THE CHANGING DUTCH LEGAL FRAMEWORK OF THE SEARCH AND SEIZURE OF SMARTPHONES

The extent and conditions in which investigation officers in the Netherlands can seize and search automated works, and the changing legal framework in the proposed amendment of the Dutch Criminal Code of Procedure

Law and Technology
Master Thesis

Viviana Minneboo
ANR: 636696
SNR: u1266482

Supervisor: Dr. Maša Galič
Second Reader: Lucas Jones

Table of Contents

List of Abbreviations

AG	Advocate-General
CCP	Criminal Code of Procedure
DPC	Dutch Penal Code
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
JOA	Judicial Organization Act
Innovation Bill	Consultation Bill of Innovation of the Dutch Criminal Code of Procedure
Koops-Committee	The Committee on Modernization of Investigation in the Digital Age
PDA	Personal digital assistant
WODC	Wetenschappelijk Onderzoek- en Documentatiecentrum (in English: Scientific Research and Documentation Centre)

1. Introduction chapter

1.1 Background

"*We used to say a man's home is his castle. Today a man's phone is his castle*" (Snowden 2016). Snowden perfectly describes our rapid changing digital world. Aspects of our private life, such as our photos, conversations, documents, bank details, and contacts, can be stored on the electronic devices that we carry with us constantly. Therefore, "a man's phone" can be compared with how we feel about our private home. The content which can be found on these electronic data carriers or automated works -which includes devices such as computers, servers, modems, routers, as well as smartphones and tablets-[1] can be of great importance during a criminal investigation. The impact of this content can be illustrated by the following Dutch case.

Earlier this year the lower court of Noord-Nederland partly based their judgment that a woman murdered her husband, on digital evidence.[2] This digital evidence was seized from her smartphone, searched, and then compared to her statements. In this case, a man was found murdered in a meadow, with no suspects. His wife stated that on the night of the murder, she went to meet her husband, but she could not find or reach him. After this, she called her father-in-law and searched with him for her husband. Based on the information that her smartphone contained, the police could reconstruct her movements at the night of the murder. Furthermore, they were able to verify her statements by searching her messages and telephone calls around the time of the murder. After comparing the evidence on the smartphone to the suspect's statements and reconstruction of the night, the police accused the woman of murdering her husband.

The information on her smartphone showed that the wife was at the crime scene at the time of the murder. Additionally, it indicated that she did not attempt to contact her husband during her search, whereas before the murder she regularly reached out to him by phone. The court found it unlikely that she would not call her husband during her search. As a consequence, the smartphone evidence made law enforcement doubt the veracity of her statements, which led the court to conclude they were false.

[1] Supreme Court, 26th of March 2013, ECLI:NL:HR:2013:BY9718.
[2] Lower Court of Noord-Nederland, 11th of July 2019, ECLI:NL:RBNNE:2019:2986.

This judgment illustrates the relevance of accessing information, which can reveal a lot about a person's private life and can also be used to (in)validate a suspect's statement. Accordingly, it is essential to understand how the search and seizure of a smartphone is regulated in Dutch law. In particular how the search and seizure of a smartphone correlates to an intrusion of the right of privacy and how this invasion is safeguarded in the Dutch law.

In Dutch law, there is a provision that legitimates searching homes but there is as yet no explicit provision for the search and seizure of data carriers and automated works. Articles 94, 95, and 96 of the Dutch Criminal Code of Procedure (hereafter: CCP) legitimatizes the search of seized objects.[3] Investigating officers base their legality for seizing data carriers and automated works on these articles by comparing these with objects.[4] Without an explicit provision for seizing and searching electronic data carriers and automated works, the Dutch Supreme Court needed to answer, whether the principle of legality is complied with by the investigation powers on these Articles.

In its most important ruling in this regard from 2017, the Dutch Supreme Court decided that the existing law does not require an explicit criminal procedural provision to conduct searches on seized electronic data carriers and automated works by an investigating officer.[5] If the invasion of privacy associated with the investigation can be considered limited, the general authority of investigation officers laid down in Article 94 in connection with Articles 95 and 96 of the CCP can be considered sufficient legitimacy. This may be the case if the investigation solely focuses on a small amount of specific data stored on the electronic data carrier or computer.[6] However, if the investigation is far-reaching, in the sense that a more or less complete picture of certain aspects of the personal life of the smartphone user has been obtained, the investigation can be illegitimate.[7]

After this ruling, the Dutch Supreme Court repeated and confirmed this part of the principle of legality by evaluating if an investigation, based on articles 94, 95 and 96 of the CCP, was illegitimate in the sense that a more or less complete picture has been obtained of a part of the

[3] Articles 94, 95 and 96 of the Dutch Criminal Code of Procedure (from here: CCP).
[4] Supreme Court, 29th of March 1994, ECLI:NL:HR:1994:AD2076.
[5] Supreme Court, 4th of April 2017, ECLI:NL:HR:2017:592, ro. 2.6.
[6] Supreme Court, 4th of April 2017, ECLI:NL:HR:2017:592, ro. 2.6.
[7] Supreme Court, 4th of April 2017, ECLI:NL:HR:2017:592, ro. 2.6.

personal life of the user of the electronic data carrier while investigating the seized electronic data carrier.[8]

The Dutch legislator intends to modernize the Criminal Code of Procedure.[9] Earlier this year, the legislator proposed a consultation Bill of Innovation of the Dutch Criminal Code of Procedure, which is called "Innovation Bill criminal proceedings" (the Innovation Bill).[10] This proposal ensures that in anticipation of the new Criminal Code of Procedure to enter into force – if it indeed becomes law – some relevant topics for criminal law practice already can be applied in order to gain experience, coming into force on 1 January 2021.[11] In this bill, the Dutch legislator proposed specific provisions as a legal basis for the search and seizure of data carriers and automated works, whilst simultaneously laying the foundation for network searches in automated works present elsewhere. It furthermore aims to broaden the authority on how data carriers and automated works can be searched.[12]

1.2 Problem statement

The Dutch government drafted a new bill for the Criminal Code of Procedure, because of existent developments in our digitally changing world and the need for an explicit legal basis for these changes.[13] Therefore, this research will focus solely on how the search and seizure of smartphones in the Netherlands is regulated. Before the new modernized Criminal Code of Procedure is going to enter into force, the legislator wants to introduce some specific Articles in the current Criminal Code of Procedure (i.e. the Innovation Bill). The Dutch legislator based these broadening Articles on several recommendations from an investigation report of the Committee on Modernization of Investigation in the Digital Age (Koops-Committee).[14] The Innovation Bill contains two recommendations which refer to the network search, which is the search in an automated work that is located elsewhere after the seizure of that automated work, and the perusal of data after the seizure of this automated work. Although the legislator based the Articles on the recommendations of the Koops-Committee, several concrete elements of the

[8] Supreme Court, 10th of July 2018, ECLI:NL:HR:2018:1121; Supreme Court, 18th of December 2018, ECLI:NL:HR:2018:2323; Supreme Court, 9th of July 2019, ECLI:NL:HR:2019:1079.
[9] *Kamerstukken II* 2017/18, 29279, nrs. 395, 402.
[10] *Kamerstukken II* 2018/19, 29279, nr. 501.
[11] *Kamerstukken II* 2018/19, 29279, nr. 501, p.4.
[12] 19th of July 2019, Concept regeling, Wetsvoorstel Innovatiewet Strafvordering, www.internetconsultatie.nl.
[13] 7th of February 2017, Memorie van Toelichting: Vaststellingswet Boek 1 van het nieuwe Wetboek van Strafvordering: strafvordering in het algemeen, p. 1.
[14] Commissie modernisering opsporingsonderzoek in het digitale tijdperk, Regulering van opsporingsbevoegdheden in een digitale omgeving, s.l. 2018, p.89-94.

committee's advice are overlooked. For instance, specific details on the kind of research or the extent of research are not included. The Koops-Committee provided recommendations for the extent of the search of the seized automated works where it also took the recent "smartphone" rulings of the Dutch Supreme Court into account about the extent of the intrusion on the privacy of a suspect.[15]

This Innovation Bill means that for testing parts of the new Code of Criminal Procedure, it is possible to deviate from provisions in the current legislation.[16] It seems however that the proposed bill still lacks specification and does not include crucial guarantees for the right to privacy which need to be examined further before this bill can become law. To contribute to the creation of a solid legal ground for the search of seized data carriers and automated works, this research will address the extent and conditions of the current legal framework and examine the proposed changes in the proposed Bill of Innovation of the Dutch Criminal Code of Procedure. Accordingly, this study will focus on how the current legal framework will change as a result of the proposed bill, and how this bill addresses the safeguards on the right to privacy if there occurs an intrusion on this right.

1.3 Literature review

During the internet consultation period of the proposed bill, from the 19th of July until August 26th in 2019, various concerns about the scope of the new Articles emerged from the responses of the internet consultation, by Bits of Freedom and the Council for the Judiciary Advice.[17] For example, Article 556 which provides a legal basis to use or record information that is still available at the time of seizure which did not appear on the seized automated work.[18] The lack of clarity about whether or not to take cognizance of the content of these messages by the search is undesirable. Furthermore, there are concerns about the amount of information which can be collected based on the new provisions. This potentially interferes with the right to privacy of citizens and suspects, whereas the guarantees remain unchanged. Houwing states that the

[15] Supreme Court, 4th of April 2017, ECLI:NL:HR:2017:584, ro. 2.6., Supreme Court, 10th of July 2018, ECLI:NL:HR:2018:1121, Supreme Court, 18th of December 2018, ECLI:NL:HR:2018:2323, Supreme Court, 9th of July 2019, ECLI:NL:HR:2019:1079; Commissie modernisering opsporingsonderzoek in het digitale tijdperk, Regulering van opsporingsbevoegdheden in een digitale omgeving, s.l. 2018, p. 89-94.
[16] Kamerstukken II 2018/19, 29279, nr. 501, p.4.
[17] Council for the Judiciary Advice Amendment to the Code of Criminal Procedure, 2th of October 2019; Houwing, L, Reactie op consultatie Innovatiewet Strafvordering, Bits of Freedom, 22th of August 2019.
[18] Council for the Judiciary Advice Amendment to the Code of Criminal Procedure, 2th of October 2019, p. 2-3; Houwing, L, Reactie op consultatie Innovatiewet Strafvordering, Bits of Freedom, 22th of August 2019, p. 2-4.

balance between the committed intrusion and the guarantees threatens to be disrupted.[19] Considering that the Innovation Bill also transfers several investigation powers from the prosecutor to the assistant-prosecutor, it shows a trend of down-scaling guarantees rather than tightening the safeguards to balance the investigation powers and the intrusion.[20]

1.4 Research questions

Based on this problem statement and literature review, the following question will be answered: *"To what extent and under which conditions can the police in the Netherlands search seized automated works, especially based on the recent "smartphone judgments", and how will this legal framework change in the proposed amendment of the Dutch Criminal Code of Procedure (Innovation Bill)?"*

To answer the main research question, the following sub-questions must be answered:

1. *Under which conditions can automated works be seized and searched under the current Dutch criminal procedure law and how does this legal framework relate to the right to privacy of the suspect?*
2. *Why was there a need for an Innovation Bill and in which ways do the recommendations of the Koops-Committee add value to this Innovation Bill and the Dutch legal framework for the search and seizure of automated works?*
3. *To what extent will the current legal framework for the search and seizure of automated works change in the proposed amendment of the Dutch Criminal Code of Procedure (Innovation Bill)?*

1.5 Methodology and methods

For answering the main research question a desk research will be conducted, which will focus on a better understanding of the current changing legal framework for the search and seizure of data carriers and automated works. Therefore, a doctrinal legal analysis will be conducted by providing a descriptive and detailed analysis, which is composed of legal rules found in primary sources to understand the current legal framework for the search and seizure of data carriers

[19] Houwing, L, Reactie op consultatie Innovatiewet Strafvordering, Bits of Freedom, 22th of August 2019, p. 2-4.
[20] Houwing, L, Reactie op consultatie Innovatiewet Strafvordering, Bits of Freedom, 22th of August 2019, p. 2-4.

and automated works. The main purpose of this analysis is to understand the flaws in the current legal framework. The primary sources which are consulted are regulations, such as the provisions of the current Dutch Criminal Code of Procedure in combination with the prevailing doctrine in case law, and Article 6 of the European Convention on Human Rights (hereafter: ECHR), and court cases generated under these Articles. To understand how this current legal framework can be improved, a literature review will be conducted which mainly focuses on the recommendations from the Koops-Committee on the search and seizure of data carriers and automated works. Furthermore, a critical analysis of the Articles of the Innovation Bill will be made, by conducting a descriptive and detailed analysis of these Articles, which is composed of the wording of the Articles of the Innovation Bill and the explanatory memorandum on the current and future legislative proposals on modernizing the Dutch Criminal Code of Procedure (hereafter: CCP). These Articles will also be analyzed by comparing these to the research and recommendations of the Koops-Committee concerning the Articles of the Innovation Bill, and by conducting a literature review.

