-50
[230] Oerlemans 'Investigating Cybercrime' (n 223), p. 77
[231] Ivana Roagna. *Protecting the right to respect for private and family life under the European Convention on Human Rights*.(2012) Council of Europe human rights handbooks, p. 45
[232] *Klass and others v. Germany* (n 208) §50; *Roman Zakharov v. Russia* App no 47143/06 (ECtHR 4 December 2015) §232-233 **[in abstracto claim mass surveillance by the intelligence service]**

safeguards that must be present in statute law to avoid abuse of power in the case of covert interception by secret intelligence services which were later strengthened in *Roman Zakharov v. Russia*.[233]

However, these minimum safeguards were developed in the context of secret surveillance executed by intelligence services. Although it follows from *Khan v. the United Kingdom* that there must be a measure of legal protection in domestic law against arbitrary interference by a public authority in the case of police surveillance[234], the ECtHR does not yet seem to apply the minimum safeguard threshold prescribed by *Weber and Saravia* and *Roman Zakharov* when assessing the necessity and proportionality of covert police powers.

Nevertheless, ECtHR case-law on police surveillance gives an indication of the safeguards that must be considered. In *Kruslin v. France, Volokhy v. Ukraine*, and *Ekimdhiez v. Bulgaria*, for example, the ECtHR attached value to presence or absence of the following safeguards against abuse: an indication of the people liable to be subjected to the restrictive measure by the order, the nature of the offenses and the circumstances that may give rise to such an order, the time limits on the duration of the restrictive measure (are they fixed and respected?), and the supervision or authorization structures in place.[235] These safeguards appear to overlap to a large extent with the minimum safeguards prescribed by *Weber and Saravia* and *Roman Zakharov* for covert surveillance conducted by intelligence services.[236]

Yet, in *Uzun v. Germany*, the ECtHR rejected the applicability of such strict safeguards in the case of GPS surveillance by the police because it considered such surveillance to interfere less with the right to respect for private life than the interception of communications.[237] Instead, the ECtHR applied the more generic assessment as prescribed by *Klass and others* in which it found no violation of the right to respect for private life, particularly because judicial review was present in the subsequent criminal proceedings – the latter offering sufficient protection against arbitrariness.[238]

From all of the above, it follows that the type of police surveillance and the extent of the subsequent interference with the right to respect for private life influences the type of safeguards that must be present to meet the condition of adequate measures against abuse. Considering that the hacking provision grants the police a set of far-reaching powers that could result in highly

[233] The minimum safeguards relate to the accessibility of the law, the scope of application of the secret surveillance measures, the duration of the measures, the procedures to be followed for storing, accessing, examining, using, communicating and destroying intercepted information, the authorization procedures, the arrangements for supervising the execution of the secret surveillance and the notification mechanisms and remedies provided for by national law
See *Weber and Saravia v. Germany* App no 54934/00 (ECtHR, 29 June 2006) §95 **[in abstracto claim mass surveillance by the intelligence service]** and *Roman Zkaharov v. Russia* (n 232) §238
[234] *Khan v. the United Kingdom* App no 35394/97 (ECtHR, 12 May 2000) §26
[235] *Kruslin v. France* App no 11801/85 (ECtHR, 24 April 1990) §34-35 **[targeted surveillance by the semi-military police force];** *Volokhy v. Ukraine* (n 226) §51-53; *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria* App no 62540/00 (ECtHR, 28 June 2007) §79-84 **[in abstracto claim mass surveillance by the intelligence and police services]**
[236] See *Weber and Saravia v. Germany* (n 233) §95 and *Roman Zkaharov v. Russia* (n 232) §238
[237] *Uzun v. Germany* (n 209) §65-66
[238] ibid §63-72

intrusive covert surveillance of the subject in the pursuit of crime prevention, and because such secret powers were previously only held by secret services in the pursuit of combatting terrorism or espionage, it could be argued that the minimum safeguards as put forward in *Roman Zakharov* should equally apply in the case of police surveillance, particularly in the absence of a single or coherent set of rules for police surveillance other than the broad assessment prescribed by *Klass and others.*

§*4.2.4 Supervisory control*

Three important themes can be identified in ECtHR case-law concerning supervisory control of secret surveillance: the bodies that conduct oversight, the moments of oversight, and the mandate of the bodies that conduct oversight.[239]

Regarding the bodies that may conduct oversight, the ECtHR has repeatedly stated that oversight on covert surveillance powers must be exercised by a body that is independent of the executive power.[240] Here, judicial control is favored, at least in the last resort, because this ensures independence, impartiality, and an adequate procedure.[241] Importantly, it follows from *Dmitru Popescu v. Romania* that the public prosecutor cannot be considered to be sufficiently independent of the executive power.[242] Moreover, the ECtHR has emphasized the value of oversight conducted by an independent board elected by parliament, an independent commission, parliamentarians on the National Police Board, a Parliamentary Ombudsman, and a Parliamentary Committee of Justice.[243]

Concerning the moments of oversight, it follows that review can take place at three instances: when surveillance is first ordered, while it is carried out, or after it has been terminated.[244] In *Kruslin,* for example, the ECtHR attached value to the prior judicial authorization by the investigative judge and the subsequent supervision of senior police officers executing the interception order, while the judge was also subjected to judicial supervision by the higher courts.[245] Meanwhile, in *Volokhy*, the ECtHR disapproved of the fact that even though review was present in the first stage when the prosecutor ordered the interception, there was no subsequent interim review of the interception order when it was carried out by law enforcement, and in the absence of any judicial oversight on the interception procedures of law enforcement, the ECtHR noted that the oversight was insufficient.[246] Finally, from *Ekimdzhiez,* it follows that even if prior judicial authorization is present, the absence of independent review on law enforcement's implementation of the covert power or the absence of judicial review afterward

---

[239] S. J. Eskens, O.L. van Daalen, N.A.N.M van Eijk, N. A. N. M. Geheime surveillance en opsporing: Richtsnoeren voor de inrichting van wetgeving (2016), *Instituut voor informatierecht.* p. 15
[240] *Klass and others v. Germany* (n 208) §21, §55-56; *Ekimdzhiez v. Bulgaria (n 235)* § *Volokhy v. Ukraine* (n 226) §*52; Kruslin v. France* (n *235)* §*34; Szabó and Vissy v. Hungary* (n 225) §77
[241] *Klass and others v. Germany* (n 208) §55-56; *Ekimdzhiez v. Bulgari (n 235)* §87; *Volokhy v. Ukraine* (n 226) §*52; Kruslin v. France* (n *235)* §*34*; *Szabó and Vissy v. Hungary* (n 225) §77
[242] *Dmitru Popescu v. Romania* App no 71525/01 (ECtHR, 26 April 2007) §70-71 **[mass surveillance by the intelligence service]**
[243] *Klass and others v. Germany* (n 208) §56; *Leander v. Sweden* (n 212) §60-67; *Ekimdzhiev v. Bulgaria* (n 235) §87
[244] *Klass and others v. Germany* (n 208) §55-56; *Roman Zakharov v. Russia* (n 232) §233
[245] *Kruslin v. France* (n 235*)* §*34*
[246] *Volokhy v Ukraine* (n 226) §53-54:

means there are no sufficient guarantees against risk of abuse.[247] Considering this, and considering the intrusive character of hacking, it would seem that oversight in all three stages is thus desirable.

Because of the secret nature of surveillance, oversight in the first two stages can only be conducted without the individual's knowledge.[248] Since this prevents the individual from being able to seek remedy, adequate safeguards that enable the individual to seek remedy after the surveillance has been finished must be present.[249] A notification obligation in which the citizen is informed that he has been subjected to covert surveillance can serve as an important safeguard because this enables citizens to exercise their right to respect for protect private life and to challenge unlawfulness of secret surveillance powers in front of an independent judge.[250] Another safeguard may be the ability to submit a complaint to a judge or independent commission about any perceived wrongdoings.[251]

Concerning the mandate of the bodies that conduct oversight, it is not only crucial that oversight is conducted, but also that this occurs effectively. The oversight body must be able to examine the lawfulness and necessity of the covert surveillance and this must not only be prescribed by law but occur in practice.[252] To this end, the ECtHR expresses in *Szabó and Vissy* that control by an independent body, normally a judge with special expertise, should be the rule and substitute solutions the exception warranting scrutiny.[253] Lack of specialized knowledge or relevant information undermines the ability of the supervisory authority to effectively conduct oversight and must be considered when examining the effectiveness of supervision.[254] Moreover, effective control can only be exercised if the body that conducts review can prevent or end unlawful behavior via a legally binding decision.[255] This also applies to ex-post oversight in which the court must be able to judge on the lawfulness and necessity of the measure, and must be able to offer compensation or be able to exclude evidence in the case it is established that the right to respect for private life was breached.[256]

Finally, it follows from *Dragojević v. Croatia* that the authorizing judicial body must present a compelling justification for authorizing measures of secret surveillance in which a detailed statement on the lawfulness, necessity, and proportionality of the measure is required.[257] From *Hambardzumyan v. Armenia*, it further follows that there cannot be effective judicial authorization if the warrant is described in a vague and non-specified manner.[258]

---

[247] *Ekimdzhiev v. Bulgaria* (n 235) §85-93
[248] *Klass and others v. Germany* (n 208) §55
[249] ibid
[250] *Klass and others v. Germany* (n 208) §57-58; *Szabó and Vissy v. Hungary* (n 225) §86; *Ekimdzhiez v. Bulgaria* (n 235) §90-91 *Uzun v. Germany* (n 209) §65-66; *Kruslin v. France* (n 235) §34
[251] *Ekimdzhiez v. Bulgaria* (n 235) §100
[252] *Klass and others v. Germany* (n 208) §53; *Szabó and Vissy v. Hungary* (n 225) §71-73; *Volokhy v Ukraine* (n 226) §52 *Roman Zakharov v. Russia* (n 232) §260-267; *Uzun v. Germany* (n 209) §71
[253] *Szabó and Vissy v. Hungary* (n 225) §77
[254] See *Roman Zkaharov v. Russia* (n 232)
[255] *Roman Zkaharov v. Russia* (n 232) §282; *Klass and others v. Germany* (n 208) §53
[256] *Dragojević v. Croatia* App no 68955/11 (ECtHR, 15 January 2015) §99; *Ben Faiza v. France* (n) §73
[257] *Dragojević v. Croatia* (n 256) §51-59
[258] *Hambardzumyan v. Armenia* App no 43478/11 (EctHR, 5 December 2019), §65-67

§4.3 Conclusion

This chapter found that through the use of the three hacking powers, private data such as (tele)communications, location data, and stored and future data are collected and subsequently processed which inevitably constitute various interferences with the right to respect for private life. Moreover, it was established that for a covert surveillance power to be necessary and proportionate, it must pass the strict necessity test, meaning the hacking power must be necessary in a democratic society in general, and be concretely necessary to obtain vital intelligence. States further have a certain but not unlimited margin of appreciation regarding the imposition of secret surveillance powers. Therefore, a restrictive measure can only be proportionate if there are effective and adequate measures against abuse. These safeguards were discussed, and it was concluded that in the absence of a single set of rules for police surveillance, and considering the intrusive nature of hacking, the minimum safeguards as prescribed by *Roman Zakharov* should apply alongside the more general assessment of *Klass and others*.

