5 Gathering publicly available online information

This chapter aims to answer the fourth research question with regard to the gathering of publicly available online information (RQ 4a): *How can the legal framework in Dutch criminal procedural law be improved to adequately regulate the gathering of publicly available online information?* Within this study, the investigative method of gathering publicly available online information is subdivided into (1) the manual gathering of publicly available online information, (2) the automated gathering of such information, and (3) the observation of online behaviours of individuals. To answer this research question, the investigative method is placed within the Dutch legal framework and further analysed to determine whether Dutch law meets the normative requirements. In chapter 3, these normative requirements were identified as follows: (1) accessibility, (2) foreseeability, and (3) the quality of the law.

In chapter 4, it was determined for each method what degree of privacy interference is involved in its application. By positioning each method on the interference 'scale', it was further determined which type of regulation is required in each case, ranging from (a) a general legal basis for light interferences, (b) detailed regulations in statutory law or guidelines for more serious interferences that restrict the investigative method (with regard to specific crimes, in duration, et cetera) and (c) detailed regulations in statutory law that restrict the investigative method with the procedural safeguard of authorisation of an investigative judge for very serious interferences. The more serious the interference, the stricter are the requirements for the (1) accessibility, (2) foreseeability, and (3) the quality of the law. In case law, the ECtHR does not always strictly separate the three normative requirements and consider them all as part of the quality of the law.[1] However, in this study, these normative requirements are examined separately. The requirement of the quality of the law focuses in this research on the level of detail of the regulations and procedural safeguards that are present in the regulations for the investigative method.

1 See, e.g., ECtHR 25 September 2001, *P.G. and J.H. v. The United Kingdom*, appl. no. 44787/98, § 44: *"The expression "in accordance with the law" requires, firstly, that the impugned measure should have some basis in domestic law; secondly, it refers to the quality of the law in question, requiring that it should be accessible to the person concerned, who must moreover be able to foresee its consequences for him, and that it is compatible with the rule of law"*

For the method of gathering publicly available online information, the analysis in subsection 4.1.3 showed that data protection regulations should apply as a baseline for this investigative method. The specific requirements that are further desirable for the regulation of the three distinguished categories of gathering publicly available online information differs per method.

Case law indicates that the ECtHR takes into consideration the fact that the type of information at issue here is publicly available to everyone, including law enforcement authorities. At the same time, the more information these authorities gather and process, the greater becomes the privacy interference that takes place. Legislators should create an adequately detailed legal basis for each variant of the investigative method in which the right to privacy is properly balanced with the particular privacy interference involved in each case. It must be noted here that ECHR rights only specify the minimum level of protection required for the individuals involved. Contracting States to the convention can incorporate further requirements in the legal frameworks that regulate the different types of information gathering used as investigative methods. In this regard, before proceeding, it is important to highlight important aspects of the Dutch legal framework that pertain to regulating investigative methods. This overview is also relevant for the analysis of the other three digital investigative methods, which is presented in chapters 6 to 8.

Features of the Dutch legal framework for investigative methods

As explained in section 1.1, the Netherlands has a civil law system with a strong commitment to the principle of legality. This is particularly the case in criminal and criminal procedural law. In criminal procedural law, as laid down in art. 1 DCCP, the legality principle prescribes that *"criminal procedure is only carried out in the manner provided by law"*.[2] Here 'law' refers to statutory law that is established by acts of the Dutch House of Representatives and reviewed by the Dutch Senate.

In the context of regulating investigative methods, the implication is that – in principle – investigative methods are regulated by statutory law. However, not all investigative methods are covered in detail in statutory law. Over time, the general rule has developed that investigative methods that (1) do not – or only in a minor way – interfere with the fundamental rights and freedoms of individuals and (2) do not endanger the integrity of criminal investigations do not require detailed regulations in criminal

2 See art. 1 DCCP.

procedural law.[3] Investigative methods that interfere with fundamental rights and freedoms of individuals in more than a minor manner or endanger the integrity of criminal investigations do require detailed regulation in law. In Dutch criminal procedural law, the possibility also exists to regulate administrative or technical aspects of investigative methods outside of criminal procedural law in lower regulations than statutory law.[4]

Similar to the *scale of gravity for privacy interferences* that was deduced from art. 8 ECHR, under Dutch law, the more that investigative methods interfere with the rights and freedoms of the involved individuals or threaten the integrity of criminal investigations, the more detailed the regulations for investigative methods must be, with more accompanying safeguards.[5] An important structural safeguard in this regard lies in the fact that, the law will determine who has the power to apply and authorise the application of investigative powers. Depending on the gravity of the power, that authority will be higher, ranging from (1) a law enforcement official[6], (2) a public prosecutor, or (3) an investigative judge. Furthermore, these powers are generally