The analysis is limited to the provisions based in the Innovation Bill alone, and will not research the entire range of changes considered in the modernization of the Dutch Criminal Procedure Code, because these provisions are still under consideration.

1.6 Structure of the chapters

This research will have the following structure. In chapter 2, the investigation authority of the search and seizure of data carriers and automated works is broadened, with a focus on the recent "smartphone judgments". Furthermore, this chapter focuses on how this will reflect on the right to privacy of a suspect. After the basis for the search and seizure of the data carriers and automated works has been addressed, chapter 3 will focus on the recommendations of the Koops-Committee to improve the current Dutch legal framework on the search and seizure of automated worrks. In chapter 4 the proposed changes of the Innovation Bill are discussed and it will be further examined how the change of the legal framework will influence the conditions of the search and seizure of automated works.

2. The Dutch legal framework for the search and seizure of automated works

Whilst our digital world is rapidly increasing, our digital footprint is changing with it. This means that nowadays our smartphone can contain more and more personal information. For instance, just going to work can mean that you send a message to a friend that you are leaving home, you can check if your train has not been delayed, and meanwhile you read the news on your smartphone or make a quick picture where you at. During this trip, you can check your e-mail, apps like Facebook or LinkedIn, and put on music whilst you send even more messages. All of this above can mean that your smartphone already collected information about your whereabouts, stored your pictures, personal messages, and information about your last opened apps and remembers what you have searched for via your browser. Our digital footprint via our smartphone has therefore expanded rapidly. This also means that our smartphone contains information that can be relevant for investigations in criminal cases. By searching the relevant information, this information can also contain a lot of private information where this search can infringe on a suspects' private life. Therefore, the police need investigatory powers, with limitations and safeguards, set in law to be able to legitimate an intrusion upon a person's privacy. This chapter will focus on how these investigatory powers are laid down under Dutch law, which will lead to the answering of the sub-question: "*Under which conditions can automated works be seized and searched under the current Dutch criminal procedure law?"*

2.1 Data carriers or automated works

The Dutch Code of Criminal Procedure and the Dutch Penal Code (hereafter: DPC) both use different terms under which a smartphone can fall under. The terms: data carrier and automated works are both mentioned in both of the Dutch Codes. In this thesis both of the terms of data carrier and automated works will be mentioned. Therefore, for a better understanding about how a smartphone may fit in both of these terms, these need to be further explained.

Data carrier

The term data carrier does not have a specific Article in which the term has been defined. But the term "data carrier" is very comprehensive. A "data carrier" is an object on which data may be or have been stored. Data as such are immaterial and abstract. In order to be captured, they

must be attached to a medium.[21] This means that, in case of a smartphone, an electronic data carrier, the scope will reach to the data which are stored on a smartphone.

Automated works

The term automated work has been laid down in Article 80sexies DPC which defines an automated work as a device designed to store, process and transfer data electronically. In 2013 the Supreme Court ruled that following legal history the concept of automated work is not limited to devices that autonomously fulfill the accumulation of functions, i.e. storage, processing and transfer of data. In the opinion of the Supreme Court, the legislator also wanted to include networks consisting of computers and/or telecommunication facilities under the term 'automated work'. Automatic processing of computer data on the basis of a program is an essential requirement. Computers, servers, modems, routers, as well as smartphones and tablets fall under this definition.[22] From the first of March 2019, this changed into: *"Automated work means any device or group of inter-connected or related devices, one or more of which process computer data automatically on the basis of a program"*.[23]

In the "smartphone-judgements" both terms are used, but the term of automated works is more in line with the smartphone we have nowadays. A smartphone can both store, process and transfer data. In the newest Article 80sexies DPC, it fits the term of a device which processes computer data automatically on the basis of a program. In the beginning of this century, the smartphone was not as developed as it is nowadays, and a lot of jurisprudence and works still refer to the (electronic) data carrier. Since, the Innovation Bill uses the term "automated works" where it also refers to smartphones, this research will both mention electronic data carriers, and automated works.

2.2 The Dutch provisions for search and seizure in the Dutch Criminal Code of Procedure

The Dutch Code of Criminal Procedure (CCP) consists of various articles that give the police the competence to seize objects. Article 94 CCP states which objects may be seized,[24] in combination with the authorization powers in Articles 95, 96, and 104 CCP to confiscate those

[21] *Kamerstukken II* 1991/92, 21551, nr. 11, p. 4.
[22] Supreme Court, 26th of March 2013, ECLI:NL:HR:2013:BY9718.
[23] Art. 80sexies Dutch Penal Code.
[24] Art. 94, paragraph 1 Dutch Code of Criminal Procedure: "Susceptible to seizure are all objects that can serve to show the truth ...".

objects.[25] Since data as such are not considered to be objects, the legal basis for the exercise of the competence means that the data carriers and automated works as such can be seized, and therefore the Articles of the CCP allows for the search of the data on it. This legal basis follows from the case law of the Dutch Supreme Court.[26] Investigating officers may, in the event of seizure, search seized objects in order to obtain information for the criminal investigation, which the Supreme Court ruled in 1985. Advocate-General Meijers also concluded this before the judgment: *"As a rule, the use of the means of seizure is only effective, if the power of seizure is understood to be as a search of the seized object. If necessary, and in the least harmful manner, seized objects will be used or dismantled during the search".*[27] Furthermore, the Supreme Court stated in this early ruling that computers and other electronic data carriers are found not to be excluded from this Article, which means that the and search and seizure of electronic data carriers can be based on these provisions.[28]

However, the power to search data as such does not only follow from Article 94 CCP but can also be derived from the relation with other provisions as mentioned above, which gives the authorization to seize these objects to certain persons.[29] If the police arrests of sustains a suspect Article 95 CCP gives the law enforcement the competence to seize objects that a suspect carries with him if these objects are susceptible to seizure by Article 94 CCP.[30] Article 96 CCP allows an investigation officer the competence to seize the objects that may be seized by Article 95 CCP and to enter any place for that purpose.[31] This is allowed in the event of either an in flagrante delicto criminal offense, which means that the police caught a criminal in the act of committing an offense or in the event of suspicion of a crime as described in Article 67 CCP,

[25] Art. 95, first paragraph, Dutch Code of Criminal Procedure: "*He who arrests or sustains the suspect can confiscate objects susceptible to seizure carried with them*.", Art. 96, first paragraph, Dutch Code of Criminal Procedure: "*If a criminal offense is discovered in the act or the event of a suspicion of a crime as described in Article 67, paragraph 1, the investigating officer is authorized to confiscate the susceptible objects and to enter any place for that purpose*.", Art. 104 Dutch Code of Criminal Procedure: "*The investigatory judge is authorized to seize all susceptible objects. Except where he carries out investigation acts according to Articles 181 to 183, seizure by the* investigatory judge *only takes place at the request of the public prosecutor*.".
[26] Supreme Court, 8th of October 1985, ECLI:NL:PHR:1985:AC0537, m.nt. A.C. 't Hart.
[27] Supreme Court, 8th of October 1985, ECLI:NL:PHR:1985:AC0537, m.nt. A.C. 't Hart, ro. 14.1.
[28] Supreme Court, 8th of October 1985, ECLI:NL:PHR:1985:AC0537, m.nt. A.C. 't Hart.
[29] Gritter, E., 'Opsporing in de digitale wereld: het onderzoek van in beslag genomen gegevensdragers', (2016) Delikt en Delikwent 43.
[30] Art. 95, first paragraph, CCP: "*He who arrests or sustains the suspect can confiscate objects susceptible to seizure carried with them*.".
[31] Art. 96, first paragraph, CCP: "*If a criminal offense is discovered in the act or the event of a suspicion of a crime as described in Article 67, paragraph 1, the investigating officer is authorized to confiscate the susceptible objects and to enter any place for that purpose*.".

which states the crimes which allow contemporary custody. The investigatory judge can also authorize the seizure if the public prosecutor requests it by an act of investigation.[32]

2.3 The Smartphone-judgments and the right to privacy of Article 8 of the ECHR

Article 134 of the CCP regulates the seizure of an object as the seizing of or keeping an object for criminal proceedings.[33] It does however not provide in a provision or explanation on how this object may be searched and how far-reaching this research may be. Since automated works can contain a lot of private information, it means that Article 8 of the European Convention of Human Rights (ECHR), the right to the private life of a person, can be infringed by searching the seized data carrier.

Article 8 ECHR guarantees the right to respect for private life and family life, home, and correspondence.[34] However, this right is not absolute and can be interfered with, which interference must comply with strict tests to be considered lawful. These can be found in the second paragraph of Article 8, interference can be found namely 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 the protection of the rights and freedoms of others. Limitations are allowed if they are "in accordance with the law" or "prescribed by law" and are "necessary in a democratic society" for the protection of one of the previous objectives.[35]

These limitations, which are allowed if they are "in accordance with the law" or "prescribed by law", can be related to a case, in 1993, where a pocket computer (which is a less advanced smartphone and used as an personal digital assistant)[36] of a suspect was seized and where the Court of Appeal of Amsterdam based their judgment on proof which consisted of seized data

[32] Art. 181 and 183 CCP.
[33] Art. 134, first paragraph, CCP: *"The seizure of any object is understood to mean the seizure or retention of that object for criminal proceedings."*
[34] Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) (ECHR) art 8: *"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 for 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."*
[35] Council of Europe/European Court of Human Rights, 2019, Guide on Article 8 of the Convention – Right to respect for private and family life, p. 9.
[36] Personal digital assistant (PDA): a small portable device that combines computer, telephony, fax and network functions, which mainly serves as a cell phone and digital agenda. It can be considered as a forerunner of the smartphone.

that was stored in -the secret memory of- the pocket computer.[37] The defense did not agree with this judgment and took the case to the Supreme Court since they believed that seizing the data -of the secret memory- of the pocket computer can be considered being in contradiction with Article 8 ECHR. In 1994 the Supreme Court, therefore, needed to conclude if the seized data that was stored in -the secret memory of- a pocket computer was in fact at variance with the provision of Article 8 of the ECHR.[38] It should be noted that the plea in this case also focused on the alleged lack of a legal basis for the search. The Supreme Court rejected the plea considering that:

"according to the official reports (...) the seizure of the relevant pocket computers, which were held by the suspect and held by the fellow suspect "G.G." during their arrest, took place based on the provisions of Articles 95 and 96 CCP and that to find the truth, searches may be carried out on seized objects, to obtain data for the criminal investigation, where data stored in computers are not exempted therefrom."[39]

The quality of the legal basis is important here. In this context, the ECtHR attaches importance to the existence or absence of a prior judicial review of the decision to conduct the searches.[40] This means that an investigatory judge should, before issuing an order to conduct the investigation, consider whether the impact that the investigation will have on a suspect's privacy can be infringed and to what extent this is allowed. Such a prior check is not yet provided for in the Netherlands, which means that investigating officers are allowed to conduct the search on a seized smartphone. There is, however, the possibility that the court that will later adjudicate the case will afterward assess the legality of the search and attach legal consequences to it. The question is whether this possibility can compensate for the lack of a prior judicial review.[41] This question has finally been answered by the Supreme Court in 2017 where the Supreme Court ruled on three "Smartphone-judgments".[42] These three rulings were ruled on the same day, the

[37] Court of Appeal of Amsterdam, 30th of March of 1993.
[38] Supreme Court, 29th of March 1994, ECLI:NL:HR:1994:AD2076
[39] Supreme Court, 29th of March 1994, ECLI:NL:HR:1994:AD2076, ro. 9.3. (translation made by the author of this thesis).
[40] ECtHR Modestou v. Greece, 16th of March 2017, nr. 51693.13, p. 44 & 54-55, ECtHR Harju v. Finland, 15th of February 2011, nr. 56716/09; ECtHR Petri Sallinen v. Finland, 27th of September 2005, nr. 50882/99.
[41] Opinion of AG Bleichrodt, 25th of October 2016, ECLI:NL:PHR:2016:1047.
[42] Supreme Court, 4th of April 2017, ECLI:NL:HR:2017:584; Supreme Court, 4th of april 2017, Supreme Court, 4th of April 2017, ECLI:NL:HR:2017:592.

fourth of April of 2017, and are largely identical but only differ in application to the specific case. Therefore, references will only be made to one of these three rulings.[43]

In the ruling of the fourth of April of 2017, the Dutch Supreme Court divided the intrusion on the right to privacy into three categories, one where there is a limited intrusion, which allows investigating officers to search data carriers and automated works to the extent of a limited number of specific stored of available data.[44] The second situation is when a more than limited intrusion has arisen when the search obtains a more or less complete picture of certain aspects of the personal life of the user of the data carrier. This intrusion is only allowed if this search is approved by a public prosecutor. The most significant violation can occur if, in advance, it is foreseeable that by searching the data carrier will conclude a far-reaching invasion on the right of privacy. For the search that can cause this intrusion, it has to be approved by an investigatory judge.