Chapter V: Necessity and proportionality of the hacking powers

This chapter examines whether, considering the various safeguards identified in sub-question 2 and the conditions for necessity and proportionality identified in sub-question 3, the three hacking powers can be considered necessary and proportionate tools for evidence gathering by the police to combat cybercrime. Firstly, it is assessed if the hacking powers correspond to a pressing social need, using the insights of the previous chapters (§5.1). Hereafter, it is examined whether the hacking powers are also proportionate by critically assessing whether the legal framework surrounding the hacking powers contain effective and adequate guarantees against abuse (§5.2). Finally, the benefits of the application of the hacking powers are balanced against the extent of the interference with the right to respect for private life, and an answer to the final sub-question is provided (§5.3)

§5.1 Do the hacking powers correspond to a pressing social need?

The hacking provision was created to fill a gap in present investigatory powers caused by three technological developments: the encryption of electronic data, cloud computing, and wireless networks (see §2.1). Perpetrators use encryption to prevent the police from accessing data that has been secured or intercepted via traditional investigatory powers. Cloud computing enables criminals to store data on various external servers located outside one's network which hampers the police's ability to locate, gain access to, and retrieve such data. Finally, wireless networks such as hotspots are used by perpetrators to remain anonymous on the network and hamper the ability of the police to intercept relevant data. Because present investigatory methods and powers are inadequate to solve the issues arising from these technological developments, and considering that there are no alternative and less intrusive investigatory powers available to the police to solve this issue, the police cannot always obtain access to the data required to prosecute and prevent cybercrime (see §3.2). Consequently, access to vital evidence required for the effective prevention and prosecution of the crime is hampered, if not made impossible, which is problematic because if there are no effective investigatory tools, cybercrime cannot be prevented and offenders cannot be brought to justice. Instead, criminals roam around freely on the internet and this significantly undermines the legal order. There is a pressing social need to close this gap in order to regain access to such data to ensure the effective prevention and prosecution of cybercrime.

It was established that by hacking an automated work to intercept confidential communications, the police can circumvent the encryption of such communications, for example, by installing a keylogger or by remotely activating the microphone. Moreover, access to encrypted stored data files can be obtained by hacking an automated work in order to secure existing and future data as via a keylogger decryption keys and login details may be obtained. Such details can also be used to gain access to a cloud account as a result of which access may be obtained to data that is stored elsewhere. Finally, future data may be secured before it is encrypted or stored in the cloud (see §2.2). These hacking powers, therefore, overcome the problems for criminal investigation caused by encryption and cloud computing as access to crucial evidence is

regained. These hacking powers can thus be said to correspond to the identified pressing social need.

However, the same cannot be said about hacking an automated work in order to conduct systematic observation. While remote activation of a GPS or WIFI signal may undoubtedly be useful, it is unclear how this hacking power corresponds to the problems and subsequent pressing need arising from encryption, cloud computing, and wireless networks. Besides, when the suspect makes use of GPS spoofing, this hacking power will not prove effective as wrongful location data is sent.[259] This hacking power is, therefore, both ineffective and unnecessary. Because this hacking power cannot be considered necessary, its proportionality will not be considered below.

§5.2 Does the legal framework surrounding the hacking powers contain effective and adequate guarantees against abuse?

The previous section found that the hacking to intercept communication and hacking to secure stored and future data correspond to a pressing social need. This section examines whether these hacking powers can also be deemed proportionate by examining whether the legal framework surrounding these hacking powers contain effective and adequate measures against abuse.

§5.2.1 Grounds

Powers of secret surveillance may only be ordered in case of suspicion of a serious criminal act.[260] With the creation of the *Special Investigatory Powers Act*, the legislator already incorporated this requirement in the standard ground that is used for the most intrusive powers.[261] Such powers may only be used in the case of pre-trial detention crimes that result in a severe breach of the legal order.[262] Considering the intrusive character of hacking, this standard was also used for hacking to intercept communications.[263] Nevertheless, a stricter standard applies in the case of hacking to secure stored data and future data as such hacking may only be ordered in the case of felonies with a minimum imprisonment of eight years or specifically designated felonies by governmental decree that seriously breach the legal order.[264] This distinction of grounds is commendable because previous analysis of the hacking powers indicated that this latter hacking functionality can be considered the most comprehensive and intrusive functionality (see §2.2.4).

Although the use of the hacking powers is restricted to serious crime, it would appear that these grounds are still rather broad, with the type of crimes ranging from minor assault and drug

[259] Mukthar Ahmad., Farid, M. A., Ahmed, S., Saeed, K., Asharf, M., & Akhtar, U. (2019, January). Impact and detection of GPS spoofing and countermeasures against spoofing. In *2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET)* (pp. 1-8). IEEE.
[260] *Klass and Others v. Germany* (n 208) §51; *Roman Zakharov v. Russia* (n 232) §260
[261] *Kamerstukken II* 1996/1997 (n 114) p. 23
[262] ibid
[263] Article 126nba(1)(b) DCCP
[264] Article 126nba(1)(d) DCCP; *Kamerstukken II* 2015/2016 (n 27), p. 29

crimes to the possession of child pornography.[265] Indeed, it would appear that restricting the use of the hacking powers to organized crime, terrorism, and life-threatening cases only would have been more desirable.[266] Also, when the decryption order was proposed alongside the hacking power as part of Computer Crime Act III, the legislator restricted the grounds of use of the decryption order to combatting terrorism and cybercrime only.[267] One may wonder, therefore, why the chosen ground regarding the nature of the crime for the hacking powers is broader, particularly considering their highly intrusive character.

Nevertheless, the legislator restricted the application of the hacking powers by subjecting the hacking to the safeguard that the felony must result in a severe breach of the legal order.[268] Not every suspicion of a felony may, therefore, justify the use of the hacking powers. However, because the assessment of whether a felony results in a severe breach of the legal order is based on the severity of the facts and circumstances under which the crime has been committed, this ground is open for interpretation. This is unfortunate because the facts and circumstances can be interpreted in different ways, thereby reducing foreseeability of the conditions under which hacking can be used.[269]

A final criticism is that the felonies for which hacking to secure stored and future data may be employed are not only determined in the DCCP but may also be designated by a governmental decree. Therefore, the guarantee provided by the legislator that the use of the hacking power to secure future and stored data will be limited to serious (cyber)crimes is undermined because a governmental decree can be amended much easier and quicker by the government since such amendment does not require the approval of the parliament as a result of which new crimes may be added to this list.[270] While this may be the case, it is important to note that states are not required to set out exhaustively by name the specific offenses which may give rise to the hacking because such crimes may vary in character and may be difficult to define in advance.[271] This is precisely what the legislator noted as he stated that designating such cybercrimes via a legal provision in the DCCP would be too limiting considering the fast-changing environment of cyber criminality.[272] It would thus seem that the nature of the crimes is sufficiently defined by the law, thereby providing adequate guarantees against abuse.

[265] See Article 67(1) jo. article 300(1) DCCP jo. article 240b DCCP; article 11 Opium law; See also Dian Brouwer; DBA Representative, in J. Kraan. 'Veel kritiek op voorgestelde hackbevoegdheid voor politie.' *NU* (11 February 2016) <https://www.nu.nl/internet/4213037/veel-kritiek-voorgestelde-hackbevoegdheid-politie.html> accessed 14 April 2020
[266] Jacob Kohnstamm; Dutch Data Protection Authority Representative, cited in Joost Schellevis and Nando Kasteleijn, 'Forse kritiek op hackbevoegdheid politie' *NOS* (11 February 2016) <https://nos.nl/artikel/2086191-forse-kritiek-op-hackbevoegdheid-politie.html> accessed 18 February 2020
Nederlandse Orde van Advocaten (n 39), §2.7-2.13
[267] *Kamerstukken II, 2015/2016,* 34372, nr. 4. p. 25
[268] Article 126nba(1) DCCP
[269] Bits of Freedom (n 39) p. 4
[270] Decision Investigation in an Automated Work (n 119), p. 27
[271] *Roman Zakharov v. Russia* (n 232) §244-247
[272] Decision Investigation in an Automated Work (n 119), p. 26-27

§5.2.2 Scope

The scope of the hacking powers and the manner of their exercise must be clearly defined by law.[273] It follows that covert surveillance powers may only be ordered against a suspect or against people that are not suspects but that may have knowledge about the crime.[274] The hacking powers meet this condition since they may only be ordered in the case of *felony conducted by a suspect* and only *an automated work in use by the suspect* may be hacked.[275] Nevertheless, this latter condition is ambiguous because this does not only incorporate the suspect's automated work but may include any automated work that the suspect uses more or less regularly (think of the computers of friends, co-inhabitants, and relatives or other third parties).[276] The automated works of third parties that are not involved may, therefore, be hacked.[277] Nevertheless, precisely the fact that suspects do not always work from their computers may necessitate the hacking of such automated works, but it can only be proportionate if further safeguards are incorporated.

Accordingly, one of the safeguards incorporated is that hacking may only be ordered by the public prosecutor if it is urgently required for the criminal investigation, a condition that prescribes a proportionality and subsidiarity test (see §3.1). Through this test, hacking is only ordered if strictly necessary and the scope is thus further restricted, however, it is important to remember that the public prosecutor cannot be deemed a sufficiently independent authority.[278] Prior authorization is, therefore, crucial in ensuring adequate and effective guarantees against abuse – something that will be further discussed in §5.2.5.

The scope is further restricted by limiting the hacking to five predefined investigatory activities that are exhaustively mentioned.[279] However, all of the special investigatory powers that can be found in Title IVA have been combined into a single provision, and once access is gained to the automated work, the police can use an unlimited amount of functionalities as a result of which access to a large amount of data is obtained that may not be required for the investigation.[280] While it may be true that the hacking provision provides the police with a set of far-reaching hacking powers that can be used for various functionalities, their use is nevertheless limited. Firstly, the hacking powers are subject to an order of the public prosecutor and subsequent authorization by the investigative judge, with every special investigatory activity that is conducted requiring a separate order.[281] Secondly, the hacking order clearly describes the nature and functionality of the technical tool in relation to the investigatory activity for which it is ordered, the part of the automated work that is targeted, and the category

[273] *Malone v. the United Kingdom* (n 208) §67-68; *Kruslin v. France* (n 235) §35-36; *Uzun v. Germany* (n 209) §61; *Volokhy v. Ukraine* (n 226) §54; *Roman Zakharov v. Russia* (n 232) §247
[274] *Klass and Others v. Germany* (n 208) §51; *Roman Zakharov v. Russia* (n 232) §243-245; *Kruslin v. France* (n *235)* §34-35; *Volokhy v. Ukraine* (n 226) §51-53; *Ekimdzhiez v. Bulgaria* (n *235)* §79-84
[275] Article 126nba(1) DCCP
[276] Škorvánek, Koops, Newell, Roberts (n 58), p.19
[277] Bits of Freedom (n 39), p. 3. ,p. 5
[278] *Dmitru Popescu v. Romania* (n 242) §70-71
[279] See article 126nba(1)(a-e) DCCP
[280] Bits of Freedom (n 39) p. 6
[281] Article 126nba(4) DCCP; *Kamerstukken II*, 2015/2016 (n 27*)* p. 19;

of data that may be secured.[282] This, in combination with the fact that the functionalities that are used in the pursuit of a certain investigatory activity are technically limited by the software that is used to secure such data, prevents the police from using an unlimited amount of functionalities in which a disproportionate amount of data is secured as a result of which the scope is restricted.[283]

Finally, concerns were raised regarding the broad notion of an automated work.[284] As seen, an automated work incorporates an undefined amount of computers and computer networks such as desktops, servers, modems, routers, smart devices, tablets, pacemakers, televisions et. Cetera.[285] This reduces the foreseeability of the scope of the hacking power, however, it would appear that this technologically neutral formulation is desirable considering the technological turbulence the legislator is increasingly confronted with.