3 The investigative method is then based upon art. 3 of the Dutch Police Act and art. 141 in conjunction with 142 DCCP. See also, e.g., Fokkens & Kirkels-Vrijman 2009 in: Borgers, Duker & Stevens (ed.) 2009 and Borgers 2015. This standard was first set in the landmark case of *Zwolsman* in 1995, in which the Dutch Supreme Court decided that searching trash bags of citizens was not a privacy-infringing investigative method to the extent that it required detailed regulations in the Dutch Criminal Procedural Code (HR 19 December 1995, ECLI:NL:HR:1995:ZD0328, *NJ* 1996, 249 m. nt. Schalken). The standard was later affirmed with regard to other investigative methods by the Dutch legislature in the explanatory memorandum to the Special Investigative Powers Act (*Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1996/97, 25 403, no. 3, p. 110 and 115) and the Dutch Supreme Court (see, e.g., HR 20 January 2009, ECLI:NL:HR:2009:BF5603, *NJ* 2009, 225, m.nt. Borgers, HR 13 November 2012, ECLI:NL:HR:2012:BW9338, *NJ* 2013, 413, m.nt. Borgers and HR 7 July 2014, ECLI:NL:PHR:2014:623). The literature reflects conflicting viewpoints concerning whether investigative methods that do not interfere with the rights and freedoms of individuals involved require a legal basis (cf. Knigge & Kwakman 2001, p. 193-205 and p. 310-325 in: Groenhuijsen & Knigge 2001).

4 See also the letter regarding the contours of the 'Modernising Criminal Procedural Law' project of 30 September 2015, p. 10-11. Available at: https://www.rijksoverheid.nl/documenten/kamerstukken/2015/09/30/brief-aan-de-tweede-kamer-modernisering-wetboek-van-strafvordering-plus-contourennota (last visited on 23 March 2016). Borgers (2015) suggested that lower regulations can also be created for investigative methods that only interfere with the rights and freedoms of individuals in a minor manner and do not threaten the integrity of criminal investigations (cf. Borgers 2015).

5 In literature, there are also other reasons identified why investigative methods should be regulated in specific provisions in Dutch criminal procedural law, such as (1) to secure the reliability of the process of evidence-gathering, (2) to secure the right to fair trial in art. 6 ECHR, (3) to increase control checks and transparency of the evidence gathering-activity, (4) to fight corruption that may be take place in evidence-gathering activities, and (5) to protect the interests of others (besides the suspect) that may be involved in the application of investigative methods (see Groenhuijsen & Knigge 2002, p. 323-326).

6 In Dutch law, higher ranking law enforcement officials exist (called deputy prosecutors), which may authorise certain investigative activities. These are not further examined in this study.

restricted by limiting their application to criminal investigations with regard to certain crimes based on a crime's severity, as this is determined by the maximum sentence that can be imposed for that crime.

In essence, the regulations for investigative methods in Dutch law are similar to the scale of gravity for privacy interferences and the quality of the law that can be derived from art. 8 ECHR (see subsection 3.3.4). Again, depending on the gravity of the power, its regulation can be restricted by way of delineation of scope of application (in terms of manner and situations in which it can be applied), duration (including possibilities for extension), through stricter reporting requirements, and stricter proportionality and subsidiarity requirements.[7] The detail of these regulations both influences foreseeability (by indicating the manner the investigative method is applied) and the quality of the law (the level of detail and authorisation levels to apply the investigative methods). Throughout the chapters 5-8, the focus on the regulations for investigative methods is on the main mechanisms by restricting investigative methods based on authorisation requirements and limiting the application to the investigation of certain crimes. The higher level of detail for regulations is achieved by these restrictions. The heightened legality principle in Dutch criminal procedural law means that investigative methods will usually have a legal basis in Dutch law. However, the accessibility of digital investigative methods can be problematic when it is not recognised a digital method is distinct to its counterpart investigative method and requires its own regulation due to its intrusiveness. There can thus be an overlap in the issues of accessibility and foreseeability. From this chapter to chapter 8, it is examined whether the Dutch law currently correctly places the privacy interference that accompanies each investigative method on the scale of gravity and adequately regulates these investigative methods.

Structure of the chapter

This chapter is structured on the basis of the three normative requirements, each of which is investigated in a separate section. Each section discusses all three categories of the gathering of publicly available information in a subsection. A fixed research scheme is used to assess the accessibility and foreseeability of the Dutch legal framework with regard to the investigative methods. This research scheme consists of examining (A) statutory law, (B) legislative history, (C) case law, and (D) public guidelines. Thereafter, it is analysed whether Dutch law meets the normative requirements for regulations, which are extracted from art. 8 ECHR in chapter 4. Based on

7 Customary principles of proper criminal procedure, including those of proportionality and subsidiarity, as well as the prohibition of abuse of power also always apply to the exercise of criminal procedural powers, even though they are not stipulated explicitly by law.

the results of the analyses, recommendations are provided to improve the Dutch legal framework.[8]

Section 5.1 thus tests the *accessibility* of the Dutch legal framework's basis for applying the investigative method in the Netherlands, while section 5.2 examines to which extent the method is regulated in a *foreseeable* manner. Section 5.3 analyses whether the Dutch legal framework meets the desired *quality of the law* in the sense that it provides adequate level of detail for the regulations with adequate procedural safeguards. Based on the results of the analyses conducted in these three sections, section 5.4 provides concrete proposals as to how Dutch criminal procedural law can be improved to adequately regulate the gathering of publicly available online information. Section 5.5 concludes the chapter by presenting a summary of the findings.