2.3.1 The way a search can be conducted

In what way the search that caused the intrusion is conducted is also important. The Dutch Supreme Court gives two examples. A minor violation occurs if the search only consists *of consulting a small* number of specific data stored or available on the electronic data carrier or in the automated work.[45] A more significant violation can particularly be the case when it concerns the search *of all data* stored or available in the electronic data carrier or the automated work *using technical aids*. How this violation can be determined is not yet foreseeable, which gave room for discussion of this determination in the literature. For example, Van der Voort states that how police officers search data carriers and automated works on average always gives more information then, for example, by the use of a telephone tap for research, so the amount of data that can be obtained from a data carrier cannot be put in the same area as other search opportunities.[46] Stevens puts it in a different perspective – it is the nature of the information that will play a decisive role in determining a possible privacy violation.[47] For which information this is and in which category of intrusion it falls following the "smartphone-judgments", Stevens pleas for making a categorization overview of judgments in which seized

[43] Supreme Court, 4th of April 2017, ECLI:NL:HR:2017:592.
[44] Supreme Court, 4th of April 2017, ECLI:NL:HR:2017:592
[45] Supreme Court, 4th of April 2017, ECLI:NL:HR:2017:592, r.o. 2.6.
[46] Van der Voort, N., Onderzoek aan een in beslag genomen smartphone: het labyrint van de (toekomstige) wetgeving en jurisprudentie, (2017) Tijdschrift voor Bijzonder Strafrecht en Handhaving.
[47] Stevens, L., 'Onderzoek in een smartphone: zoeken naar een redelijke verhouding tussen privacybescherming en werkbare opsporing', (2017) Ars Aequi, p. 730-735.

data were obtained and which kind of intrusion occurred. This overview could help for making decisions in future individual matters. Therefore, the next paragraphs will focus on the judgements where the ruling refers to either a limited intrusion or a more then limited intrusion on the privacy of a subject.

Dutch case law after the "Smartphone-judgments"

There is as yet only a couple of court cases available that have ruled on the intrusiveness of a search of a data carrier. In order to understand the cases, a better understanding of the Dutch judicial system is needed. In the Netherlands, the judicial system consists of a lower Court, a Court of Appeal, and a Supreme Court. The Lower and the Court of Appeal are fact-finding courts. The lower Court will base its judgment on all of the relevant facts within the criminal procedure and on applying the rule of law. If an accused person does not agree with the lower Court, he will still be able to appeal, after which the Court of Appeal will once again assess all the facts of the case (and apply the rule of law). If a suspect still does not agree with the fact-finding court (the Court of Appeal), he can appeal in cassation. The Supreme Court does not look again at the facts of a criminal case, but will only examine whether the lower Court has applied all the rules of the law correctly. In cassation, an Advocate-General (in short: AG) will first give an opinion of the case to the Supreme Court, after which the Supreme Court will pass their judgment.

Limited intrusion on the right to privacy

The following three cases consist of limited intrusiveness' of the searches. One 2017 Supreme Court ruling[48], is about a single WhatsApp-conversation which led to a house search. The search of the smartphone was conducted manually by a police officer and yielded no more than several missed phone calls, messages, and WhatsApp messages. Later on, the smartphone has also been read with specific forensic equipment. According to the AG Harteveld, this intrusion could still be considered to be legitimate and based on Article 94 because the first intrusion was of a minor nature.[49] This ruling led to the application of Article 81 of the Judicial Organization Act (hereafter: JOA). This Article allows the Supreme Court to refer to this Article in their judgment if the Supreme Court finds that a submitted complaint cannot lead to a reversal by the Supreme Court and does not require an answer to legal questions in the interest of the legal

[48] Supreme Court, 4th of November of 2017, ECLI:NL:HR:2017:2869.
[49] Opinion of AG Harteveld, 26th of September of 2017, ECLI:NL:PHR:2017:1245

unity or the legal development.[50] The Supreme Court is therefore not required to address the objections further.

In a 2018 Supreme Court ruling,[51] a police officer unlocked a smartphone of a suspect by swiping the screen, which was not protected by a password. During this, he looked at the videos that the smartphone contained and one of these videos was used as evidence. This case also ended with the application of article 81 JOA of the Supreme Court. AG Bleichrodt further explained this conclusion.[52] He stated that the Court of Appeal ruled that in the present case no situation has occurred in which a more or less complete picture has been obtained of certain aspects of the personal life of the accused so that the involvement of the public prosecutor or the investigatory judge in the investigation on the telephone was not required. The Court of Appeal had taken into account that in this case there was no investigation into all data stored or available on the smartphone, whilst it also follows from the evidence that no technical tools were used to take note of the data stored on the smartphone; the telephone of the defendant could be unlocked without an access code and the photo and video files were not secured with an access code. In this view, the AG states that the Court of Appeal has evidently and not incomprehensibly deduced from the aforementioned official reports that this was a manual investigation that resulted in no more than a minor invasion of privacy.[53]

Another 2018 Supreme Court ruling,[54] was about a 'focused look' by a police officer of a photo gallery of a suspect's smartphone. The Court of Appeal held that Article 94 CCP provides a sufficient basis for the seizure of the smartphone and that, given the suspicion that had arisen, the search of that phone is not only necessary but also proportionate.[55] It concluded that the targeted viewing of photographs in the photo gallery of the accused's smartphone does not constitute a more than limited invasion of privacy, as referred to in Article 8 of the ECHR. The AG Vegter alluded to the possibility that the photo gallery consisted of hundreds or thousands of photos so that this could be an indication of more than a limited search.[56] But that was not argued by the defense and did not receive an explicit ruling from the Supreme Court which ruled that the judgment of the Court of Appeal does not

[50] Article 81 of the Judicial Organization Act.
[51] Supreme Court, 23th January of 2018, ECLI:NL:HR:2018:71.
[52] Opinion of AG Bleichrodt, 28th of November 2017, ECLI:NL:PHR:2017:1470, ro. 26.
[53] Opinion of AG Bleichrodt, 28th of November 2017, ECLI:NL:PHR:2017:1470, ro. 26.
[54] Supreme Court, 10th of July of 2018, ECLI:NL:HR:2018:1121.
[55] Court of Appeal of Amsterdam, 12th of September 2016. ECLI:NL:GHAMS:2016:3676.
[56] Opinion of AG Vegter, 15th of May 2018, ECLI:NL:PHRL2018:764.

testify to an error of law, is not incomprehensible and, also because of what has been put forward by and on behalf of the accused in this respect, is adequately substantiated.

From these cases it can be concluded that a limited intrusion of the right to privacy can occur if the search only consists of a manually focused look, which can be a more targeted viewing of photographs in photo gallery, or missed calls and viewing messages or WhatsApp Messages.[57] However, this could be a more than limited search if this consists of hundreds or thousands of photos.[58] Or in the case of a search of all data stored or available on the smartphone. However, in the first case of 2017 the AG concluded that the latter use of special forensic equipment could, if the first intrusion has already been made, nevertheless means that there is only a case of a limited intrusion of privacy.[59] Whereas in 2018 the AG concluded somewhat differently, that is if technical tools were used to take note of the data stored on the smartphone, this can lead to a more then limited intrusion of privacy.

A more than limited intrusion of privacy

The following two Supreme Court cases focuses on the reasoning behind determining a more than limited intrusion of privacy.

The Supreme Court ruled the 18th of December 2018 that if a search has been conducted, it should be determined whether a more than limited intrusion of privacy had been made with the further search. [60] In this case the Court of Appeal had established that the search was carried out using technical tools into data stored or available in the smartphone, in particular into photographs, film files, and WhatsApp calls, as a result of a video file found during a so-called quick scan that gave rise to the suspicion that the smartphone contained child pornography images.[61] Because of the "Smartphone judgment of 2017", the Court of Appeal should, therefore, have established, when assessing whether art. 94 of the CCP constitutes a sufficient legal basis for the further investigation carried out by the investigating officers into

[57] Supreme Court, 10th of July of 2018, ECLI:NL:HR:2018:1121.; Court of Appeal of Amsterdam, 12th of September 2016. ECLI:NL:GHAMS:2016:3676; Supreme Court, 4th of November of 2017, ECLI:NL:HR:2017:2869.
[58] Opinion of AG Vegter, 15th of May 2018, ECLI:NL:PHRL2018:764.
[59] Supreme Court, 4th of November of 2017, ECLI:NL:HR:2017:2869; Opinion of AG Harteveld, 26th of September of 2017, ECLI:NL:PHR:2017:1245.
[60] Supreme Court, 18th of December 2018, ECLI:NL:HR:2018:2323.
[61] Court of Appeal of Amsterdam, 25th of January 2017, ECLI:NL:GHAMS:2017:216.

the confiscated smartphone of the defendant, whether that investigation constituted a more than limited invasion of privacy.

Furthermore, in the latest Smartphone-judgment of the Supreme Court of the 9th of July,[62] the Supreme Court ruled that the reasoning of the Court of Appeal of Arnhem-Leeuwarden was not sufficiently substantiated. Regarding the provisions of the "Smartphone judgments" the Supreme Court took into account that the Court of Appeal of Arnhem-Leeuwarden did consider that "the police were selective in the investigation on the smartphone", but that it did not establish based on which and with a view to which, a selection, which included at least all stored photographs and films, was made.[63] However, this did not lead to cassation because the Supreme Court took into account that an unjustified infringement of the right guaranteed by the first paragraph of Article 8 of the ECHR in the criminal proceedings against the accused does not necessarily have to have legal consequences and that the defense has not sufficiently substantiated that a situation arises in the present case in which the application of exclusion of evidence must be considered necessary. The Court of Appeal could therefore only have rejected that defense.

AG Jorge posits that his judgment brings a refinement of the somewhat coarse measure of the use of technical means and/or software to investigate or secure the entire contents of a smartphone, for which investigators are not competent without a court order or authorization. This is because the mere possibility of examining the content of a smartphone does not yet provide a more or less complete picture of certain aspects of the user's personal life. This will be the case if the content is investigated in a non-targeted way and if specific information is searched for.[64]

2.3.2 The legal effect of the intrusion on the right to privacy

The smartphone-judgments also referred to the rules laid down for the determination of whether the result of the obtained evidence has caused an infringement of the right to privacy and what kind of legal effect this must-have. The Supreme Court referred to the 2013 judgment,[65] in which the Supreme Court formulated rules for the application of the exclusion of evidence as a legal consequence of a procedural defect as referred to in art. 359a of the

[62] Supreme Court, 9th of July 2019, ECLI:NL:HR:2019:1079.
[63] Court of Appeal of Arnhem-Leeuwarden, 14th of July 2017, ECLI:NL:GHARL:2017:6069.
[64] Supreme Court, 9th of July 2019, ECLI:NL:HR:2019:1079, m.nt. N. Jorge.
[65] Supreme Court, 19th of February 2013, ECLI:NL:HR:2013:BY5321.

Code of Criminal Procedure concerning evidence obtained directly as a result of a certain formal defect. It can lead to the exclusion of evidence, penalty reduction, or merely stating the observation of the proof of absence. According to the research of the WODC 2017, by Devrou et al., an appeal on having a legal effect for the application of exclusion of evidence, will often prove successful.[66] In most cases, the courts will simply state that the evidence is obtained directly as a result of a certain formal defect without giving it a particular legal effect. It can be said that it is still unclear to what extent the search of seized data can occur and if – or when – there is an intrusion on the right to privacy. In the following rulings, there was a more than limited intrusion.

In a 2019 ruling of the Supreme Court,[67] a smartphone was read by a digital forensic officer using forensic software. As a result pictures were found showing the suspect holding a weapon which, given the scratch damage and the serial number, was most likely the weapon which the police had previously seized. The court agreed with the defense that this involved a more than limited infringement of the privacy of the suspect.[68] However, in spite of this infringement, the evidence was not excluded, since it had neither been stated nor had it appeared that the access, by the investigating officers, to private data belonging to the accused had led to any further dissemination of private data or any other concrete disadvantage, other than in the context of the criminal case under investigation. This case ended with the application of article 81 JOA by the Supreme Court.