§5.2.3 Duration

The hacking may be ordered by the public prosecutor for a maximum period of four weeks, after which the hacking order can be prolonged for blocks of four weeks indefinitely.[286] When the hacking encompasses the intercepting of communications, a separate order from the public prosecutor and subsequent authorization by the investigative judge is required in which the time limit is similarly set on four weeks with a possibility for prolongation for blocks of four weeks, indefinitely.[287] Any prolongation is subject to an authorization of the investigative judge, who assesses the necessity and subsidiarity of the hacking order, thereby limiting the duration of the hacking to what is strictly necessary.[288] If the investigative judge decides that the hacking is no longer necessary, she can refuse authorization in a legally binding decision, terminate the hacking order, or give the public prosecutor a deadline to end the investigation, thereby ensuring optimal and effective protection of citizens.[289] There is thus a fixed period that is adhered to, and it is also clear under what conditions the hacking order can be prolonged or terminated.[290] Nevertheless, it would be desirable to include a final deadline on the maximum period of extensions.

[282] Article 126nba(2)DCCP
[283] Article 8, 9, 23(2) Decision Investigation in an Automated Work (n 119)
[284] Bits of Freedom (n 39), p. 5;
College Bescherming Persoonsgegevens 'Consultatie conceptwetsvoorstel Computercriminaliteit III' (17 February 20140) <https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/z2013-00349.pdf> accessed 10 August 2020, p. 8;
Dutch Bar Association Representative, cited in Joost Schellevis and Nando Kasteleijn, 'Forse kritiek op hackbevoegdheid politie' *NOS* (11 February 2016) <https://nos.nl/artikel/2086191-forse-kritiek-op-hackbevoegdheid-politie.html> accessed 18 February 2020
[285] *Kamerstukken II* 2015/2016 (n 27), p.86
[286] Article 126nba(3) DCCP
[287] See article 126l and article 126m DCCP (intercepting and recording communications)
[288] *Kruslin v. France* (n *235)* §34-35; *Volokhy v. Ukraine* (n 226) §51-53; *Ekimdzhiez v. Bulgaria* (n *235)* §79-84
[289] *Klass and Others v. Germany* (n 208) §53; *Roman Zakharov v. Russia* (n 232) §282;
[290] *Klass and Others v. Germany* (n 208) §52; *Kruslin v. France* (n 235) §34-35; *Volokhy v. Ukraine* (n 226) §51-53; *Ekimdzhiez v. Bulgaria* (n 235) §79-84

§5.2.4 Procedures for storing, accessing, examining, using, communicating and destroying intercepted information

After the data has been secured via hacking, it is automatically stored on the infrastructure of the technical team.[291] Only the technical team can access the data and any change to the content is automatically detected.[292] The technical team transfers the results to the tactical team who further processes the data.[293] To prevent tunnel view in the assessment of such data, there is a separation between the technical team and the tactical team which ensures the reliability and objectivity of the investigation.[294]

Moreover, because the technical infrastructure contains personal data that is further processed, the *Police Data Act* applies.[295] In the case of data processing for criminal investigation purposes in light of upholding the legal order, such data must be deleted if they are no longer necessary for the investigation but may be processed for half a year if the data results in the start of a new criminal investigation after which it must be deleted.[296] Once deleted, the police data will be retained for a period of five years to handle complaints and to account for transactions after which they are permanently destroyed.[297] For police reports, a *lex specialis* rule applies which prescribes that once two months have exceeded after the termination of the criminal investigation or after the notification, the public prosecutor must delete such data.[298] As such, there is a clear and adequate procedure for storing, accessing, examining, using, and communicating, and destroying the intercepted information.[299] One may wonder, however, whether the retention period of five years is proportionate, particularly when no criminal indictment is initiated.

§5.2.5 Authorization procedure and arrangements for supervising the execution

The public prosecutor can only issue a hacking order to the police (executive power) if prior written authorization from the investigative judge (judicial power) is obtained, with every special investigatory activity requiring a separate order of the public prosecutor and subsequent authorization of the investigative judge.[300] Via prior authorization, ex-ante oversight by an independent judicial body is ensured, thereby reducing the risk of potential abuse of powers by

[291] Article 13(1), 27(1) Decision Investigation in an Automated Work (n 119); see also p. 16
[292] Article 7 Decision Investigation in an Automated Work (n 119); see also p. 16
[293] Article 24(1) and 29(1) Decision Investigation in an Automated Work (n 119)
[294] *Kamerstukken II* 2015/2016 (n 27), p. 31
[295] *Police Data Act* as amended by Council Directive 2016/680/EU 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 [2016] OJ *J L119/4.5*
[296] Article 9(4) *Police Data Act*
[297] Article 14(1) *Police Data Act*
[298] Article 126nba(6) jo. 126cc DCCP
[299] *Roman Zakharov v. Russia* (n 232) §250-254
[300] Article 126nba(4) in relation with article 126l and 126m DCCP

the executive power.[301] The reliability of such oversight is increased by the fact that the public prosecutor's hacking order is subject to various information requirements as a result of which the investigative judge can adequately assess whether the hacking order is lawful and meets the conditions of proportionality and subsidiarity.[302] The investigative judge's authorization further contains motivation regarding why the hacking is necessary and must also define the period for which the authorization is granted.[303] Prior authorization by the investigative judge is a strong safeguard because it avoids the investigative judge from rubber-stamping authorizations and increases transparency in the case of ex-post oversight conducted by a criminal court.[304]

Nevertheless, one may wonder whether such prior oversight can always be effectively conducted. Beijer et al. found, for example, that the investigative judge rarely refuses to grant authorizations because the investigative judge assumes that the lawfulness of special investigatory powers will be challenged in front of the criminal court.[305] Moreover, Bits of Freedom and the Dutch Bar Association have suggested that prior authorization is just a formality, as the figures on the police's use of the internet tap indicate the ease with which authorizations are granted.[306] As such, ex-ante oversight may not be effective in practice.[307] Another issue is that the proportionality and subsidiarity of the hacking can only be adequately assessed if the investigative judge has the special expertise required to assess the technical dangers associated with the hacking.[308] While there are various ways for the public prosecutor and the investigative judge to obtain such expertise, for example, by appointing an expert or attending training in a special knowledge center for cybercrime prevention, the legislator states that most public prosecutors and investigative judges lack the technical expertise required to conduct such an assessment.[309] Still, it would appear that with adequate training, special cybersecurity investigative judges can be used to achieve effective oversight and thereby restrict the use of the hacking powers to what is strictly necessary.

Oversight is further strengthened by the fact that the public prosecutor must notify the Central Examination Committee (hereafter: CEC)[310] of his intent to issue a hacking order and obtain prior written authorization from the Board of the Public Prosecutor's Office. As previously seen, the Board does not grant or deny authorization until CEC has issued advice based on a strict and thorough assessment of the hacking order. This procedure only applies to a limited amount of investigatory powers, and by subjecting the hacking powers to this procedure,

[301] *Klass and Others v. Germany* (n 208) §21, §55-56, *Ekimdzhiez v. Bulgaria (n 235)* §84, *Volokhy v. Ukraine* (n 226) §52, *Kruslin v. France (n235)* §34, *Szabó and Vissy v. Hungary* (n 225) §77; *Roman Zakharov v. Russia* (n 232) §259

[302] See article 126nba(2) DCCP that lists them exhaustively

[303] Article 126nba(4) DCCP; *Roman Zakharov v. Russia* (n 232) §260-262;

[304] *Dragojević v. Croatia* (n 256) §51-59; *Hambardzumyan v. Armenia (n 258)* §*65-67;* Eskens et. al (n 239) p.36;

[305] Beijer et. al (n 151), p. 193; N. van Buiten, 'De modernisering van de Wet BOB – Herinneren we ons de IRT-affaire nog?', DD 2016/10, afl. 3, p. 130-144, p. 142; Eskens et. al (n 239) p. 32

[306] Nederlandse Orde van Advocaten (n 39), §2.7; Bits of Freedom (n 39), p. 4,

[307] *Klass and Others v. Germany* (n 208) §53, *Szabó and Vissy v. Hungary* (n 225) §71-74, *Volokhy v. Ukraine* (n 226) §52, *Roman Zakharov v. Russia* (n 232) §260-267; *Uzun v. Germany* (n 209) §71

[308] *Szabó and Vissy v. Hungary* (n 225) §77;

[309] Article 176 DCCP; *Kamerstukken II* 2015/2016 (n 27), p. 33, 39

[310] As seen in 3.1.2, the CEC is an internal advisory body consisting of members of the police and the public prosecution body.

additional oversight is added in the first stage which is commendable. However, because CEC and the Board are part of the executive power (the public prosecutor's office and the police), this oversight is internal.[311] It may, therefore, be desirable to introduce an external chairman and (partial) staffing containing external experts in the field.[312]

Moreover, while the legislator stated that the Board would be requested to amend the *Instruction Investigatory Powers* to include hacking an automated work in the list of investigatory powers for which this above procedure applies, this inclusion has, almost 1.5 years after Computer Crime Act III came into force, not yet occurred as a result of which this procedure is not (yet) legally binding.[313] One may, therefore, wonder if central examination by CEC and subsequent authorization by the Board are indeed taking place.

During the execution of the hacking, the Inspectorate Justice and Security supervises the execution of the hacking order by the police, particularly their compliance with the rules of the DCCP and the Decision Investigation.[314] However, this cannot be considered independent oversight as the Inspectorate falls under the Authority of the Minister of Justice and Security.[315] General oversight is also conducted by the investigative judge on the criminal investigation, and since every amendment, supplementation, extension, prolongation, or termination of the hacking order is subject to prior written authorization from the investigative judge, review of the legality, proportionality and the subsidiarity of the hacking occurs every four weeks.[316] Nevertheless, it would be desirable to increase the oversight conducted during the execution of hacking, for example, by having the investigative judge present during the hacking.

Finally, ex-post oversight by an independent judge on the application of the hacking powers and the lawfulness of the evidence gathering stage is conducted in the case of a criminal indictment of the suspect. Because the investigative judge can never be part of the criminal court in charge of the criminal investigation, the independence of the court is ensured.[317] Because all investigatory activities are automatically logged or otherwise reported (think of a police report by the technical or tactical teams regarding hacking activities and findings), transparency is increased, thereby ensuring effective ex-post oversight.[318] Such data must be attached to the procedural documents, thereby enabling the involved parties to use such information to their advantage and to conduct an adequate assessment. A problem arises, however, when the technical nature of such data renders it unreadable for the criminal judge, public prosecutor or lawyer unless an expert is hired as a result of which the accessibility to such data required for ex-post oversight is undermined.[319] It would, therefore, be desirable to include the possibility for the suspect to hire an expert free of charge.