In a 2019 ruling of the Amsterdam Court of Appeal,[69] the Court granted a penalty reduction as a sanction for a formal failure whilst searching a smartphone instead of the exclusion of evidence. The Court considered that the suspect's telephone was obtained through a claim for extradition. Furthermore, the entire content of the accused's phone had been examined and the files had been read with the aid of technical tools. The manner in which the suspect's smartphone was investigated therefore resulted in a more than limited intrusion of the suspect's privacy. Additionally, no warrant was obtained from a public prosecutor or investigatory judge, although this is required according to the Smartphone judgment of the Supreme Court of 2017.

[66] Devroe, E., Malschm M., Matthys, J. & Minderman, G., *Toezicht op strafvorderlijk overheidsoptreden*, [2017] WODC.
[67] Supreme Court, 11th of June 2019, ECLI:NL:HR:2019:891.
[68] Court of Appeal of Amsterdam, 6th of April 2018, ECLI:NL:GHAMS:2018:1218.
[69] Court of Appeal of Amsterdam, 23thrd of October 2019, ECLI:NL:GHAMS:2019:4341.

The Smartphone Judgements of 4th of April of 2017 got referred back to the Court of Appeal of Amsterdam, and let to another appeal in cassation. This time the appeal concerned the illegality of a smartphone search and the legal consequences attached as stipulated in art. 359a CCP. The appeal was aimed to exclude evidence.[70]

The Court of Appeal of Amsterdam determined that the contents of the smartphone seized by the suspect had been completely read using software, without prior permission from the public prosecutor or the investigatory judge.[71] As a result, there had been more than limited intrusion of the privacy of the suspect with irreparable formal defects. The Court of Appeal argued that the mere observation of that formal defect would suffice, inter alia because the suspect did not specify in detail what his disadvantage consisted of.

On the 5th of November 2019, AG Spronken released his opinion.[72] In his opinion, the AG addressed the question as to what extent the court must (ex officio) investigate the extent of the intrusion, before deciding whether, and if so, which, legal consequences should be attached as referred to in art. 359a CCP. According to him, in the present case, the Court of Appeal failed to attach legal consequences. That is why, according to the AG, the opinion of the court that no disadvantage has been found is not sufficiently reasoned.

However, the Supreme Court did not agree with the AG and ruled in its judgment of the 18th of February 2020 that the Court did sufficiently reason that no legal consequences needed to be attached to the formal default.[73] The Supreme Court took, similarly to the AG, into consideration that the Court of Appeal accounted for the fact that that the defendant had not made concrete in which way the suspect had suffered a disadvantage as a result of the formal default. Only the Court of Appeal took more specific details into account when reasoning that no disadvantage was caused by the formal default. These specific details included; that the investigating officers who carried out the investigation acted in good faith, that the culpability of their actions was low, that there was no situation in which the responsible authorities made insufficient efforts to prevent violations of the relevant rule from the moment at which this "structural failure" must have been known to them, and that the Public Prosecutor, if he had been asked to do so, would have granted permission to search the accused's smartphone.

[70] Supreme Court, 4th of April 2017, ECLI:NL:HR:2017:592.
[71] Court of Appeal of Amsterdam, 23th of April, ECLI:NL:GHAMS:2018:1434.
[72] Opinion of AG Spronken, 5th of November, ECLI:NL:PHR:2019:1121.
[73] Supreme Court, 18th of February 2020, ECLI:NL:HR:2020:123.

Therefore, the Court of Appeal concluded that the formal default was established but that there was no case in which the application of exclusion of evidence qualified,[74] nor was there a disadvantage caused by the formal default that lends itself to compensation by way of reduction of the penalty.[75] Through this judgment, the Supreme Court, therefore, clarified that when there is sufficient reasoning provided by courts (the Lower Court and also the Court of Appeal) they can conclude that no legal consequences need to be attached to a formal default.

3.3 Conclusion

Based on the findings in this chapter data carriers and automated works can be searched and seized based on the Articles 94, 95, 96 and 104 of the CCP. However, for the competence of the search of data carriers and automated works the Dutch Supreme Court divides the conducted searches into different kinds of intrusions which are linked to authorities which can order these specific searches. However, since there are yet not a lot of specific cases on these violations, the extent of this framework is not yet specific enough. From the subjected cases in this research the following restrictions can be derived. If a minor violation occurs when the search only consists of consulting a small number of specific data stored or available on the electronic data carrier or in the automated work, then an investigation officer is allowed to conduct the search. This is the case when a targeted viewing of photographs in a photo gallery takes place or it can be the case when a targeted look at pictures and videos is taken. However, this can be different if the content is investigated in a non-targeted way and if specific information is searched for, which could be an indication of more than a limited search if the search obtains a more or less complete picture of certain aspects of the personal life of the user of the data carrier. Therefore, a more significant violation can particularly be the case when it concerns the search *of all data* stored or available in the electronic data carrier or the automated work *using technical aids*. This intrusion is only allowed if this search is approved by a public prosecutor. The most significant violation can occur if, in advance, it is foreseeable that searching the data carrier will entail a far-reaching invasion on the right of privacy. The search that can result in this intrusion, must be approved by an investigatory judge.

[74] Supreme Court, 19th of February 2013, ECLI:NL:HR:2013:BY5321.
[75] Supreme Court, 30th of March 2004, ECLI:NL:HR:2004:AM2533.

3. The modernization of the Dutch Criminal Code of Procedure

In the previous chapter the current legal framework for the search and seizure of data carriers and automated works has been laid down. This chapter will discuss the modernization of the Dutch Criminal Code of Procedure which is taking place through the Innovation Bill. The discussion will commence by stating how the process of modernization of the Dutch Criminal Code of Procedure takes place, after which it will focus on the relevant recommendations for this research by the Koops-Committee. All of this will lead to answering the sub-question: *Why was there the need for an Innovation Bill and in what way do the recommendations of the Koops-Committee add value to this Innovation Bill and the Dutch legal framework for the search and seizure of automated works?*

3.1 The modernization of the Dutch Criminal Code of Procedure

The Dutch Criminal Code of Procedure came into effect on the first of January 1926.[76] The Dutch legislator realized that the current Criminal Code of Procedure – even when considering the adaptations made after it originally came into effect – cannot respond well to digital changes and considered it therefore advisable get the Criminal Code of Procedure fully up to date.[77] This will not be a revision, but a modernization of the Criminal Code of Procedure. This entails that the system and terminology will be rearranged and organized, the development of law – based on court decisions and societal changes- will be codified and the aim, therefore, is to have a code that can last for a longer period of time.

In the preliminary phase which led to the legislative proposal draft of the innovated Criminal Code of Procedure, extensive consultations were held with organizations within the criminal justice chain[78] to ensure an up-to-date, sustainable and workable proposition. Nevertheless, the final draft of the innovated Criminal Code of Procedure, published for consultation in February 2017, received criticism. This concerned both criticism of more conceptual aspects ("seizure" of data, assignment of authority) as well as practical objections to certain articles or the lack thereof.[79] Shortly after the publication of the consultation version, in April 2017, the Supreme

[76] Stb. 1921, 14 , Stb. 1925, 343.
[77] 7th of February 2017, Memorie van Toelichting: Vaststellingswet Boek 1 van het nieuwe Wetboek van Strafvordering: strafvordering in het algemeen, p. 4.
[78] Organizations within the criminal justice chain: the explanatory memorandum mentions the following parties: the public prosecution service, the Dutch bar association, the judiciary, the police, special investigation services, the personal data authority, victim assistance in the Netherlands and the royal constabulary.
[79] Commissie modernisering opsporingsonderzoek in het digitale tijdperk, Regulering van opsporingsbevoegdheden in een digitale omgeving, s.l. 2018, p. 6.

Court gave their long-awaited ruling on smartphones – the so-called "smartphone judgment",[80] which was received more favorably than the draft legislative proposal.[81]

All this led to the creation of a committee tasked with more fundamental reflection on the criminal investigation in a digital context, more specifically regarding the search and seizure of automated works, the committee for the modernization of investigation in the digital era (the Koops-Committee).[82] In 2018 the Koops-Committee introduced their report and made suggestions for the modernization of the Criminal Code of Procedure. The relevant suggestions for this research – considering the introduced Articles by the Innovation Bill – will be further laid down in the following paragraph.

3.2 Recommendations by the Koops-Committee

The Koops-Committee was set up at the request of the Directorate for Law and Legal Affairs of the Ministry of Justice and Security.[83] The committee has been given the task of advising the minister on whether the statutory regulation of the criminal investigation, as laid down in the draft legislation for the proposal of the modernization of Book 2 of the Criminal Code of Procedure, was satisfactory, or whether it needed adjustments or additions. Two questions that the committee had to consider during their research are important to this research. The committee had – among other things – the task of investigating whether the new rules regarding digitally stored data and the proposed definition and regulation of the attachment of data are workable and adequate and, if so, which alternative there would be. The second question was, whether, in the light of the Smartphone judgment,[84] the draft articles for searching automated works had to be amended. For this research three categories of recommendations made by the Koops-Committee are relevant. These are the proposed criteria for a "systematic" exercise of competence regarding the intrusion on the privacy of the suspect, the introduction of the legal authority to conduct research on incoming messages and the broadening of the legal authority to conduct a network search. These recommendations will be elaborated on in the following paragraphs.

[80] Supreme Court, 4th of April 2017, ECLI:NL:HR:2017:592.
[81] Commissie modernisering opsporingsonderzoek in het digitale tijdperk, Regulering van opsporingsbevoegdheden in een digitale omgeving, s.l. 2018, p. 6.
[82] Commissie modernisering opsporingsonderzoek in het digitale tijdperk, Regulering van opsporingsbevoegdheden in een digitale omgeving, s.l. 2018, p. 6.
[83] Staatscrt. 12th of July 2017, nr. 39081; Staatscrt. 28th of December 2017, nr. 73969.
[84] Supreme Court, 4th of April 2017, ECLI:NL:HR:2017:592.

3.3 Proposed criteria for a "systematic" exercise of competence regarding the intrusion on the privacy of the suspect

The Koops-Committee has proposed an assessment framework for the exercise of the competence of investigation in a digital environment which is subdivided between a limited a more than limited, and very serious intrusions on the privacy of a suspect.[85] The Koops-Committee has found a connection with the word "systematic". The general idea is that a specific legal provision is necessary when there is a "more than limited invasion of privacy" which is specified as resulting in "a more or less complete picture of certain aspects of the personal life". The concept of "more than limited infringement" which is used in the Smartphone-judgments was seen as almost similar to the concept of "systematic".[86] The Koops-Committee, therefore, proposed to introduce the criteria of non-systematic practice, systematic practice, and far-reaching systematic exercise of competence with a coherent distinction between an investigation officer, a public prosecutor, and an investigatory judge as to the competent authority.[87] The criteria of systematic and far-reaching systematic exercise of competence will first be further explained.

Systematic exercise of competence

The Koops-Committee has introduced the word "systematic", a choice of words that is in its juridical context different than how we use it in our normal speech. The Koops-Committee explains this by elaborating that, for instance, research in open sources is so intensive and thorough that a more or less complete picture of certain aspects of personal life emerges. In that case, when there is such intensive research in an open source, an explicit legal basis is required.[88] This can be related to the search in smartphones as well, since a search in smartphones also can be so intensive and thorough that a more or less complete picture of certain aspects of the personal life emerges, like it has been concluded in the "smartphone-judgements".[89] The criteria of "systematic" include acts that would not be considered systematic in normal speech, but which in a legal sense have the effect of committing a "more

[85] Commissie modernisering opsporingsonderzoek in het digitale tijdperk, Regulering van opsporingsbevoegdheden in een digitale omgeving, s.l. 2018, p. 36.
[86] Commissie modernisering opsporingsonderzoek in het digitale tijdperk, Regulering van opsporingsbevoegdheden in een digitale omgeving, s.l. 2018, p. 37.
[87] Commissie modernisering opsporingsonderzoek in het digitale tijdperk, Regulering van opsporingsbevoegdheden in een digitale omgeving, s.l. 2018, p. 39.
[88] Commissie modernisering opsporingsonderzoek in het digitale tijdperk, Regulering van opsporingsbevoegdheden in een digitale omgeving, s.l. 2018, p. 37-39.
[89] Supreme Court, 4th of April 2017, ECLI:NL:HR:2017:592.

than minor infringement". A clear example the Koops-Committee gave is the accessing and examining of publicly accessible sources: even a single search can provide a substantial picture of the suspect's personal life. Short-term observation with a technical aid in a brothel can also be considered as systematic by legal standards.[90]