---

[311] *Dragojević v. Croatia App no 68955/11* (ECtHR, 15 January 2015). *JBP 2015/57*, ann. by Lindeman, §7
[312] *Kamerstukken II* (n 267), p. 10
[313] See article 5.1 of *Instruction Investigatory Powers* (n 109)
[314] Article 126nba(7) DCCP; Decision Investigation in an Automated Work (n 119), p. 23-24; See article 65(1)(2) Police Act 2012
[315] See article 65(2) Police Act 2012
[316] Article 170(2) DCCP ; Article 126nba(5) DCCP; Article 180(3) DCCP
[317] Article 268(2) DCCP
[318] *Roman Zakharov v. Russia* (n 232) §272 , p. 25
[319] *Kamerstukken II* 2015/2016 (n 27), p. 8

Another problem is that not every criminal investigation ends in the indictment of a suspect as a result of which ex-post oversight cannot be conducted by the criminal court – something that is further discussed under §5.2.6.

§5.2.6 Notification mechanisms and remedies

The ECtHR has emphasized the importance of ensuring adequate remedy, particularly considering the covert nature of the investigatory powers as a result of which a review often cannot be exercised by the suspect in the first two stages.[320] Since not every hacking may result in a criminal indictment, the legislator incorporated the safeguard of the notification obligation to ensure that a targeted individual is nonetheless ensured a right of redress.[321] Indeed, the targeted individual must be informed of the fact that he was subjected to hacking and of the type of information that was secured when the criminal investigation reasonably allows it.[322] Once aware of the hacking, the individual can challenge the lawfulness of such hacking by submitting a complaint before the criminal court or the police, or by bringing a claim of tort before the civil court in which the national ombudsman may also become involved, thereby providing an adequate remedy.[323]

However, the notification obligation is not always strictly followed in practice, and even if informed it suffices for the public prosecutor to provide a global overview of the nature of the relevant data captured.[324] It may, therefore, be the case that the targeted individual will never become aware of the intrusion, and, even in the case of notification, the lack of detailed information impedes the ability of the targeted individual to challenge the lawfulness of the hacking before an independent court.

For this reason, the parliamentary party Groenlinks proposed the creation of an independent commission that could assess the lawfulness of the hacking order ex-post but this motion was rejected.[325] This is surprising considering that a similar commission has already proven to be highly effective in the case of the Dutch Intelligence Service. Their independent commission executes both general oversight on the procedures surrounding the hacking in all three phases, and particular oversight in a concrete case ex-post.[326] Considering the highly intrusive nature of hacking and the potential absence of oversight ex-post, it would appear that the creation of a similar independent commission for police hacking is desirable.

---

[320] *Klass and others v. Germany* (n 208) §55
[321] Article 126bb DCCP
[322] ibid
[323] Article 552a DCCP; Book 6 article 162 Dutch Civil Code of Procedure; Eskens et al (n 239) p. 33 Decision Investigation in an Automated Work (n 119), p. 24-25; *Klass and Others v. Germany* (n 208) §57-58; *Szabó and Vissy v. Hungary* (n 225) §86, *Ekimdzhiez v. Bulgaria* (n 235) §90-91, *Uzun v. Germany* (n 209) §65-66; *Kruslin v. France* (n 235) §34
[324] Spapens, Siesling & de Feijter, 'Brandstof voor de opsporing evaluatie, Wet bevoegdheden vorderen gegevens,' (2011) BJU, p 99. ; College Bescherming Persoonsgegevens (n), p. 11
[325] *Kamerstukken II*, 2017/2018, 34372, J
[326] *Kamerstukken II*, 2015/2016 (n 267), p. 10

§5.2.7 Overview of the findings and recommendations

Having critically assessed the legal framework surrounding the hacking powers using the insights of ECtHR case-law, the findings are portrayed in the table below.

Overview	**Grounds** (individual)	**Scope** (general)	**Duration** (general)	**Procedures** (general)	**Authorization & oversight** (general)	**Notification & Remedies** (general)
Hacking in order to intercept (tele)communications **Hacking in order to secure future & stored data**	- Pre-trial detention crime (felony) that causes a serious breach of the legal order - Felony with minimum imprisonment of 8 years - Designated felonies that cause a serious breach of the legal order	**Nature of the crime**: - Serious crime **Categories of people**: - Suspect - Computerized device in use by the suspect **Nature of powers** - 5 investigatory activities, various functionalities **Further safeguards**: - Technical limitation software functionalities - Information requirements restricting scope (nature and functionality of technical tool, part of targeted computerized device, category of data that may be secured). **Hacking order issued by public prosecutor must be urgently required** (necessity, proportionality and subsidiarity test)	**Fixed period**: 4 weeks **Extension**: Blocks of 4 weeks indefinitely if urgently required (requires prior authorization investigative judge who conducts a necessity, proportionality and subsidiarity test) **Termination**: If no longer urgently required	Functional separation technical team and tactical team <u>Technical team:</u> - Expertise in ICT - Conducts hacking - Transfers data to an infrastructure - Transfers relevant data to tactical team - Automatic logging <u>Tactical team:</u> - Examine, analyze and use data required for investigation - Report investigatory activities conducted **Data deletion**: - When no longer necessary or up until 6 months <u>Lex specialis:</u> - 2 months after termination criminal investigation/after notification in case of police report **Data retention**: - 5 years to handle complaints and to account for transactions	**Phase 1**: - Authorization by investigative judge (independent) and the Board (- Oversight by CEC **Phase 2**: - Oversight by Inspection Justice and security - Oversight by public prosecutor and investigative judge **Phase 3**: - Oversight by independent criminal court **Further safeguards**: Hacking order and authorization subject to various information requirements enabling adequate assessment and motivation investigative judge Automatic logging and police reports mandatory Public scrutiny	- Notification obligation - Ex-post oversight by independent criminal court - Complaint to the police - Tort claim before civil court
Criticism	- Not limited to the most serious felonies with a broad range of felonies being applicable - Ambiguity surrounding safeguard of severe breach of the legal order	- Third parties may be subject to hacking because of broad notion computerized device in use by the suspect	- No final limit on extensions of hacking	- Disproportionate retention term	- Investigative judge rarely refuse authorizations because of passive legality test - Lack of special expertise investigative judge - CEC/Board internal oversight and not certain if oversight actually occurs due to lack of codification - Inspection Security and Justice are not independent	- Technical expertise required for ex-post oversight - Notification obligation not always followed in practice - Vague information in notification - No independent commission that conducts oversight, whereas the Dutch Intelligence Service does foresee in this

It follows that the legal safeguards against abuse prescribed by ECtHR case-law regarding police surveillance (see §4.2.3) are present in the legal framework surrounding the hacking powers. In fact, the Dutch legislator appears to have incorporated the minimum safeguards against abuse as prescribed in *Roman Zakharov* for police hacking, even though the ECtHR has as yet not required this in the case of police surveillance. This is commendable considering the highly intrusive nature of police hacking. The grounds and scope of application are clearly defined in statutory law as there is a clear definition of the nature of the crime, the category of people liable to be subjected to the hacking, and the circumstances under which the hacking may be ordered. Various safeguards are further incorporated that restrict the scope of application (severe breach of the legal order, urgently required requirement, five powers, technical limitations, time limits).

Moreover, regarding authorization and oversight (see §4.2.4), it follows that oversight by an independent judicial body in the first stage is achieved through prior authorization by the investigative judge, while the Board and CEC perform internal review. Review in the second stage is performed by the Inspectorate (internal review) and the investigative judge (general review) although this latter review is limited compared to the first stage. Finally, independent review in the last stage is ensured by the criminal court in the case of criminal indictment, while in the absence of such indictment the targeted person is nonetheless informed through the notification obligation. Consequently, the person can submit a claim of tort before the civil court or submit a complaint to the police or criminal court. The effectiveness of the review is further ensured through the condition that the hacking must be urgently required for the criminal investigation (proportionality and subsidiarity test) and strict information and motivation requirements regarding the hacking order and the subsequent authorization. Finally, through logging obligations and police reports, the criminal judge is also informed. As such, it appears the legal framework surrounding the hacking powers contains adequate and effective guarantees against abuse.

Nevertheless, there is also room for improvement. Firstly, it would be recommendable to set a maximum deadline for the extension of the hacking order as currently the hacking can be extended indefinitely. Secondly, it is important to reconsider the retention period of personal data as a retention period of five years appears to be a disproportionate, particularly when no criminal indictment is initiated. Thirdly, it would be desirable to subject investigative judges and public prosecutors involved in examining the legality, proportionality, and subsidiarity of the hacking order to mandatory training in a special knowledge center for cybercrime prevention. Fourthly, the review procedure of CEC and the Board must be codified as soon as possible. Fifthly, it would be desirable to include an external chairman and external experts in CEC, the Board, and the Inspectorate. Sixthly, to improve the oversight during the execution of the hacking, it would be desirable to have the investigative judge present during the hacking. Seventhly, suspects against whom a criminal indictment has been initiated must have the ability to hire an expert free of charge to ensure effective review. Eighthly, an independent commission must be created to ensure effective remedy, particularly in the absence of a criminal indictment. Finally, because hacking to conduct systematic observation cannot be deemed necessary, this hacking power must be removed from the hacking provision.

§5.3 Balancing test and conclusion

The benefits of the application of the hacking powers must be balanced against the extent of the intrusion. It follows that the hacking powers to intercept communications and to secure existing and future stored data correspond to a pressing social need and fill the gap in present investigatory powers as a result of which access to key evidence is regained by the police in the pursuit of one of the legitime aims, namely the prevention and prosecution of cybercrime. To this end, the hacking powers have already proven effective as the Dutch police recently managed to arrest more than a hundred criminals through the use of hacking software that enabled them to intercept and decrypt communications exchanged by phones and to listen to such communications in real-time.[327] On the other hand, these hacking powers may severely interfere with the right to respect for private life of suspects and third parties. As such, there must be effective, and adequate guarantees against abuse. Because these are present, the interference with the right to respect for private life is limited to what is strictly necessary and proportionate as a result of which the government remains within its margin of appreciation. It would thus appear that a fair balance has been struck between the benefits of the hacking powers and the extent of the intrusion with the right to respect for private life.

This chapter thus found that hacking to intercept confidential communications and hacking to secure existing and future data are necessary and proportionate tools for evidence gathering by the police to combat cybercrime. This is not the case for hacking to conduct systematic observation, however, as this hacking power does not correspond to a pressing social need and cannot be deemed effective.

[327] Henk van Gelder & Jelle Tieleman. 'Ruim honderd criminelen gearresteerd dankzij nieuwe kraaksoftware van politie oost Nederlands' (02 July, 2020) https://www.ad.nl/nijmegen/ruim-honderd-criminelen-gearresteerd-dankzij-nieuwe-kraaksoftware-van-politie-oost-nederland~acba02a0/ accessed 7 August 2020

Chapter VI: Conclusion

On March 1st, 2019, Computer Crime Act III came into force in the Netherlands which introduced the investigatory power of lawful hacking into article 126nba of the DCCP. This provision enables the police to covertly and remotely access an automated work in use by the suspect in order to determine certain aspects of the automated work or user, to intercept confidential communications, to conduct systematic observation, to secure existing and future data, and to render data inaccessible – all of this in the pursuit of cybercrime prevention and prosecution.