The Koops-Committee also adds that the “more than minor infringement” needs to be "reasonably foreseeable in advance". This is indicated in the question whether the exercise of power is systematic, which ought to be asked and answered prior to the deployment, based on the intended actions to collect and process data and all other circumstances of the case, including the information already known from the file about the suspect, and about possible third parties whose data could reasonably be foreseen.[91] This "reasonably foreseeable” criterion is an objective criterion: it concerns what data an investigating officer should reasonably foresee in the case at hand, based on general and context-specific rules of experience and a reasonable assessment of the circumstances of the case.[92] If the exercise of power leads to a more or less complete picture of certain aspects of a person's private life, while this could not reasonably have been foreseen in advance, this does not make the exercise of that power systematic with retrospective effect, and it is therefore not retrospectively unlawful if the relevant requirements for systematic had not been met. The Koops-Committee also addressed that it is important to emphasize that it concerns certain aspects of a person's private life; it is not relevant for “systematic” whether a large part of a person's private life comes into the picture, it is about a certain part (often related to a certain role a person has in social life, such as father, teacher, golfer, house of prayer, pub visitor) coming to the fore more or less completely (for example by forming an image of all contacts within that social capacity).[93]

Far-reaching systematic exercise of competence

The Koops-Committee defines that a far-reaching systematic exercise of competence can occur if – with current knowledge – there is an indication that more, or more sensitive, data is present than previously estimated, to such an extent that there is a real chance that such data

[90] *Kamerstukken II* 1997/98, 25 403, nr. 7, p. 47.
[91] Commissie modernisering opsporingsonderzoek in het digitale tijdperk, Regulering van opsporingsbevoegdheden in een digitale omgeving, s.l. 2018, p. 38.
[92] Commissie modernisering opsporingsonderzoek in het digitale tijdperk, Regulering van opsporingsbevoegdheden in een digitale omgeving, s.l. 2018, p. 38.
[93] Commissie modernisering opsporingsonderzoek in het digitale tijdperk, Regulering van opsporingsbevoegdheden in een digitale omgeving, s.l. 2018, p. 38.

may come into the picture again during follow-up investigations, then this can lead to a very intrusive invasion of privacy and a higher authority will have to be called in.[94]

The question when an invasion of privacy will prove very intrusive, and therefore an authorization by the investigatory judge will be required in addition to an order from the public prosecutor, requires an additional criterion. The Koops-Committee proposed the criterion of far-reaching systematic exercise of competence, which is approached in the same way as the criterion of systematic exercise of competence, but with an additional condition that indicates that it concerns a very far-reaching invasion of privacy. The exercise of competence can be far-reaching systematic if a radical picture of a person's private life can reasonably be foreseen in advance. The Koops-Committee concludes that this intrusion can emerge in two alternative ways.

1. Firstly, a radical picture of a person's private life can arise if a more or less complete picture of an essential part of a person's private life emerges; the radical view here consists of a deep view of a person's private life, in which an essential part comes to the fore. Essential parts are those parts that are closely related to a person's living atmosphere. The Koops-Committee gave as an example, the exercise of a power in which it is reasonably foreseeable in advance that "sensitive" personal data will be copied, can, under certain circumstances, affect an essential part of a person's private life (namely his medical, sexual, religious, political or ethnic identity).

2. In the second place, a radical picture of a person's private life can arise if a more or less complete picture of a substantial part of a person's private life is created; the intrusion here consists of a broad view of a person's private life, in which several parts emerge more or less completely, related to different roles in social life, such as a person's family life, work, sports, club life, nightlife, circles of friends, consumer behavior and relationship with service providers. When one part of a person's private life is more or less fully disclosed, it can be considered systematic; when a significant number of aspects of a person's private life are exposed together, it can be considered as a far-reaching systematic exercise of competence. What matters most is that information from different contexts of a person's life is put together in such a way that

[94] Commissie modernisering opsporingsonderzoek in het digitale tijdperk, Regulering van opsporingsbevoegdheden in een digitale omgeving, s.l. 2018, p. 39.

the picture as a whole becomes far-reaching, without the information from each of those contexts being necessarily far-reaching in itself.

Conclusion proposed criteria for "systematic" exercise of competence

In conclusion, the concept of "systematic" can be seen as an abstract and material criterium: the exercise of power is systematic if it is, in advance, reasonably foreseeable that a more or less complete picture of certain aspects of someone's private life can arise. Furthermore, Koops-Committee assesses that the use of powers must always to comply with the general principles of subsidiarity and proportionality. Besides, a power may only be exercised if this is in the interest of the investigation and as to the more far-reaching features, these can only be applied when urgently necessary.[95] The Koops-Committee refers in its research to the Mosaic-theory, which – in short – boils down to the fact that, for the assessment of the extent of a privacy breach, one should not look at loose stones, but at the image that arises when you put these necessary stones together.[96] In the case of a non-systematic exercise of competence, only loose stones are collected and viewed. Whereas in the case of a systematic exercise of competence, by putting stones together, a certain image ("mosaic") of a person is created. In the case of a far-reaching systematic exercise of competence, a far-reaching image of a person is created, which gives insight into his being (deep) or a significant part of his private life (wide). In mosaic imagery: the necessary pebbles together form a portrait of a person, and that portrait can be far-reaching if - as in a Rembrandt portrait - you can look in through someone's eyes (deep), or if it is a full-length portrait (wide).[97]

The proposed criteria can be summarized as following:

1) *Non-systematic exercise of competence*

   When it is not reasonably foreseeable that a more or less complete picture of certain aspects of someone's private life can arise, an investigation officer is authorized as the competent authority for this legal competence.

2) *Systematic exercise of competence*

[95] Commissie modernisering opsporingsonderzoek in het digitale tijdperk, Regulering van opsporingsbevoegdheden in een digitale omgeving, s.l. 2018, p. 48-49.
[96] Commissie modernisering opsporingsonderzoek in het digitale tijdperk, Regulering van opsporingsbevoegdheden in een digitale omgeving, s.l. 2018, p. 40.
[97] Commissie modernisering opsporingsonderzoek in het digitale tijdperk, Regulering van opsporingsbevoegdheden in een digitale omgeving, s.l. 2018, p. 40.

When it is reasonably foreseeable that a more or less complete picture of certain aspects of someone's private life can arise. It this is the case, only a public-prosecutor (or someone higher) has the competence to grant the power.

3) *Far-reaching systematic exercise of competence*

When it is reasonably foreseeable in advance that a radical picture of someone's private life may arise. This is specified in two ways. First of all, if a more or less complete picture emerges of an essential part of someone's private life, where the intrusiveness consists of a deep view of someone's private life. And if a more or less complete picture is created of a significant part of a person's private life, in which several parts come to the fore more or less fully and relate to different roles in social life. If one of these two situations will arise, an investigatory judge needs to authorize the legal authority.[98]

3.4 The network search

When searching a smartphone it can be that the investigation needs to be broadened to data that is not stored directly on that smartphone, but on an another device or network located elsewhere. This is the case if data has been generated but not stored on the smartphone but in cloud storage services.[99] For instance, a webmail account, such as Gmail, or on an online storage service, like Dropbox.[100] To access the data that is stored on these cloud storage services, the possibility to search these data can be done by a network search.

Based on Articles 125i and 125j CCP it is already possible to search data stored in an automated work that is located elsewhere during a search at a location or place.[101] Article 125i CCP grants a legal basis for conducting a search when investigation officers are searching a location or place. Then they are allowed to record data stored or recorded on a data carrier in that place. In the interest of the investigation, it is possible to record that data. Furthermore, Article 125j CCP allows that in the event of a search, data stored in an automated work present elsewhere which is reasonably necessary to ascertain the truth and may be searched at the place where this search takes place. If such data is found, it can be recorded. This search cannot extend beyond the

[98] Commissie modernisering opsporingsonderzoek in het digitale tijdperk, Regulering van opsporingsbevoegdheden in een digitale omgeving, s.l. 2018, p. 40.
[99] 19th of July 2019, Memorie van Toelichting Innovatiewet Strafvordering, www.internetconsultatie.nl, p. 28
[100] Discussiestuk 'Onderzoek ter plaatse, inbeslagneming en doorzoeking en onderzoek van gegevensdragers en in geautomatiseerde werken' van 6 juni 2014, p. 52-53.
[101] Art. 125j CCP.

limits of access which the persons who normally work or reside at the location where the search takes place have to the automated work from that place, with the consent of the right holder.

However, in practice, it can only become apparent during a search that it is not the seized smartphone that contains the information sought, but that this information appears to be stored elsewhere.[102] Therefore, often after the search of a seized device such a network search would be needed. Since Article 125j CCP only allows for a network search to take place while searching a site or location, due to the limited scope of the application of the Article, it could be that the network search is no longer possible at that point in time.[103] Only then it is allowed to record data stored or recorded on a data carrier in that place and, if it is in the interest of the investigation, only then is it allowed to keep a record of such data. Therefore, the Koops-Committee stated that the legal extension of the possibility of a network search after a seizure, and in situations of an arrest but also in cases where the police will stop someone on the street for something he did wrong and where the police can give a warning or write a fine, is urgently desirable, and cannot wait until the modernized CCP will entry into force.[104]

To perform a network search, the Koops-Committee suggested that it is better to connect this to the possibility that the network search takes place in a different place. Whereby the person who is or was a user of the automated work being searched is the rights-holder. Also, this network-search may not go further than the access that the user of the seized automated work has to the automated work elsewhere, with the permission of the entitled party.[105] Besides, it should be possible for a network search to take place with forensic investigation equipment, whereby no more access should be obtained than which would be the case if it was done manually within the original automated work. This means that the access should, therefore, be limited to that which would have been obtained in the case of investigations carried out from the original automated work, so the network search cannot be expanded by for instance parts of the remote server to which the user has no access rights.[106]

[102] 19th of July 2019, Memorie van Toelichting Innovatiewet Strafvordering, www.internetconsultatie.nl, p. 28
[103] Commissie modernisering opsporingsonderzoek in het digitale tijdperk, Regulering van opsporingsbevoegdheden in een digitale omgeving, s.l. 2018, p. 109.
[104] Commissie modernisering opsporingsonderzoek in het digitale tijdperk, Regulering van opsporingsbevoegdheden in een digitale omgeving, s.l. 2018, p. 118.
[105] Commissie modernisering opsporingsonderzoek in het digitale tijdperk, Regulering van opsporingsbevoegdheden in een digitale omgeving, s.l. 2018, p. 111-112.
[106] Koops, B.J. and Oerlemans, J.J., Strafrecht & ICT, Den Haag: [2019] SDU, Chapter 3, p. 134.

Concerning the duration of the network search, the Koops-Committee believes that the network search may take as long as reasonably necessary to obtain all of the data required, with the recommendation that the duration of the network search should in principle not exceed a few days.[107] There may be deviations from this recommended duration under certain circumstances, but if more time is required to carry out the network search in all reasonableness, then this must be elaborated upon in the justification. This reasoning can also be found in the before-mentioned investigation of incoming messages after a seizure or during a network search, where the Koops-Committee determined that this period may be as long as is reasonably necessary to obtain the necessary data, however, limited to a few days whereas it can be that a longer period to search is needed, when the reasoning for why a longer period is needed, is sufficiently motivated. However, two differences can be seen between these two periods.

The Koops-Committee does point out the principles of subsidiarity and proportionality that limit the reasonable period within which a network search based on later research can be conducted.[108] They specifically refer to searching a seized smartphone after it has been seized. If this is conducted after a month, while this could also reasonably have been investigated after a week, the basis for conducting a network search based on the late investigation in the smartphone lapses. After all, there a substantial chance that in the automated work elsewhere, there will now be (considerably) more data than on the pretext of the original seizure of the smartphone.

With regard to the competent authority for the exercise of this authorization, the Koops-Committee matches this authority with the earlier criterion of "systematic".[109] When investigating messages entrusted to a third party and protected under Article 13 of the Constitution, the investigatory judge must always issue an authorization.