While hacking may on the one hand empower the police in their criminal investigation as electronic data can be covertly and easily secured, it is simultaneously a far-reaching power that inevitably interferes with the right to respect for private life enshrined in Article 8 of the ECHR. Such interference by the police can only be justified if it is in accordance with the law, and is necessary in a democratic society in the pursuit of a legitimate aim. This latter condition is precisely where the problem lies, however, as various actors openly questioned the necessity and proportionality of the hacking provision.

Considering the above, this thesis researched whether the new investigatory power to hack, introduced in article 126nba of the DCCP, could be considered a necessary and proportionate tool for evidence gathering by the police to combat cybercrime, particularly when considering the right to respect for private life in article 8 ECHR. To this end, the focus was on hacking to intercept confidential communications, hacking to conduct systematic observation, and hacking to secure existing and future stored data, because these hacking powers result in highly intrusive covert surveillance of the targeted individual.

To answer the research question, the rationale of the Dutch legislator behind the creation of the hacking provision was first discussed as well as which concrete hacking powers the hacking provision granted to the police. Next, the legal framework surrounding the hacking powers was examined in which the conditions of use, safeguards, and oversight mechanisms were identified, and it was critically examined whether there were no alternative and less intrusive powers than the hacking power available to the police. Hereafter, it was discussed how the hacking powers interfered with the right to private life enshrined in article 8 of the ECHR, and what conditions must be fulfilled according to ECtHR case-law for a restrictive measure to be necessary and proportionate, in particular in case of surveillance measures conducted by law enforcement. Finally, all of the insights were combined to critically assess and evaluate whether the hacking powers could be considered necessary and proportionate tools for evidence gathering by the police to combat cybercrime.

This thesis found that the hacking provision was created because of a presumed gap in investigatory powers available to the police caused by three technological developments: the encryption of electronic data, wireless networks (hotspots), and cloud computing. These technological developments cause anonymity on the network and undermine the police's ability to effectively locate, access, and retrieve data required for criminal investigation. Consequently, access to crucial evidence is hampered if not made impossible, which impedes the effective

prevention and prosecution of cybercrime, and resulted in a pressing need for criminal investigation to regain access to such data. It was found that through the use of the hacking powers to intercept and record confidential communications, and to secure existing and future stored data, encryption can be circumvented and data stored on an external server can be retrieved, however, the hacking power to conduct systematic investigation did not correspond to any of the problems arising from the technological developments.

A thorough legal analysis was then conducted regarding the investigatory powers available to the police, and it was found that there were no alternative and less intrusive powers available to the police that could fully overcome the issues caused by encryption, wireless networks, and cloud computing. ECtHR case-law was then examined and it was determined that for the hacking powers to be necessary, they had to be strictly necessary. As such, the hacking powers had to correspond to a pressing social need and needed to be proportionate to the legitimate aim pursued, as well as be strictly necessary to obtain vital evidence. It was concluded that in the absence of any subsidiary means to obtain access to electronic data, hacking to record and intercept confidential communications and hacking to secure existing and future stored data could be considered necessary tools for evidence gathering to combat cybercrime because they correspond to a pressing social need in the pursuit of a legitimate aim. Hacking to conduct systematic observation, however, could not be deemed a necessary tool for evidence gathering by the police because it did not correspond to a pressing social need and is ineffective.

Hereafter, the proportionality of the hacking powers was addressed. ECtHR case-law was used to assess whether the legal framework surrounding the hacking powers contained adequate and effective measures against abuse. Firstly, this thesis found that the grounds and scope of application are clearly defined in law as there is a clear definition of the nature of the crime, the category of people liable to be subjected to the hacking, and the circumstances under which the hacking may be ordered. Secondly, various safeguards are incorporated that restrict the scope of application (there must be a felony that results in severe breach of the legal order, the hacking must be urgently required for the criminal investigation, the hacking is limited to five investigatory activities, technical limitations are present, time limits are fixed). Moreover, authorization and oversight are ensured as the public prosecutor can only issue the hacking after prior authorization of the investigative judge is obtained who is independent of the executive power while the Board and CEC also conduct internal review. Review in the second stage is further performed by the Inspection (internal review) and by the investigative judge (general review). Finally, independent review in the last stage is ensured by the criminal court in the case of criminal indictment, while in the absence of such indictment, the targeted person is nonetheless informed through the notification obligation. As such, it was concluded that the legal framework surrounding the hacking powers contains adequate and effective guarantees against abuse, and the hacking powers that were earlier identified as necessary can, therefore, also be considered to be proportionate tools for evidence gathering by the police to combat cybercrime.

Nevertheless, it was concluded that there is also room for improvement which resulted in the following recommendations Firstly, it would be recommendable to set a maximum deadline on the extension of the hacking order as currently the hacking can be extended for blocks of four weeks indefinitely. Secondly, it is important to reconsider the retention period of personal data as five years appears to be a disproportionate time to retain this personal data, particularly when no criminal indictment is initiated. Thirdly, it would be desirable to subject investigative judges and public prosecutors involved in examining the legality, proportionality, and subsidiarity of the hacking to mandatory training in a special knowledge center for cybercrime prevention. Fourthly, the review procedure of CEC and the Board must be codified as soon as possible. Fifthly, it would be desirable to include an external chairman and external experts in CEC, the Board, and the Inspection. Sixthly, to improve the oversight during the execution of the hacking, it would be desirable to have the investigative judge present during the hacking. Seventhly, suspects against whom a criminal indictment has been initiated must have the ability to hire an expert free of charge to ensure effective review. Eighthly, an independent commission that conducts oversight must be created to ensure effective remedy, particularly in the absence of a criminal indictment. Finally, because hacking to conduct systematic observation cannot be deemed necessary, this hacking power must be removed from the hacking provision. Through the incorporation of these recommendations, citizens are provided with optimal protection against arbitrary interference and guaranteed an effective right to redress.

After the mainly legal analysis and evaluation of the hacking powers to record and intercept communications, to conduct systematic observation, and to secure existing and future stored data, further research is required into the remaining two hacking powers that were incorporated into the hacking provision, namely the use of the hacking power to identify a user or automated work, and the use of the hacking power to render data inaccessible. Moreover, considering that this thesis was conducted from a strictly legal viewpoint, it would be advisable to examine the hacking powers from a more theoretical perspective as well in which academic literature is used beyond the Netherlands (for example, United States and Canada). To this end, comparative research between the Dutch hacking powers and the hacking powers of other countries would be fruitful.

With that being said, this thesis showed that citizens must always remain critical and cautious towards newly introduced powers by the Government that impede the right to respect for private life. While the introduction of new investigatory powers may be in the pursuit of a legitimate aim, protecting your privacy is vital too. Therefore, as Edward Snowden rightly notes: “Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say.”

Bibliography

Primary sources

Legislation

Council of Europe law

European Convention on Human Rights as amended, Rome, 4.XI.1950

Convention on Cybercrime, Budapest, 23.XI.2001

Legislative proposals by the European Commission

Commission, Proposal for a regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters COM (2018) 225 final

Commission, Recommendation and Annex to Recommendation for a council decision authorising the opening of negotiations in view of an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters COM (2019) 70 final

Commission, Recommendation for a council decision authorizing the participation in negotiations on a second Additional Protocol to the Council of Europe Convention on Cybercrime COM (2019) 71 final

Dutch statutory law

Dutch Criminal Code of Procedure, The Hague, 15.I.1921

Civil Code of Procedure, The Hague. 1.I.1992

Computer Crime Act I (Stb. 1993, nr. 33)

Computer Crime Act II (Stb. 2006, nr. 301)

Police Data Act, The Hague, 21.VII.2007 as amended by Council Directive 2016/680/EU 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 [2016] OJ J L119/4.5

Instruction Investigatory Powers (Stc. 2011, nr. 3240) as amended by Stc. 2012, nr. 10486)

Police Act 2012 (Stb. 2012, nr. 315)

Computer Crime Act III (Stb, 2018, nr. 322)

Decision Investigation in an Automated Work (Stb. 2018, nr. 340)

Case-law

European Court of Human Rights

Handyside v. the United Kingdom App no 5493/72 (ECtHR 7 December 1976)

Klass and others v. Germany App no 5029/71 (ECtHR 6 September 1978)

Sunday Times v. the United Kingdom App no 6538/74 (ECtHR 26 April 1979)

Silver and others v. the United Kingdom App no 5947/72; 6205/73; 7052/75; 7061/75; 7107/75; 7113/75; 7136/75 (ECtHR 25 March 1983)

Malone v. the United Kingdom App no 8691/79 (ECtHR, 2 August 1984)

Leander v. Sweden App no 9248/81 (ECtHR 26 March 1987)

Kruslin v. France App no 11801/85 (ECtHR 24 April 1990)

Halford v. the United Kingdom App no 20605/92 (ECtHR 25 June 1997)

Amann v. Switzerland App no 27798/95 (ECtHR 16 February 2000)

Khan v. the United Kingdom App no 35394/97 (ECtHR 12 May 2000

P.G. and J.H. v. the United Kingdom App no 44787/98 (ECtHR 25 September 2001)

Peck v. the United Kingdom App no 44647/98 (ECtHR 28 January 2003)

Weber and Saravia v. Germany App no 54934/00 (ECtHR 29 June 2006)

Volokhy v. Ukraine App no 23543/02 (ECtHR 2 November 2006)

Copland v. the United Kingdom App no 62617/00 (ECtHR 3 April 2007)

Dmitru Popescu v. Romania App no 71525/01 (ECtHR 26 April 2007)

Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria App no 62540/00 (ECtHR 28 June 2007)

S. and Marper v. The United Kingdom App no 30562/04, 30566/04 (ECtHR 4 December 2008)

Uzun v. Germany App no 35623/05 (ECtHR 2 September 2010)

Dragojević v. Croatia App no 68955/11 (ECtHR 15 January 2015).

Roman Zakharov v. Russia App no 47143/06 (ECtHR 4 December 2015)

Szabó and Vissy v. Hungary App no 37138 /14 (ECtHR, 6 June 2016)

Trabajo Rueda v. Spain App no 32600/12 (ECtHR 30 May 2017)

Ben Faiza v. France App no 31446/12 (ECtHR 8 February 2018)

Hambardzumyan v. Armenia App no 43478/11 (ECtHR 5 December 2019),

Supreme Court of the Netherlands

Procurator General's Office of the Dutch Supreme Court 17 December 2013, ECLI:NL:PHR:2013:2696

Procurator General's Office of the Dutch Supreme Court 30 September 2014, ECLI:NL:PHR:2014:2162

Federal Constitutional Court of Germany

BVerfGE [Federal Constitutional Court] 27 February 2008, 1 BvR 370/07, ECLI:DE:BVerfG:2008:rs20080227.1bvr037007 (Ger.).

Parliamentary documents

Kamerstukken II, 1989/1990, 21 551, nr. 3

Kamerstukken II, 1996/1997, 25 403, nr. 3

Kamerstukken II, 1998/1999, 26 671, nr. 3

Kamerstukken II, 2015/2016, 34 372, nr. 3

Kamerstukken II, 2015/2016, 34 372, nr. 4

Kamerstukken II, 2017/2018, 34 372, J

Secondary sources

Literature

Ahmad M, Farid M. A, Ahmed S, Saeed K, Asharf M., & Akhtar U. (2019, January). Impact and detection of GPS spoofing and countermeasures against spoofing. In *2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET)* (pp. 1-8). IEEE.