3.5 Investigation of incoming messages after a seizure or during a network search

The Koops-Committee addressed a bottleneck in the search when new substantive data becomes available on (or via) an automated work or digital data carrier after the seizure or

[107] Commissie modernisering opsporingsonderzoek in het digitale tijdperk, Regulering van opsporingsbevoegdheden in een digitale omgeving, s.l. 2018, p. 113.
[108] Commissie modernisering opsporingsonderzoek in het digitale tijdperk, Regulering van opsporingsbevoegdheden in een digitale omgeving, s.l. 2018, p. 114.
[109] Commissie modernisering opsporingsonderzoek in het digitale tijdperk, Regulering van opsporingsbevoegdheden in een digitale omgeving, s.l. 2018, p. 115-117.

during a network search because it is not yet enshrined in law to search this new substantive data.[110] Therefore they divided the coincidental capture of data, which in Dutch is called "bijvangst" (from here: "bycatch"). They divided this bycatch by pure or foreseeable (or non-unforeseeable) bycatch.[111] The Koops-Committee considers that in the case of a short and natural lapse of time there can arise pure bycatch: all data on the automated work or the digital data carrier will then form part of the data which can be investigated, including the coincidental capture of newly received messages, without the need for additional authorization or standardization.[112]

However, in Article 13 of the Dutch Constitution, it has been laid down that communications that are in the transport phase, or with a provider and obtained through the provider, are protected by the protection of the secrecy of communications.[113] Since bycatch can be considered as communications that are still in the transport phase or previously stored within a provider, this bycatch may fall within the scope of this Article. Regarding a smartphone this is, however, only the case if the investigation has an active role in retrieving the messages that were previously stored within a provider or were in the transport phase. Thus, in that case, these messages fall within the realm of the protection offered by Article 13 of the Constitution. Therefore, the Koops-Committee further explained which authorities may justify an infringement of Article 13 of the Dutch Constitution for the search of incoming messages after a seizure or during a network search. The bycatch can therefore only be obtained with prior authorization from the investigatory judge if needed for the investigation. In conclusion, it means that obtaining messages that fall under this protection requires authorization from the investigatory judge. With regard to the period during which this bycatch can be searched, the Koops-Committee determined that it may be as long as is reasonably necessary to obtain the necessary data, however, in principle this period should be limited to a few days. It can be that a longer period to search is needed, in which case there is some room for this, but only if the reasoning as to why a longer period is needed, is sufficiently motivated.[114]

---

[110] Commissie modernisering opsporingsonderzoek in het digitale tijdperk, Regulering van opsporingsbevoegdheden in een digitale omgeving, s.l. 2018, p. 94 etc.
[111] Commissie modernisering opsporingsonderzoek in het digitale tijdperk, Regulering van opsporingsbevoegdheden in een digitale omgeving, s.l. 2018, p. 94 etc.
[112] Commissie modernisering opsporingsonderzoek in het digitale tijdperk, Regulering van opsporingsbevoegdheden in een digitale omgeving, s.l. 2018, p. 93.
[113] Art. 13 of the Dutch Constitution: "*1. The secrecy of letters shall be inviolable, except, in cases provided for by law, by order of the court. 2. Telephone and telegraph secrecy shall be inviolable, except, in the cases provided for by law, by or with the authorisation of those designated by law.".*
[114] Commissie modernisering opsporingsonderzoek in het digitale tijdperk, Regulering van opsporingsbevoegdheden in een digitale omgeving, s.l. 2018, p. 93.

3.6 Conclusion

The Koops-Committee introduces a different legal framework for the authorization to conduct a search on automated works, with different allocations on the authorizations to conduct the search. The *non-systematic exercise of competence; w*hen it is not reasonably foreseeable that a more or less complete picture of certain aspects of someone's private life can arise, an investigation officer is authorized as the competent authority and no further permission would be required. The *systematic exercise of competence; w*hen it is reasonably foreseeable that a more or less complete picture of certain aspects of someone's private life can arise, then only a public-prosecutor (or someone higher) has the competence to grant this power. And the *far-reaching exercise of competence;* when it is in advance reasonably foreseeable that a radical picture of someone's private life may arise. This is specified in two ways. First of all, if a more or less complete picture emerges of an essential part of someone's private life, where the intrusiveness consists of a deep view of someone's private life. And if a more or less complete picture is created of a significant part of a person's private life, in which several parts come to the fore more or less fully, and relate to different roles in social life. If one of these two situations will arise, an investigatory judge has the competence to authorize the legal authority. The Koops-Committee also addressed that it is important to emphasize that "systematic" concerns certain aspects of a person's private life; it is not relevant for "systematic" whether a large part of a person's private life comes into the picture, it is about a certain part (often related to a certain role a person has in social life, such as father, teacher, golfer, house of prayer, pub visitor) coming to the fore more or less completely (for example by forming an image of all contacts within that social capacity).[115] The Koops-Committee, therefore, created a more clarified framework laying down the scope of the different types of intrusion and the authorization needed for conducting the search.

The Koops-Committee also introduced the idea of broadening the possibility of ordering a network search, like Article 125j, regarding automated works which have been seized, to be done at the police station. In this case, similarly to one earlier discussed, the committee stated that this broadening should not wait until the modernized CCP will entry into force.[116] This could be done manually and with the help of technical equipment, thus if this is limited to that information which could have been obtained in the case of the investigations -manually- carried

[115] Commissie modernisering opsporingsonderzoek in het digitale tijdperk, Regulering van opsporingsbevoegdheden in een digitale omgeving, s.l. 2018, p. 38.
[116] Commissie modernisering opsporingsonderzoek in het digitale tijdperk, Regulering van opsporingsbevoegdheden in een digitale omgeving, s.l. 2018, p. 118.

out from the original automated work. When determining the competent authority for the exercise of this authorization, the Koops-Committee recommends matching this authority with the earlier criterion of "systematic".[117]

Furthermore, the Koops-Committee introduced the possibility to broaden the search which can be conducted to incoming messages. If these incoming communications are in the transport phase, or with a provider and obtained through the provider, and are protected by the protection of the secrecy of communications, then this could only be done after an order issued by an investigatory judge.[118]

[117] Commissie modernisering opsporingsonderzoek in het digitale tijdperk, Regulering van opsporingsbevoegdheden in een digitale omgeving, s.l. 2018, p. 115-117.
[118] Art. 13 of the Dutch Constitution: "*1. The secrecy of letters shall be inviolable, except, in cases provided for by law, by order of the court. 2. Telephone and telegraph secrecy shall be inviolable, except, in the cases provided for by law, by or with the authorisation of those designated by law.".*

4. The changing legal framework under the Innovation Bill

In the previous chapter, the modernization of the Dutch Criminal Code of Procedure, as is taking place through the Innovation Bill, has been discussed by addressing how the modernization of the Dutch Criminal Code of Procedure is going and the relevant recommendations for this research by the Koops-Committee. In this chapter, the relevant draft Articles of the Innovation Bill are introduced and it will be further discussed how this Innovation Bill will change the Dutch legal framework for the search and seizure of automated works. This discussion will focus on both the network search and the search of incoming messages, which, at first, are discussed separately. As it is possible that incoming messages appear during a network search, these newly introduced powers might overlap. Therefore, both powers will also be discussed together. This chapter will answer the following sub-question:
To what extent will the current legal framework for the search and seizure of automated works change in the proposed amendment of the Dutch Criminal Code of Procedure (Innovation Bill)?

4.1 Introduction of the Innovation Bill

After the Koops-Committee made its recommendations, and other relevant organizations within the criminal justice chain made their suggestions,[119] the legislator introduced a draft proposal for the Innovation Bill on the 6th of June 2019.[120] The Innovation Bill facilitates that some of the recommendations that are relevant for the criminal law practice can already be applied to gain practical experience, before the new Criminal Code of Procedure entries into force.[121] This will be based on pilot projects, where organizations within the criminal justice chain can gain experience in improving the provisions based in the Innovation Bill, identify possible implementation consequences, and consider whether accompanying policy is necessary.[122]

The legislator introduced three new articles regarding the search and seizure of automated works.[123] Articles 554 and 555 focus on enabling a network search in the context of an investigation after the seizure of an automated work, which will be discussed in more depth in

[119] The explanatory memorandum mentions the following parties: the public prosecution service, the Dutch bar association, the judiciary, the police, special investigation services, the personal data authority, victim assistance in the Netherlands and the royal constabulary.
[120] 19th of July 2019, Concept regeling, Wetsvoorstel Innovatiewet Strafvordering, www.internetconsultatie.nl.
[121] 19th of July 2019, Memorie van Toelichting Innovatiewet Strafvordering, www.internetconsultatie.nl, p. 1.
[122] The explanatory memorandum mentions the following parties: the public prosecution service, the Dutch bar association, the judiciary, the police, special investigation services, the personal data authority, victim assistance in the Netherlands and the royal constabulary.
[123] These Articles are included in the Annex.

paragraph 4.2. Article 556 introduces the new possibility for the search of incoming messages after an automated work has been seized. This Article will be further elaborated on in paragraph 4.3.

4.2 Enabling a network search after the seizure of an automated work

The first two new draft Articles, 554 and 555, broaden the scope of the types of technology which can be searched after the seizure of an automated work.[124] Based on the current article 125j CCP, information that is not stored on an automated work but in an automated work which is located elsewhere can be searched, this practice is called a network search. However, this current Article only allows a network search at the location – and time – during which officers are searching a place.[125] This entails that under current legislation, for instance, when a smartphone is seized during that search, it is not possible to conduct a network search at the police station. In the case of a seized smartphone during an arrest, current legislation does not allow for a network search to be conducted, because this was only permitted during an actual search. The Koops-Committee therefore urgently requested for this Article to be broadened. The combined Articles 554 and 555 of the Innovation Bill, will create a possibility to conduct a network search after a smartphone has been seized.

The authorization to order a network search and the period in which this can be conducted

The new Articles 554 and 555 allow the public prosecutor to order a network search following the seizure of the automated work. In general, the public prosecutor must order the network search within one month of the seizure. However, the public prosecutor may decide to extend this decision-making period by one month at a time. Which is not limited to one extension, but can take place an unlimited amount of times.[126] After the order has been given, an investigation officer is allowed to perform the network search.[127] The period to conduct the network search can be granted for three days, and can later be extended with another three days to a maximum of six days.[128]

[124] 19th of July 2019, Memorie van Toelichting Innovatiewet Strafvordering, www.internetconsultatie.nl, p. 27-30.
[125] 19th of July 2019, Memorie van Toelichting Innovatiewet Strafvordering, www.internetconsultatie.nl, p. 27-30.
[126] 19th of July 2019, Memorie van Toelichting Innovatiewet Strafvordering, www.internetconsultatie.nl, p. 30.
[127] 19th of July 2019, Memorie van Toelichting Innovatiewet Strafvordering, www.internetconsultatie.nl, p. 28-29.
[128] 19th of July 2019, Memorie van Toelichting Innovatiewet Strafvordering, www.internetconsultatie.nl, p. 28-29.

The competent authority for the exercise of this authorization, as mentioned in the current Innovation Bill, is not in line with the recommendations of the Koops-Committee as the latter takes the proposed criterion of "systematic" very seriously and therefore prescribes for different intrusions to have a different authority which is allowed to conduct a search. Since, these criteria have not been introduced in the Innovation Bill, it is still unclear in which cases (of intrusion on the privacy of a suspect) which competent authority is allowed to order and conduct a search that can lead to this intrusion. However, this competent authority actually should be decided upon in relation to the Smartphone-judgements.[129] Therefore, if in advance it is foreseeable that by conducting a network search this will conclude a far-reaching invasion on the right of privacy, the network search should be ordered by an investigatory judge instead of the proposed public prosecutor.[130] For instance, if the search is being done after a couple of months a lot of additional data might be found. When connecting to the network it can mean that for instance in the cloud, or messages via e-mail or other network stored messages could come up, which would not have been found at the time of the seizure. Since it can be reasonably foreseeable that, considering the findings of additional data, this could lead to a serious intrusion, this network search should be ordered by an investigatory judge.