Arora R, Parashar A. 'Secure user Data in Cloud Computing using Encryption Algorithms' (2013) *International Journal of Engineering Research and Applications Vol 3 Issue 4*, pp. 1922-1926

Beijer A., Bokhorst R.J., Boone M, Brants C.H, Lindeman J.M.W. 'De Wet bijzondere opsporingsbevoegdheden-eindevaluatie.' (2004) *WODC-reeks onderzoek en beleid, 222*.

Brenner S, Clarke L. 'Distributed Security: A New Model of Law Enforcement.' *John Marshall Journal of Computer & Information Law*, Forthcoming.

Council of Europe. 'Guide on Article 8 of the Convention – Right to respect for private and family life'. (31 December 2019).

Dragojević v. Croatia App no 68955/11 (ECtHR, 15 January 2015). *JBP 2015/57*, annotation by Lindeman

Eskens S.J, van Daalen O.L, van Eijk N. A. N. M. Geheime surveillance en opsporing: Richtsnoeren voor de inrichting van wetgeving (2016). *Instituut voor informatierecht.*

Gerards H. *EVRM – Algemene leerstukken* (2011) The Hague: Sdu Uitgevers

Grabosky P. 'The Evolution of Cybercrime, 2004-2014' (2014). *RegNet Research Paper* No. 2014/58

Kilkelly U. 'The right to respect for private and family life. *A Guide to the Implementation of Article 8*,' (2003) 200310-11.

Koops B.J. 'The internet and its opportunities for cybercrime', (2010) *Tilburg Law School Legal Studies Research Paper Series* No. 09/2011.

Koops B.J. 'De dynamiek van cybercrimewetgeving in Europa en Nederland.' (2012) 38 *Justitiële Verkenningen* (1). pp. 9-24

Koops B.J. *Het decryptiebevel en het nemo-teneturbeginsel* (2012). Boom Lemma.

Koops B.J., Newell, B. C., Timan, T., Skorvanek, I., Chokrevski, T., & Galic, M. (2016). A typology of privacy. *U. Pa. J. Int'l L., 38,* 483

Koops B.J. & Schellekens, M. H. M. 'Computercriminaliteit II: de boeven zijn er - nu de wet weer.' (1999) *Nederlands Juristenblad*, 74(37).

Lewis J, Zheng D.E, Carter W.A. *The effect of encryption on lawful access to communications and data*. (2017). Rowman & Littlefield

Nuth M.S. 'Taking advantage of new technologies: For and against crime.' (2008). *Computer Law & Security Review*, *24*(5), 437

Oerlemans J.J. *Investigating cybercrime* (2017) Amsterdam University Press

Oerlemans J.J. 'Normering van digitale opsporingsmethoden.' (2017) *Research paper van de Faculteit Militaire Wetenschappen Nederlandse Defensie Academie.*

Roagna I. *Protecting the right to respect for private and family life under the European Convention on Human Rights*. (2012) Council of Europe human rights handbooks,

Škorvánek I, Koops B.J, Newell B.C, Roberts A.J. 'My Computer is My Castle: New Privacy Frameworks to Regulate Police Hacking' (2019) *Brigham Young University Law Review*, forthcoming.

Spapens T, Siesling M, & Feijter E. D. *Brandstof voor de opsporing*. (2011). Boom Juridische uitgevers.

Van Buiten N. 'De modernisering van de Wet BOB – Herinneren we ons de IRT-affaire nog?', *DD 2016/10*, nr. 3.

Wall D. *Cybercrime: The Transformation of Crime in the Information Age*. (2007). *Vol. 4.* Polity

Wall D. 'Hunting, Shooting and Phishing: New Cybercrime Challenges for Cybercanadians in the 21st Century' (2008). *Eccles Centre for North American Studies*, London

Wall D. 'Crime, security, and information communication technologies: The changing cybersecurity threat landscape and implications for regulation and policing' in R. Brownsword, E. Scotford and K. Yeung (2017) (eds) *The Oxford Handbook on the Law and Regulation of Technology*, Oxford: Oxford University Press

Blogs, websites, newspapers

Bits of Freedom, 'Reactie op consultatie Wetsvoorstel Computercriminaliteit III' Attachment 651730 to *Kamerstukken II*, 2015/2016, 34 372, nr. 3

College Bescherming Persoonsgegevens 'Consultatie conceptwetsvoorstel Computercriminaliteit III' (17 February 2014) <https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/z2013-00349.pdf> accessed 10 August 2020

Gildred J. 'How to encrypt your data for cloud storage' *Cloudwards* (18 May 2018) <https://www.cloudwards.net/how-to-encrypt-your-data-for-cloud-storage/#Zero-Knowledge-Cloud-Storage> accessed 12 May 2020

Hoffman C. 'Why you shouldn't host an open Wifi-Network without a password.' *Howtogeek* (26 September 2016) <https://www.howtogeek.com/132925/htg-explains-why-you-shouldnt-host-an-open-wi-fi-network/> accessed 5 April 2020

Kharpal A. 'Apple vs. FBI: All you need to know.' CNBC (29 March 2016) <https://www.cnbc.com/2016/03/29/apple-vs-fbi-all-you-need-to-know.html> accessed 13 May 2020

Kraan J. 'Veel kritiek op voorgestelde hackbevoegdheid voor politie.' *NU* (11 February 2016) <https://www.nu.nl/internet/4213037/veel-kritiek-voorgestelde-hackbevoegdheid-politie.html> accessed 14 April 2020

Ministry of Justice and Security. ‘Nieuwe wet versterkt bestrijding cybercriminaliteit’ (28 February 2020) <https://www.rijksoverheid.nl/actueel/nieuws/2019/02/28/nieuwe-wet-versterkt-bestrijding-computercriminaliteit> accessed 19 February 2020

Nederlandse Orde van Advocaten,’Betreft: concept-wetsvoorstel tot verbetering van de opsporing en vervolging van computercriminaliteit (Computercriminaliteit III)’ Attachment 651732 to *Kamerstukken II* 2015/2016, 34 372, nr. 3

Privacy International, ‘Government hacking’ <https://privacyinternational.org/learning-topics/government-hacking> accessed 22 February 2020

Schellevis J. & Kasteleijn N. ‘Forse kritiek op hackbevoegdheid politie’ *NOS* (11 February 2016) <https://nos.nl/artikel/2086191-forse-kritiek-op-hackbevoegdheid-politie.html> accessed 18 February 2020

Van Gelder H. & Tieleman J. ‘Ruim honderd criminelen gearresteerd dankzij nieuwe kraaksoftware van politie oost Nederlands’ (02 July, 2020) <https://www.ad.nl/nijmegen/ruim-honderd-criminelen-gearresteerd-dankzij-nieuwe-kraaksoftware-van-politie-oost-nederland~acba02a0/> accessed 7 August 2020

Appendices

A. Dutch Criminal Code of Procedure: Translation

Book I. General provisions

Title. IV Several Special Coercive Measures

Second section. Pre-trial detention

Article 67(1)
[1.]A pre-trial detention order may be issued based on suspicion of:
a. a felony which carries a statutory term of imprisonment of at least four years;
b. any of the felonies defined in articles 132, 138a, 138ab, 138b, 139c, 139d(1) and (2), 139h(1) and (2), 141a, 137c (2), 137d(1), 137e(2), 137g(2), 151, 184a, 254a, 248d, 248e, 272, 284(1), 285(1), 285b, 285c, 300(1), 321, 323a, 326c(2), 326d, 340, 342, 344a, 344b, 347(1), 350, 350a, 350c, 350d, 351, 395, 417bis, 420bis.1, 420quater, and 420quater.1 of the Criminal Code;
c. any of the felonies defined in:
article 86i(1) of the Electricity Act [Elektriciteitswet 1998]
article 66h(1) of the Gas act [Gaswet];
article 8.12(1)(2) of the Animal Act [Wet dieren];
article 175(2)(b) or (3) in conjunction with (1)(b) and 176(2) in conjunction with article 7(1)(a)(c) of the Road Traffic Act 1994; [Wegensverkeerswet 1994]
article 30(2) of the Civil Authority Special Powers Act [Wet Buitengewone Bevoegdheden Burgerlijk Gezag];
articles 52, 53(1) and 54 of the Conscientious Objections against Military Service Act [Wet Gewetensbezwaren Militaire Dienst];
article 36 of the Betting and Gaming Act [Wet op de Kansspelen];
article 11(2) and 11a of the Opium Act [Opiumwet];
article 55(2) of the Weapons and Ammunition Act [Wet Wapens en Munitie];
article 11 of the Temporary Home Exclusion Order Act [Wet Tijdelijk Huisverbod].
article 8 of the Temporary Administrative Measures to Counter-Terrorism Act [Tijdelijke wet bestuurlijke maatregelen terrorismebestrijding]

Seventh section. Search in order to record data

Article 125i
The power to search a place for the purpose of recording data stored or recorded in a data carrier at this place shall be conferred on the investigative judge, the public prosecutor, the assistant public prosecutor under the same conditions as referred to in articles 96b, 96c(1), (2) and (3), 97 (1) to (4) inclusive, and 110 (1) and (2). They may record this data in the interest of the investigation. Articles 96(2), 98, 99 and 99a shall apply mutatis mutandis.

Article 125j

[1]. In the case of a search, an automated work located elsewhere may be searched for data stored in that device or system that is reasonably required in order to reveal the truth from the place where the search takes place. If such data is found, then it may be recorded.

[2.] The search shall be limited to the extent that the persons, who normally work or reside at the place where the search is being conducted, have access thereto from that place with the consent of the person entitled to use the computerised device or system.

Article 125k

[1.] Insofar as is specifically required in the interest of the investigation, the person who may be reasonably believed to have knowledge of the security system of an automated work may be ordered, if section 125i or section 125j is applied, to provide access to the automated works present or parts thereof. The person who is ordered to do so must comply with this order, if requested, by providing the knowledge about the security system.

[2.] Subsection (1) shall apply mutatis mutandis if encrypted data is found in an automated work. The order shall be directed to the person who may be reasonably believed to have knowledge of the manner of encryption of this data.

[3.] The warrant, referred to in subsection (1), shall not be given to the suspect. Section 96a(3) shall apply mutatis mutandis.

Title IVA: Special investigative powers

First section. Systematic surveillance

Article 126g

[1.] In the case of suspicion of a felony, the public prosecutor may, in the interest of the investigation, order an investigating officer to systematically follow a person or systematically observe his movements or behaviour.

[2.] In the case of suspicion of a felony as defined in article 67(1), which felony in view of its nature or the relation to other serious offences committed by the suspect constitutes a serious breach of the legal order, the public prosecutor may determine, in the interest of the investigation, that an enclosed place, not being a home, will be entered without the consent of the person entitled to use the premises, for the purpose of executing the warrant

[3.] The public prosecutor may determine that a technical device will be used for the purpose of executing the warrant, insofar as no confidential information is recorded by means of that device. A technical device shall not be attached to a person, unless with his consent.

[4.] The warrant shall be issued for a period of maximum three months. It may be extended each time for a period of maximum three months.