The Koops-Committee stressed the importance of the principles of subsidiarity and proportionality which limit the reasonable period within a network search, based on later research, can be conducted.[131] If a network search could be done within the timespan of a week, it should no longer take place after a month, because, as concluded before, it can be foreseeable that after a longer period there will be additional data (by-catch) found, which would not have been found at the time of the seizure. The before-mentioned criteria would definitely preclude the search after two months (or even more), as can now be done based on the new proposed Article 555. The explanatory memorandum mentions that in case of the seizure of a single smartphone, the search should take place as quickly as possible, whereas if there are a lot of seized automated works, the extended period gives the investigators the possibility to hold the seized automated works for a while to assess the need for research.[132] However, it is be

[129] Supreme Court, 4th of April 2017, ECLI:NL:HR:2017:592.
[130] Supreme Court, 4th of April 2017, ECLI:NL:HR:2017:592.
[131] Commissie modernisering opsporingsonderzoek in het digitale tijdperk, Regulering van opsporingsbevoegdheden in een digitale omgeving, s.l. 2018, p. 114.
[132] 19th of July 2019, Memorie van Toelichting Innovatiewet Strafvordering, www.internetconsultatie.nl, p. 30.

foreseeable that seized automated works will not be searched directly.[133] The arrival of new messages can provide a perverse incentive to wait longer to start the investigation so that the period in which they can arrive is extended.[134] The legislator could consider that the public prosecutor, with the authorization of the investigatory judge, can extend this legal (investigation) period (each time) by a period to be specified by the investigatory judge.[135]

In 2018 there was a case in which Telegram messages which arrived after the smartphone had been seized were searched. The lower court of the Hague, ruled that the search of these ongoing communications was considered undesirable in the eyes of the legislator in the context of the network search.[136] The Koops-Committee also suggested that searching messages entrusted to a third part could fall under the protection of the secrecy of communications, which is protected under Article 13 of the Constitution.[137] This could be the case if communications are in the transport phase, or with a provider and obtained through the provider. In that case, the investigatory judge must always issue an authorization to search these messages.[138]

For incoming private messages, it should be kept in mind that in July 2014 a legislative proposal to revise Article 13 of the Constitution has been submitted.[139] This legislative proposal aims to extend the scope of this Article to all telecommunications, which will include all current and future means of communication. This aims at getting the protection of communications secrecy in line with the current state of information technology and to make Article 13 of the Constitution future-proof. Therefore, all of the content of communications of a private nature should be protected by the Constitution, irrespective of the means or technique by which they are communicated.[140] After the Senate had already agreed to the proposal, on 11 July 2017 the House of Representatives also unanimously agreed to it. As a result, the proposal for

[133] Wetenschappelijke commissie van de Nederlandse Vereniging voor Rechtspraak, Advies Innovatiewet Strafvordering, 5th of October, 2019, p. 2-4.
[134] Houwing, L, Reactie op consultatie Innovatiewet Strafvordering, Bits of Freedom, 22th of August 2019.
[135] Houwing, L, Reactie op consultatie Innovatiewet Strafvordering, Bits of Freedom, 22th of August 2019.
[136] Court of Appeal of The Hague, 19th of December 2018, ECLI:NL:GHDHA:2018:3529: *"If the network search takes place at the police station, it is a search at a (much) later time than the time of the search itself. In that case, especially in the current era of far-reaching (internet) interconnectivity between automated works, there is a considerable chance that data will be obtained at that later moment of network search that was not yet available at the time of the search itself. However, as has already been discussed above, the legislator has considered the latter undesirable in the context of the network search."*
[137] Art. 13 of the Dutch Constituion.
[138] Commissie modernisering opsporingsonderzoek in het digitale tijdperk, Regulering van opsporingsbevoegdheden in een digitale omgeving, s.l. 2018, p. 115-117.
[139] *Kamerstukken II* 2013/2014, 33 989, nr 3.
[140] 19th of July 2019, Memorie van Toelichting Innovatiewet Strafvordering, www.internetconsultatie.nl. .

amendment of the Constitution is at first reading by both Houses.[141] It will now be submitted for a second reading to the current House of Representatives and, after that, to the new Senate. If both agree on the proposal, that the scope of Article 13 of the Constitution will be broadened, and therefore, in the future, permission to search all telecommunications will have to be signed off on by an investigatory judge.

The broadening scope of the network search in the light of Article 125j CCP

The allowed place to conduct a network search deviates from Article 125j CCP since the network search can now be conducted at the place where the automated work is being stored after a seizure. This entails the network search no longer requires that it will take place during a search at a place for recording data.[142] The network search can, therefore, be performed in another place. However, the network search is limited to the extent to which the user of the seized automated work has access to the data that is stored in the other automated work at stake which is located elsewhere.[143] More specifically, lawful access must be translated to the legitimate access the user of the seized automated work has to the automated work elsewhere.[144] Article 125j CCP uses the term "rights holder" and the Innovation Bill uses the term "user" which has been introduced on behalf of the Koops-Committee.[145] For instance, it can be possible that the suspect was in possession of someone else's smartphone, which does not make him the rights holder to that smartphone, but he could still have accessed, for instance, his social media or e-mail on that smartphone. It could also be that a smartphone has been stolen and that the suspect used that smartphone, in which case he would also not be the legitimate rights holder to that smartphone.[146] The term "user" is therefore more suitable for the purposes of a network search conducted in automated works.

The safeguards under which a network search can be conducted

The explanatory memorandum does not specify to what extent the network search can take place. However, it states that it has not been determined that the investigation must take place

[141] *Kamerstukken II* 2016/2017, 33 989, nr. 69; *Kamerstukken I* 2016/2017, 33 989 A.
[142] Article 125j CCP.
[143] Commissie modernisering opsporingsonderzoek in het digitale tijdperk, Regulering van opsporingsbevoegdheden in een digitale omgeving, s.l. 2018, p. 111-112.
[144] 19th of July 2019, Memorie van Toelichting Innovatiewet Strafvordering, www.internetconsultatie.nl, p. 27-30.
[145] Commissie modernisering opsporingsonderzoek in het digitale tijdperk, Regulering van opsporingsbevoegdheden in een digitale omgeving, s.l. 2018, p. 112.
[146] 19th of July 2019, Memorie van Toelichting Innovatiewet Strafvordering, www.internetconsultatie.nl, p. 29.

within the initial – seized – automated work. It follows the Koops-Committee that for the purposes of the investigation, tools are available which have been specially developed to perform a forensically sound "cloud-search" with integrity. Whereas if the network-search is conducted manually it is possible that after connecting the automated work to the internet it will receive a delete command. Therefore, the legislator prefers to use forensic equipment to conduct a network search. If these tools are used, no more access should be obtained than which would be the case if it was done manually within the original automated work.[147] The explanatory memorandum does not specify this further, but the Koops-Committee specified that the access should, therefore, be limited to that which would have been obtained in the case of investigations carried out from the original automated work, and therefore this search should be conducted as quickly as possible and not after a couple of months.[148] This could mean that the network search cannot be expanded by, for instance, parts of the remote server to which the user has no access rights.[149]

However, as it is unclear to what extent this search can be executed, and how this execution will be monitored, the legislator should consider the possibility of safeguards to protect the defendant against the intrusion that the network search can make on his or her private life. In cases where the scope of the network search will not extend to a far-reaching invasion on the right of privacy this can be monitored by the proposed public prosecutor. However, as explained in the previous paragraph, it is possible that the network search needs to be ordered by an investigatory judge if the network search could result in – or lead to – a far-reaching intrusion of the privacy of the user of the automated work.[150] This procedure would be in line with the Smartphone-judgments and it provides safeguards by ordering investigation officers to investigate, prior to the network search, if it could be foreseen that this could have a far-reaching impact on the private life of a suspect, and if so, narrow their network search.

4.3 Searching incoming messages on seized automated works

Article 556 follows the recommendations of the Koops-Committee by introducing the possibility to search incoming data, and therefore messages, on seized automated works.[151] For

[147] 19th of July 2019, Memorie van Toelichting Innovatiewet Strafvordering, www.internetconsultatie.nl, p. 29.
[148] Commissie modernisering opsporingsonderzoek in het digitale tijdperk, Regulering van opsporingsbevoegdheden in een digitale omgeving, s.l. 2018, p. 111-112.
[149] Koops, B.J. and Oerlemans, J.J., Strafrecht & ICT, Den Haag: [2019] SDU, p. 134.
[150] Council for the Judiciary Advice Amendment to the Code of Criminal Procedure, 2th of October 2019, p.3-4.
[151] 19th of July 2019, Memorie van Toelichting Innovatiewet Strafvordering, www.internetconsultatie.nl, p. 30-31.

the investigation officers, it is under the current legislation unclear whether it is allowed to search messages received on a smartphone after it has been seized, which are 'incoming messages'.[152] This lack of clarity has been addressed by the Koops-Committee and they suggested adding a provision to allow the search of incoming messages.

The authorization for the search of incoming messages and to which extent these can be searched

According to the new provision, the public prosecutor is allowed to order that an investigation officer takes cognizance of data or records stored on an automated work. This authority is that of the public prosecutor if this order is given within three days after the initial seizure of the automated work. If this period needs to be extended, the public prosecutor can extend it, after having obtained authorization from the investigatory judge, for a period of one month. The explanatory memorandum only explains that after a period of three days an order from the investigatory judge is needed since a relatively long period could bring additional information within the scope of the search that was not yet available when the initial seizure power was exercised.[153]

This is not in line with the recommendations of the Koops-Committee. The Koops-Committee concluded that incoming messages could fall under the protection of Article 13 of the Constitution if the investigation has an active role in retrieving the messages that were previously stored at a provider or were in the transport phase.[154] It, therefore, recommended that the legislator should indicate, with examples in the explanatory memorandum, the degree of the initiative of the investigation that will fall under the scope of the protection of Article 13 of the Constitution. An example would be a situation in which the investigation requires the use of active synchronization, entailing that during the search investigation officers connect a smartphone to the network. Consequentially, the smartphone will retrieve various messages and information which were not yet stored on the smartphone before the search would take place. If these incoming messages fall within the scope of protection of Article 13 of the Constitution, for example, e-mails and personal messages on Facebook or WhatsApp,

[152] Politieacademie 2019, Digitalisering en de opsporingspraktijk, juridische aspecten, versie 3.3, p. 25.
[153] 19th of July 2019, Memorie van Toelichting Innovatiewet Strafvordering, www.internetconsultatie.nl, p. 30.
[154] Commissie modernisering opsporingsonderzoek in het digitale tijdperk, Regulering van opsporingsbevoegdheden in een digitale omgeving, s.l. 2018, p. 93.

an order from the investigatory judge is needed to authorize the search.[155] This has also be concluded by the District Court of the Central-Netherlands,[156] which ruled that authorization from the investigatory judge was needed to search notifications that came into the Telegram-app after the seizure.[157]

Furthermore, based on the Innovation Bill it prohibited to seize an automated work with the sole purpose of capturing incoming communications, in other words: to search this new available substantive data.[158] To achieve these ends, investigation officers have other possibilities: the powers which are laid down in the Articles 126l (the telephone tap)[159], 126m (recording confidential information)[160], and 126nba (hacking)[161] of the current CCP. The exercise of these powers is only justified after an order has been given by an investigatory judge. However, the longer the period of the newly introduced competence continues, the more this will relate to these powers, and therefore it is required to have obtained authorization of the investigatory judge after the period of three days.[162] This distinction could be considered to be insufficient for the difference in guarantees. Therefore, the proposed provision can regulate the ability to take note of this communication but the breach of the confidentiality of communication takes place when the data is inspected, not only when it is recorded. The intrusion that takes place based on the proposed provision is, therefore, comparable to the powers for which authorization from the investigatory judge is required.[163]

4.4 Searching incoming messages in relation to the network search

It is possible that during a network search investigation officers will use active synchronization. This means that during the search investigation officers connect a smartphone to the network. If they connect the smartphone to the network this means that the smartphone can retrieve various messages and information which were not yet stored on the smartphone before the

[155] Commissie modernisering opsporingsonderzoek in het digitale tijdperk, Regulering van opsporingsbevoegdheden in een digitale omgeving, s.l. 2018, p. 93.
[156] Lower Court of Midden-Nederland, 7th of June 2018, ECLI:NL:RBMNE:2018:2655.
[157] Lower Court of Midden-Nederland, 7th of June 2018, ECLI:NL:RBMNE:2018:2655: *"Investigation on a seized telephone into messages that will arrive on the chat program" Telegram "requires a decision of the* investigatory judge *under article 101 DCCP because these messages can be considered as letters that have not yet are open."*
[158] 19th of July 2019, Memorie van Toelichting Innovatiewet Strafvordering, www.internetconsultatie.nl, p. 31.
[159] Article 126l CCP: -in short- the telephone tap.
[160] Article 126m CCP: -in short- recording confidential information.
[161] Article 126nba CCP: -in short- hacking.
[162] 19th of July 2019, Memorie van Toelichting Innovatiewet Strafvordering, www.internetconsultatie.nl, p. 31.
[163] Houwing, L, Reactie op consultatie Innovatiewet Strafvordering, Bits of Freedom, 22th of August 2019, p. 3-5.

search.

The authority and period for the search of incoming messages concerning the network search

It is possible that both timeframes, that to gain authorization for the search of incoming messages and to that to order the network search, overlap. The distinction between one month on the one hand for the network search and three days on the other hand for the incoming messages may not be useful, since they are in such close connection, because during a network search incoming messages can also be made available.[164] Undoubtedly, in the case of a seized smartphone and computer networks it is reasonable to expect that there will be incoming messages after the seizure. This means that an order of the investigatory judge will almost always be needed. Therefore, the Council for the Judiciary Advice proposed to change the periods, based in Articles 555 and 556, to a first period of three days where the public prosecutor himself can order a network search. This has to be completed within three days, and within these three days, it is allowed to also search the incoming available messages which were not at the automated work on the day of the seizure. After these three days, the investigatory judge will need to order both the network search and the search of the incoming data. This investigatory judge will have to examine whether the research interest is still urgent enough and whether this interest justifies further investigation. Furthermore, they state that the investigatory judge should also examine whether there is an undesirable circumvention of other statutory regulations.