[5.] The warrant shall be in writing and shall state:

a. the felony and if known, the name or otherwise the most precise description possible of the suspect;

b. the facts or circumstances which show that the conditions, referred to in subsection (1), have been met;

c. the name or the most precise description possible of the person referred to in subsection (1);
51
d. in the application of subsection (2), the facts or circumstances which show that the conditions, referred to in that subsection, have been met, as well as the place to be entered;
e. the manner in which the surveillance order will be executed, and
f. the term of validity of the surveillance order
6. In the case of urgent necessity, the surveillance order may be issued verbally. In that case the public prosecutor shall put the surveillance order in writing within three days.
[7.] As soon as the conditions referred to in subsection (1) are no longer met, the public prosecutor shall determine that the execution of the surveillance order has ended.
[8.] The warrant may be amended, supplemented, extended or terminated in writing and stating reasons. In the case of urgent necessity, the decision may be given verbally. In that case the public prosecutor shall put this decision in writing within three days.
[9.] A surveillance order as referred to in subsection (1) may also be issued to a person in the public service of a foreign state. Requirements may be set for these persons by Governmental Decree. Subsections (2) to (8) inclusive shall apply mutatis mutandis.

Sixth section. Recording confidential communications by means of a technical device

Article 126l
[1.] In the case of suspicion of a felony as defined in article 67(1), which felony in view of its nature or the relation to other serious offences committed by the suspect constitutes a serious breach of the legal order, the public prosecutor may, if urgently required in the interest of the investigation, order an investigating officer as referred to in article 141(b) and (c) to record confidential communications by means of a technical device.
[2.] The public prosecutor may, in the interest of the investigation, determine that an enclosed place, not being a home, will be entered without the consent of the person entitled to use the premises for the purpose of executing the order. If urgently required in the interest of the investigation and in the case of a felony which carries a statutory term of imprisonment of at least eight years, he may determine that a dwelling will be entered without the consent of the person entitled to use the premises for the purpose of executing the warrant. Article 2(1, last sentence) of the General Act on Entry into Dwellings shall not apply.
[3.] The warrant to record confidential communications shall be in writing and shall state:
a. the felony and if known, the name or otherwise the most precise description possible of the suspect;
b. the facts or circumstances which show that the conditions, referred to in subsection (1) and, if subsection (2, second sentence) applies, the conditions referred to in subsection (2), have been met;
c. at least one of the persons who participate in the communications, or, if the warrant relates to communications in an enclosed place or in a means of transport, one of the persons who participate in the communications or the most precise description possible of that place or that means of transport;
d. in the application of subsection (2), the place to be entered;
e. the manner in which the warrant will be executed, and

f. the term of validity of the warrant.
[4.] The warrant may only be issued following authorisation to be granted by the investigative judge based on a request of the public prosecutor. The authorisation shall relate to all elements of the warrant. If a home may be entered for the purpose of executing the warrant, that power shall be explicitly stated in the warrant.
[5.] The warrant shall be issued for a period of maximum four weeks. The term of validity may be extended for a period of maximum four weeks each time.
[6.] Article 126g(6) to (8) inclusive shall apply mutatis mutandis, on the understanding that the public prosecutor shall require authorisation from the investigative judge for amendment, supplementation or extension. If the public prosecutor determines that a home will be entered for the purpose of executing the warrant, the warrant may not be issued verbally. As soon as the conditions, referred to in subsection (2, second sentence), are no longer met, the public prosecutor shall determine that the execution of the warrant is terminated.
[7.] In the case of urgent necessity, authorisation from the investigative judge, referred to in subsections (4) and (6), may be granted verbally, unless subsection (2, second sentence) is applied. In that case the investigative judge shall put the authorisation in writing within three days.
[8.] An official report on the recording shall be prepared within three days.

Seventh Section. Investigation of communications by means of automated works

Article 126m
[1.] In the case of suspicion of a felony as defined in article 67(1), which felony in view of its nature or the relation to other serious offences committed by the suspect constitutes a serious breach of the legal order, the public prosecutor may, if urgently required by the investigation, order an investigating officer to record by means of a technical device, non-public communications which are conducted through the use of the services of a communication service provider.
[2.] The warrant shall be in writing and shall state:
a. the serious offence and if known, the name or otherwise the most precise description possible of the suspect;
b. the facts or circumstances which show that the conditions, referred to in subsection (1), have been met;
c. where possible, the number or another indication by means of which the individual user of the communication service is identified as well as, insofar as is known, the name and the address of the user;
d. the term of validity of the warrant;
e. a description of the nature of the technical device or the technical devices by means of which the communications are recorded.
[3.] If the warrant relates to communications which are conducted through a public telecommunication network or by use of a public telecommunication service within the meaning of the Telecommunications Act, the warrant shall – unless such is impossible or is not permitted in the interest of the criminal proceedings – be executed with the assistance of the provider of the public telecommunication network or the public telecommunication service and

the warrant shall be accompanied by the request for assistance from the public prosecutor to the provider.
[4.] If the warrant relates to communications other than the communications referred to in subsection (3), the provider shall – unless such is impossible or is not permitted in the interest of the criminal proceedings – be given the opportunity to assist in the execution of the warrant.
[5.] The warrant, referred to in subsection (1), may only be issued following written authorisation to be granted by the investigative judge based on a request of the public prosecutor. Article 126l(5) to (8) inclusive shall apply mutatis mutandis.
[6.] Insofar as is specifically required in the interest of the investigation, the person, who may be reasonably presumed to have knowledge of the manner of encryption of the communications, may be requested, if subsection (1) is applied, to assist in decrypting the data by either providing this knowledge, or undoing the encryption.
[7.] The request referred to in subsection (6) shall not be directed to the suspect.
[8.] Article 96a(3) and article 126l(4), (6) and (7) shall apply mutatis mutandis to the request referred to in subsection (6).
[9.] Rules pertaining to the manner in which the warrant referred to in subsection (1) and the requests referred to in subsections (3) and (6) may be given and the manner of compliance with such requests shall be set by Governmental Decree.

Article 126n
[1.] In the case of suspicion of a felony as defined in article 67(1), the public prosecutor may, in the interest of the investigation, request the provision of data on a user of a communication service and the communication traffic data pertaining to that user. The request may only relate to data designated by Governmental Decree and may involve data which:
a. was processed at the time of the request, or
b. is processed after the time of the request.
[2.] The request, referred to in subsection (1), may be directed to any provider of a communication service. Article 96a(3) shall apply mutatis mutandis. If the request, referred to in subsection (1) relates to a person who can claim source protection, it can only be made after prior written authorization of the investigative judge based on a request of the public prosecutor. Article 218a, subsection (2) shall apply mutatis mutandis.
[3.] If the request relates to data as referred to in subsection (1, second sentence)(b), the request shall be made for a period of maximum three months.
[4.] The public prosecutor shall have an official record of the request prepared, which shall state:
a. the felony and if known, the name or otherwise the most precise description possible of the suspect;
b. the facts or circumstances which show that the conditions, referred to in subsection (1), have been met;
c. if known, the name or otherwise the most precise description possible of the person about whom data is requested;
d. the data requested;
e. if the request relates to data as referred to in subsection (1, second sentence)(b), the period to which the request relates.

[5.] If the request relates to data referred to in subsection (1, second sentence)(b), the request shall be terminated as soon as the conditions, referred to in subsection (1, first sentence), are no longer met. The public prosecutor shall have an official record made of amendment, supplementation, extension or cancellation of the request.
[6.] Rules pertaining to the manner in which the public prosecutor requests data may be set by Governmental Decree.

Article 126na
[1.] In the case of suspicion of a felony, the investigating officer may, in the interest of the investigation, request the provision of data pertaining to name, address, postal code, town, number and type of service of a user of a communication service. Article 126n(2) shall apply.
[2.] If the data, referred to in subsection (1), is not known to the provider and is necessary for the application of article 126m or article 126n, the public prosecutor may, in the interest of the investigation, request the provider to retrieve and provide the requested data in a manner to be determined by Governmental Decree.
[3.] In the case of a request, as referred to in subsection (1) or (2), article 126n(4)(a)(b)(c) and (d) shall apply mutatis mutandis and article 126bb shall not apply.
[4.] Rules pertaining to the manner in which the investigating officer or the public prosecutor will request the data may be set by or pursuant to Governmental Decree

Eight section. Investigation in an automated work

Article 126nba
[1.] In the case of suspicion of a felony as defined in Article 67(1), which felony in view of its nature or the relation to other serious offences committed by the suspect constitutes a serious breach of the legal order, the public prosecutor may, if urgently required by the investigation, order a designated investigating officer to remotely access an automated work in use by the suspect, to conduct investigation with or without the assistance of a technical device, with the aim to:
a. determine certain characteristics of the automated work or user, such as the identity or location and the recording thereof;
b. execute a warrant as referred to in articles 126l of 126m;
c. execute a warrant as referred to in article 126g, whereby the public prosecutor can determine that a technical device is attached to a person in order to execute the warrant;
and, in the case of a felony, which carriers a prison sentence of eight years or more, or in case of a felony that has been designated by a governmental decree:
d. record data that is stored in the automated work, or to record data which is not stored until after the time of issuing the order, insofar as reasonably necessary to reveal the truth;
e. render data, as referred to in Article 126cc sub section (5) inaccessible. Article 11.7a of the Telecommunications Act does not apply to acts which require the execution of an order as referred to in the first sentence.
[2.] The warrant, referred to in sub section (1), shall be in writing and shall state:
a. the felony and if known, the name or otherwise the most precise description possible of the suspect;

b. if possible, a number or other indication by which the automated work can be identified and, if known, that the data are not stored in the Netherlands;
c. the facts or circumstances which show that the conditions, referred to in subsection (1), have been fulfilled;
c. where possible, the number or another indication by means of which the individual user of the communication service is identified as well as, insofar as is known, the name and the address of the user;
d. the nature and functionality of the technical device, referred to in subsection (1), that is used for the execution of the warrant
e. the investigatory activity or activities, referred to in subsection (1) with a view to which the warrant is given and, if this concerns investigatory activity a, d or e, a clear description of the actions to be performed;
f. regarding which part of the automated work and which category of data the warrant will be given
g. the term of validity of the warrant
h. in the case of a warrant as referred to in the first paragraph, under c, a notification of the intention to attach a technical device to a person.
[3.] The warrant, referred to in subsection (1), shall be issued for period of maximum four weeks. The term of validity may be extended for a period of maximum four weeks each time.
[4.] The warrant, referred to in subsection (1), may only be issued following authorisation to be granted by the investigative judge based on a request of the public prosecutor. The authorisation shall relate to all elements of the warrant and shall state the term for which the warrant is valid.
[5.]The warrant, referred to in the subsection (1), may be amended, supplemented, extended or terminated in writing and stating reasons on the understanding that the public prosecutor requires an authorization from the investigative judge for any amendment, supplementation or extension. In the case of urgent necessity, the decision of the public prosecutor and the authorization of the investigative judge may be given orally. In that case, the public prosecutor and the investigative judge shall put this decision in writing within three days.
[6.] After the investigation has ended, the technical device will be removed. If the technical device cannot be removed or cannot be completely removed and this poses risks to the functioning of the automated work, the public prosecutor will inform the administrator of the automated work and make the necessary information available for the complete removal. The provisions of Article 126cc subsection (1) apply mutatis mutandis.
[7.] Supervision of the execution of the warrant, referred to in subsection (1), by the officials, referred to in Article 141(d), and the persons, referred to in Article 142(1)(b), is exercised by the Inspection, referred to in Article 65 of the Police Act 2012, in accordance with the provisions of Chapter 6 of the Police Act 2012.
[8.] By or pursuant to Governmental Decree, rules will be set regarding:
a. the authorization and expertise of the investigating officers who may be charged with the remote access to the automated work and the investigation, as referred to in the first paragraph, and the cooperation with other investigating officers;
b. the automated recording of data about the execution of the order referred to in the first paragraph.