However, since it can be foreseen that the chances are very high that messages will be received at the automated work after a seizure, it could also be that these messages fall under the scope of Article 13 of the Constitution.[165] This is the case if the investigation has an active role in retrieving the messages that were previously stored within a provider or were in the transport phase. In that case the search of these incoming messages should be ordered by an investigatory judge. Therefore, the close connection between the network search and the incoming messages can lead to a high burden for investigatory judge.

[164] Council for the Judiciary Advice Amendment to the Code of Criminal Procedure, 2th of October 2019; they refer to Commissie modernisering opsporingsonderzoek in het digitale tijdperk, Regulering van opsporingsbevoegdheden in een digitale omgeving, s.l. 2018, p. 92.
[165] Houwing, L, Reactie op consultatie Innovatiewet Strafvordering, Bits of Freedom, 22th of August 2019.

4.4 Conclusion

The current proposed Articles in the Innovation Bill, Articles 554-556, have been introduced in 2019 following the recommendations of the Koops-Committee. However, the legislator followed only a couple of recommendations that the Koops-Committee has made and did not include the most important recommendation, which is to introduce criteria of "systematic" exercise of competence. Therefore, it is not yet clear how far the newly proposed exercises of competences will reach. To authorize the network search, a distinction must be made between the systematic practice to obtain an authorization and the far-reaching systematic practice to obtain an authorization, to know if this must be ordered by the public-prosecutor or if this needs an authorization of the investigatory judge. The timeframe in which these authorizations can be obtained, which the Koops-Committee did not give an explicit indication for, is also not in line with the intrusion it results in if a network search could take place for a larger period of time then the allowance for the search of the incoming messages. Therefore, this needs to be specified further to understand which kind of authorization has to be given. At this point, Article 556, for the authorization of the search of incoming messages in the first three days after the seizure, is missing if the search of incoming messages which fall under the scope of Article 13 of the Constitution is allowed to be ordered by the public prosecutor or that this must be done by the investigatory judge. Furthermore, the overlap which can occur during the period of conducting the network search and the incoming messages is not in line with the authorization for conducting the network search if this can be ordered by the public prosecutor. In conclusion, the legislator is attempting to broaden the scope of the search which can take place within seized automated works, but has not yet come to create a clear legal framework in light of the extend of authorization with regard to intrusion of the personal life of a suspect and, more specifically, which legal authority is allowed to order or authorize such an intrusion.

5. Conclusion

This research focused on the following question: *"To what extent and under which conditions can the police in the Netherlands search seized automated works, especially based on the recent "smartphone judgments", and how will this legal framework change in the proposed amendment of the Dutch Criminal Code of Procedure (Innovation Bill)?"*

This research has shown that the legal framework of the search and seizure of automated works has been completely laid down in court decisions. There is no specific Article in the Dutch Criminal Code of Procedure for the search and seizure of automated works yet, and therefore the extent to, and conditions under, which this can take place have been given by the Dutch Supreme Court. In order to conduct a search and decide on the appropriate authority to order this search, the Dutch Supreme Court divided the authority based on the intrusion on the private life of a person. A situation where there is a minor intrusion, which allows investigating officers to search automated works to the extent of a limited number of specific stored of available data, can occur, for example, in a targeted viewing of photographs in a photo gallery or in the case of a targeted look at pictures and videos. The second situation arises when a more than limited intrusion has arisen when the search obtains a more or less complete picture of certain aspects of the personal life of the user of the data carrier, which can particularly be the case when it concerns the search *of all data* stored or available in the electronic data carrier or the automated work *using technical aids*. This intrusion is only allowed if this search is approved by a public prosecutor. The most significant violation can occur if, in advance, it is foreseeable that searching the data carrier will lead to a far-reaching invasion on the right of privacy. The search which could lead to this intrusion, has to be approved by an investigatory judge. However, the scope of these ranges of intrusion are only based on a couple of cases, since there are not yet a lot of different court cases which ruled on the scope of the different intrusions.

With the Innovation Bill, Articles 554-556 have been introduced in 2019 in which the legislator followed the recommendations made by the Koops-Committee, but the legislator decided not to follow their most important recommendation, which was to introduce the criteria of "systematic" exercise of competence. Which means, that with the Innovation Bill the scope of the search and seizure of automated works only have been broadened, without an

explicit reaction from the legislator to the framework which is based on court rulings, in which way automated works can be seizes and searched.

The legislator decided to extend the search and seizure of automated works with a network search, which now can be done from the police station instead of during a search at a place. The legislator also made it possible to extend the search by also searching incoming messages which were not yet stored on an automated work during the seizing. The intrusion that these broadened articles allow, the period in which these are allowed and the authority which can order this, are not yet in line, and will need to be adjusted before these articles can enter into force. If these two competences are combined, and used for a couple of months, this could cause a reasonably foreseeable intrusion on the privacy of a suspect. The infringement that can be made is therefore one that should only take place after an investigatory judge ordered this. Furthermore, in light of the proposed change of Article 13 of the Constitution, all interception of digital communication can only take place after this has been ordered by at least an investigatory judge. Even though this has not yet been enshrined in law, this means that the new articles may prove to be in violation of the constitution. The Innovation Bill therefore does broaden the scope for the search and seizure of automated works but does not completely specify in which ways the intrusion on the right to privacy can exactly occur. The Innovation Bill simply attaches an authorization of the public officer or an investigatory judge to the competence, without clarifying in which situations it may be needed to gain permission from a higher authority instead of the public officer, to allow the different types of intrusions on the right to privacy of a suspect.

Annex

English translation of the specific Articles which lay in the Innovation Bill of the Dutch Criminal Code of Procedure[166]*:*

Enabling a network search in the context of an investigation after the seizure of an automated work:

Article 554
In the manner provided for in Article 555, it is possible to deviate from Article 125j after seizure of an automated work to investigate in an automated work present elsewhere to investigate the data stored in that work in the context of the investigation.

Article 555
1. The public prosecutor may, after seizing an automated work, order in the interest of the investigation that an investigating officer investigates data which are reasonably necessary to display the truth which are stored in an automated work elsewhere. If such data is found, it can be recorded.
2. The investigation of data in an automated work present elsewhere does not go beyond the extent where the user of the seized automated work has access to it with the consent of the person entitled to the automated work present elsewhere.
3. The order shall be issued at least within one month after the seizure of the automated work. The public prosecutor can extend this period by one month at a time.
4. The order is given for a maximum period of three days. It can be extended once for a maximum period of three days.

Providing in an arrangement that after the seizure of an automated work, in the context of an investigation, incoming messages for a specific period can be investigated:

Article 556
1. The public prosecutor may, after seizing an automated work, order in the interest of the investigation that an investigating officer, for a period of three days after the seizure, takes cognizance of data or records stored on the automated work that were not yet available at the time of the seizure.
2. The public prosecutor may, after having obtained authorization from the investigatory judge and if the interests of the investigation so require, order that the three-day period be extended for *a maximum period of one month*

[166] Translated by the Author of this research.

List of references

Table of legislation

Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) (ECHR).

Kamerstukken I 2016/2017, 33 989 A.

Kamerstukken II 1997/98, 25 403, nr. 7.

Kamerstukken II 2013/2014, 33 989, nr 3.

Kamerstukken II 2016/2017, 33 989, nr. 69.

Kamerstukken II 2017/18, 29279, nr. 395,

Kamerstukken II 2017/18, 29279, nr. 402.

Kamerstukken II 2018/19, 29279, nr. 501.

7th of February 2017, Memorie van Toelichting: Vaststellingswet Boek 1 van het nieuwe Wetboek van Strafvordering: strafvordering in het algemeen.

19th of July 2019, Concept regeling, Wetsvoorstel Innovatiewet Strafvordering, www.internetconsultatie.nl.

19th of July 2019, Memorie van Toelichting Innovatiewet Strafvordering, www.internetconsultatie.nl.

Case Law

Lower Courts:

Lower Court of Noord-Nederland, 11th of July 2019, ECLI:NL:RBNNE:2019:2986.

Lower Court of Midden-Nederland, 7th of June 2018, ECLI:NL:RBMNE:2018:2655.

Courts of Appeal:

Court of Appeal of Amsterdam, 30th of March 1993.

Court of Appeal of Amsterdam, 12th of September 2016. ECLI:NL:GHAMS:2016:3676.

Court of Appeal of Amsterdam, 25th of January 2017, ECLI:NL:GHAMS:2017:216.

Court of Appeal of Arnhem-Leeuwarden, 14th of July 2017, ECLI:NL:GHARL:2017:6069.

Court of Appeal of Amsterdam, 6th of April 2018, ECLI:NL:GHAMS:2018:1218.

Court of Appeal of The Hague, 19th of December 2018, ECLI:NL:GHDHA:2018:3529.

Court of Appeal of Amsterdam, 23thrd of October 2019, ECLI:NL:GHAMS:2019:4341.

Supreme Court:

Supreme Court, 8th of October 1985, ECLI:NL:PHR:1985:AC0537, m.nt. A.C. ‘t Hart.

Supreme Court, 29th of March 1994, ECLI:NL:HR:1994:AD2076.

Supreme Court, 30th of March 2004, ECLI:NL:HR:2004:AM2533.

Supreme Court, 19th of February 2013, ECLI:NL:HR:2013:BY5321.

Supreme Court, 26th of March 2013, ECLI:NL:HR:2013:BY9718.

Supreme Court, 4th of April 2017, ECLI:NL:HR:2017:584.

Supreme Court, 4th of april 2017, ECLI:NL:HR:2017:588.

Supreme Court, 4th of April 2017, ECLI:NL:HR:2017:592.

Supreme Court, 4th of November of 2017, ECLI:NL:HR:2017:2869.

Supreme Court, 23th January of 2018, ECLI:NL:HR:2018:71.

Supreme Court, 10th of July 2018, ECLI:NL:HR:2018:1121.

Supreme Court, 18th of December 2018, ECLI:NL:HR:2018:2323.

Supreme Court, 11th of June 2019, ECLI:NL:HR:2019:891.

Supreme Court, 9th of July 2019, ECLI:NL:HR:2019:1079.

Supreme Court, 9th of July 2019, ECLI:NL:HR:2019:1079, m.nt. N. Jorge.

Supreme Court, 18th of February 2020, ECLI:NL:HR:2020:123.

ECtHR

ECtHR Harju v. Finland, 15th of February 2011, nr. 56716/09.

ECtHR Petri Sallinen v. Finland, 27th of September 2005, nr. 50882/99.

ECtHR Modestou v. Greece, 16th of March 2017, nr. 51693.13.

Books

Council of Europe/European Court of Human Rights, 2019, Guide on Article 8 of the Convention – Right to respect for private and family life.
Koops, B.J. and Oerlemans, J.J., Strafrecht & ICT, Den Haag: [2019] SDU.
Politieacademie 2019, Digitalisering en de opsporingspraktijk, juridische aspecten, versie 3.3.

Opinions, Recommendations and Reports

Commissie modernisering opsporingsonderzoek in het digitale tijdperk, Regulering van opsporingsbevoegdheden in een digitale omgeving, s.l. 2018.

Council for the Judiciary Advice Amendment to the Code of Criminal Procedure, 2th of October 2019.

Devroe, E., Malschm M., Matthys, J. & Minderman, G., *Toezicht op strafvorderlijk overheidsoptreden*, [2017] WODC.

Discussiestuk 'Onderzoek ter plaatse, inbeslagneming en doorzoeking en onderzoek van gegevensdragers en in geautomatiseerde werken' van 6 juni 2014.

Houwing, L, Reactie op consultatie Innovatiewet Strafvordering, Bits of Freedom, 22th of August 2019.

Opinion of AG Bleichrodt, 25th of October 2016, ECLI:NL:PHR:2016:1047.

Opinion of AG Harteveld, 26th of September of 2017, ECLI:NL:PHR:2017:1245.
Opinion of AG Bleichrodt, 28th of November 2017, ECLI:NL:PHR:2017:1470.
Opinion of AG Vegter, 15th of May 2018, ECLI:NL:PHRL2018:764.
Opinion of AG Spronken, 5th of November 2019, ECLI:NL:PHR:2019:1121.
Wetenschappelijke commissie van de Nederlandse Vereniging voor Rechtspraak, Advies Innovatiewet Strafvordering, 5th of October, 2019.

Articles and Journals

Gritter, E., 'Opsporing in de digitale wereld: het onderzoek van in beslag genomen gegevensdragers', (2016) Delikt en Delikwent 43.
Van der Voort, N., 'Onderzoek aan een in beslag genomen smartphone: het labyrint van de (toekomstige) wetgeving en jurisprudentie', (2017) Tijdschrift voor Bijzonder Strafrecht en Handhaving.
Stevens, L., 'Onderzoek in een smartphone: zoeken naar een redelijke verhouding tussen privacybescherming en werkbare opsporing', (2017) Ars Aequi, p. 730-735.