[9.] Rules pertaining to the application of the power referred to in subsection 1 may be set by or pursuant to Governmental Decree in case it is unknown where data are stored.

Ninth section. Requesting data.

Article 126nd

[1.] In the case of suspicion of a felony as defined in article 67(1), the public prosecutor may, in the interest of the investigation, request the person, who may be reasonably presumed to have access to specific stored or recorded data, to provide this data.
[2.] A request, as referred to in subsection (1), may not be directed to the suspect. Article 96a(3) shall apply mutatis mutandis. The request may not relate to personal data concerning a person's religion or life principles, race, political persuasion, health, sex life or membership of a trade union. If the request, referred to in subsection (1) relates to a person who can claim source protection, it can only be made after prior written authorization of the investigative judge based on a request of the public prosecutor. Article 218a, subsection (2) shall apply mutatis mutandis.
[3.] A request as referred to in subsection (1) shall be in writing and shall state:
a. if known, the name or otherwise the most precise description possible of the person or persons about whom data is being requested;
b. the most precise description possible of the data being requested and the period within which and the manner in which said data should be provided;
c. the legal ground on which the request is made.
[4.] In the case of urgent necessity, the request may be given verbally. In that case the public prosecutor shall later put the request in writing and provide it to the natural or legal person to whom the request is directed within three days after the request was made.
[5.] The public prosecutor shall prepare an official record of the provision of data, which shall state:
a. the data referred to in subsection (3);
b. the data provided;
c. the felony and if known, the name or otherwise the most precise description possible of the suspect;
d. the facts or circumstances which show that the conditions, referred to in subsection (1), have been met.
e. the reason why the data is being requested in the interest of the investigation.
[6.] In the case of suspicion of a criminal offence other than the felony referred to in subsection (1), the public prosecutor may, in the interest of the investigation, make a request as referred to in that subsection with the prior written authorisation of the investigative judge. The investigative judge shall grant the authorization based on the request of the public prosecutor. Subsections (2) to (5) inclusive shall apply mutatis mutandis. Article 126l(7) shall apply mutatis mutandis.
[7.] Rules pertaining to the manner in which the data is to be requested and provided may be set by Governmental Decree.

Article 126ng

[1.] A request as referred to in article 126nc(1), 126nd(1) or 126ne(1) and (3), and article 126nf(1) may be directed to the provider of a communication service within the meaning of article 138g, insofar as the request relates to data other than the data which may be requested under application of article 126n and 126na. The request may not relate to data stored in the automated work of the provider and which is not intended for this provider or does not originate from this provider.

[2.] In the case of suspicion of a felony as defined in section 67(1), which felony in view of its nature or the relation to other serious offences committed by the suspect constitutes a serious breach of the legal order, the public prosecutor may, if urgently required in the interest of the investigation, request the provision of the data referred to in subsection (1, last sentence) from the provider which may be reasonably presumed to have access to said data, insofar as said data evidently originates from the suspect, is intended for him or relates to him or served for commission of the felony, or the felony was evidently committed in relation to said data.

[3.] A request, as referred to in subsection (2), may not be directed to the suspect. Article 96a(3) shall apply mutatis mutandis.

[4.] A request, as referred to in subsection (2), may only be made following prior written authorisation to be granted by the investigative judge based on a request of the public prosecutor. Article 126l(7) shall apply mutatis mutandis.

[5.] Article 126nd(3) to (5) and (7) shall apply mutatis mutandis.

Article 126nh

[1.] The public prosecutor may, if required in the interest of the investigation, in or immediately after the application of section 126nd(1), 126ne(1) or (3), or 126nf(1), order the person who may be reasonably presumed to have knowledge of the manner of encryption of the data referred to in these articles to assist in decrypting the data by either undoing the encryption, or providing this knowledge.

[2.] The order shall not be given to the suspect. Article 96a(3) shall apply mutatis mutandis.

Book Two. Criminal Procedure in the First Instance

Title I. The Criminal Investigation

Third section. Reporting by Investigating Officers

Article 152:

[1.] The civil servants who are charged with the detection of criminal offences shall prepare as soon as possible an official record of the criminal offence detected by them or of their detection activities or findings.

[2.] The preparation of an official record may be omitted under the authority of the Public Prosecution Service.

Fifth section. Decisions on prosecution {chapter}

Title II: The investigative judge in charge the criminal investigation

Article 170:
[1.] In each District Court the investigative judge shall be charged with handling criminal cases.
[2.] The investigative judge shall be specifically charged with exercising supervisory powers in regard of the criminal investigation, ex officio in cases prescribed by law and in addition, on application of the public prosecutor or the suspect or his defence counsel.

Article 180
[1.] The investigative judge shall see to it that the criminal investigation is not unduly delayed.
[2.] The investigative judge may, on application of the suspect or his defence counsel, and if he conducts ex officio investigative acts under articles 181 to 183 inclusive, also assess the progress in the criminal investigation. The investigative judge may instruct the case documents to be submitted to him for that purpose. If he considers such necessary, the investigative judge shall hear the public prosecutor and the suspect or his defence counsel.
[3.] The investigative judge may set the public prosecutor a time limit for conclusion of the criminal investigation. The investigative judge may also present the case to the District Court, with a view to the application of article 36

Title VI: Handling of the case by the court

First section. Court hearing

Article 268
1. Criminal cases shall be tried and decided by a three-bench division, save for the exceptions mentioned in the law.
2. The judge who conducted any investigation in the case as investigative judge shall not, under penalty of nullity, sit in the case at the court hearing, except for application of section 316(2).
3. The judges and the clerk to the court shall exclusively sit at the bench of the District Court.

B. Decision Investigation in an Automated Work: Translation

[Besluit onderzoek in een geautomatiseerd werk]

CHAPTER 4: RECORDING OF INFORMATION ON THE EXECUTION OF A WARRANT IN LOGS

Article 5 Logging

[1.] During the execution of a warrant, data shall be continuously and automatically recorded in logs regarding:

(a). the activities carried out in the pursuit of a warrant

(b) access to a technical device;

(c) data recorded on the technical infrastructure, either with or without the assistance of a technical tool in the pursuit of a warrant

(d) the functioning of the technical infrastructure.

[2.] If, by their very nature, the information on the activities, referred to in subsection (1)(a) cannot be automatically recorded, an investigating officer of a technical team shall manually record the operations.

Article 6 Determination of irregularities

[1.] The recording of data in logs referred to in Article 5 shall be carried out in such a way that, both during the period in which the warrant is to be executed, and after the execution of the warrant, it can be determined whether an irregularity has occurred which affects the reliability and integrity of the data recorded in a technical infrastructure for the purposes of the warrant.

[2.] If an irregularity is detected, an investigating officer from a technical team shall make a report, which shall be sent to the public prosecutor.

Article 7 Reliability and integrity of the logs

[1.] The contents of the logs will not be changed.

[2.] The logs shall be accessible only to officials appointed by the chief of police.

[3.] When recording data, measures shall be taken to prevent the modification or access to the recorded data by unauthorized persons and measures shall be taken to be able to determine afterwards whether any modification or unauthorized access has taken place.

CHAPTER 5 TECHNICAL REQUIREMENTS FOR A TECHNICAL TOOL FOR CARRYING OUT INVESTIGATORY ACTIVITIES

Article 8 Targeted operation

A technical device is designed in such a way that its operation can be limited to the functionality or functionalities specified in the warrant

Article 9 Targeted detection and registration

[1.] A technical device detects and records data only for the purposes of the functionality or functionalities specified in the warrant.

[2.] A technical tool containing a functionality or functionalities for recording telecommunications shall detect and record only the communication that takes place using one or more identifying features of the automated work of the individual user or users to whom the warrant relates.

Article 10 Reliability and integrity

[1.] A technical device shall record data in such a way that the content of the recorded data is identical to the content of the data detected.

[2.] A technical device shall be protected against altering its operation, against modification of the recorded data and against the knowledge of the recorded data by unauthorized persons.

Article 13 Transport

[1.] A technical tool automatically transports the recorded data to a technical infrastructure.

[2.] A technical device shall secure the recorded data during transport to a technical infrastructure against modification of the recorded data and against access of the registered data by unauthorized persons

CHAPTER 7 CARRYING OUT INVESTIGTORY ACTIVITIES IN AN AUTOMATED WORK

Article 23 Installation of a technical device

[1.] The installation of a technical device in an automated work shall be carried out by an investigating officer of a technical team.

[2.] The investigating officer shall, when installing a technical device, limit its operation to the functionality or functionalities specified in the warrant.

[3.] The investigating officer shall prepare a report regarding the installation of the technical device, which shall be sent to the public prosecutor.

[4.] If an irregularity occurs at the time of the installation of a technical device, the investigating officer shall state this in the report

Article 24 Carrying out the investigatory activities

[1.] The carrying out of investigatory activities in an automated work shall be done by an investigating officer of a technical team.

[2.] The investigating officer shall prepare a report regarding the carrying out investigatory activities which shall be sent to the public prosecutor.

[3.] If an irregularity occurs during the investigatory activities, the investigating officer shall state this in the report

Article 25 Removal of a technical device

[1.] A technical device shall be removed from an automated work as soon as a warrant has been executed or no later than once the period specified in the order, within which the order is to be executed has expired.

[2.] The removal of a technical device shall be carried out by an investigating officer of a technical team.

[3.] The investigating officer shall prepare a report of the removal, which shall be sent to the public prosecutor.

Article 27 Recording of data on a technical infrastructure

[1.] The recording of data during the investigation takes place on a technical infrastructure.

[2.] A technical infrastructure shall be designed in such a way that the unique data recorded by a technical device is recognized when data are recorded.

[3.] A technical infrastructure shall be designed in such a way that the date and time of commitment are recorded when the data are recorded.

Article 28 Reliability and integrity of a technical infrastructure

[1.] The content of the data recorded on a technical infrastructure shall not be changed.

[2.] The data recorded shall be accessible only to officials appointed by the Chief of Police.

[3.] When recording data, measures shall be taken to prevent the modification or access to the recorded data by unauthorized persons and measures shall be taken to be able to determine afterwards whether any modification or unauthorized access has taken place.

CHAPTER 8 PROVISION OF DATA RECORDED DURING EXECUTION OF A WARRANT

Article 29 Provision and processing of recorded data

[1.] The secured data stored on a technical infrastructure order, referred to in Article 27, shall be provided to an investigating officer responsible for the investigation.

[2.] Where it is necessary to make a selection from data recorded on a technical infrastructure, an investigating officer of a technical team shall carry out an editing using a copy of the data recorded on the technical infrastructure pursuant to Article 27. The processed information shall be provided to an investigating officer responsible for the investigation.

[3.] When selecting data, an investigating officer from a technical team shall record the editing carried out in respect of the copy of the recorded data in a report, that is sent to the public prosecutor.