5.1 Accessibility

An accessible basis in law means that the individual involved has an adequate indication of which regulations apply to the use of investigative methods in a particular case.[9] This section examines the accessibility of the regulations with regard to the gathering of publicly available online information.

As explained above, due to the heightened legality principle in Dutch criminal procedural law, it is expected that the legal basis for investigative methods will be accessible. It is rare that Dutch law enforcement authorities use secret internal guidelines and that such guidelines provide the legal basis for the application of investigative methods. However, it is possible that a digital investigative method is so novel that it has not yet been assigned a legal basis or that the Dutch legislature has failed to both distinguish it and create the corresponding detailed regulations that it requires. In that sense, the law may not be accessible, because there is no distinct clear legal basis for the digital variant.

The accessibility of all three categories of gathering publicly available online information is examined separately in subsections 5.1.1 to 5.1.3. Subsection 5.1.4 presents conclusions regarding the accessibility of the investigative method in Dutch law.

8 The recommendations are provided in section 5.4, as opposed to in each section that analyses the adequacy of the Dutch legal framework in terms of the identified normative requirements. This is done to present the relationships between these recommendations in a clearer manner.

9 See subsection 3.2.2 under A.

5.1.1 Manual gathering of publicly available online information

The manual gathering of publicly available information has been compared to the gathering of information from open sources, such as newspapers and telephone directories. In an online context, publicly available information can be manually gathered by utilising search engines and by gathering information from online forums and social media services. The accessibility of this investigative method in Dutch law is examined below using the research scheme that is mentioned in the introduction to this chapter.

A Statutory law

The manual gathering of publicly available online information is not regulated in detail in the DCCP. The investigative method can be based on the general task description for law enforcement officials to investigate crimes that is contained in art. 3 of the Dutch Police Act, insofar as the investigative method (1) does not interfere – or interferes in only a minor way – with the fundamental rights and freedoms of individuals and (2) does not endanger the integrity of criminal investigations. Art. 3 of the Dutch Police Act reads as follows:

"The police have the task, subordinate to the competent authority and in compliance with the applicable rules, to ensure the effective enforcement of the law and provide assistance to those in need".[10]

This provision itself does not explicitly state that law enforcement officials can derive from it the authority to investigate crimes and therewith apply investigative acts that interfere with the right to privacy. It only describes the broad task description of law enforcement officials. The task of criminal law enforcement, including the investigation of crimes, falls under the task of the effective enforcement of the law. The competent authority in that context is the public prosecutor. Given the general nature and broadness of this provision, it can be concluded that statutory law itself does not provide a distinct explicit legal basis for the manual gathering of publicly available online information.

B Legislative history

In 1999, the Minister of Justice stated in its explanatory memorandum to the Computer Crime Act II that: *"law enforcement officials can look around in the digital world and take notice of publicly available information just like anyone else*".[11] It added that *"an explicit basis in law is not required for this activity, insofar the activities are part of the tasks of law enforcement authorities"*.[12] No mention is

10 All translations of the statutory provisions are made by the author.

11 *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1998/99, 26 671, no. 3 (explanatory memorandum Computer Crime Act II), p. 35.

12 See also *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1998/99, 26 671, no. 3 (explanatory memorandum Computer Crime Act II), p. 35.

made about the investigative method in the explanatory memorandum to the Special Investigative Powers Act.

The explanatory memorandum then specified that: "*the power to look around on a publicly accessible network does not imply the power to systematically download information about individuals from the Internet and store that information in police systems*".[13] Thereafter it warned that the gathering of information from the Internet is regulated by *data protection regulations* that restrict this type of evidence gathering to the degree that it is necessary to properly execute the police task.[14]

Dutch legislative history thus indicates that this investigative method can be based on art. 3 of the Dutch Police Act, whilst it is further restricted by data protection regulations. In the literature, this view is supported by Van der Bel, van Hoorn, and Pieters (2013, p. 325). At the same time, the explanatory memorandum to the Computer Crime Act II states that a distinct legal basis is required for the application of the investigative method, i.e., a special investigative power in the DCCP, *"as soon as the investigation can be characterised as 'systematic'"*.[15] However, it does not state which special investigative power should apply in such a case. Koops (2012, p. 34) argues that the special investigative power for systematic observation applies when information is systematically gathered from the Internet. The special investigative power for systematic observation is formulated in art. 126g(1)DCCP Dutch as follows:

"In case of reasonable suspicion of a crime, a public prosecutor can order a law enforcement official to systematically follow a person or systematically observe the behaviours of a person, insofar this is in the interest of the investigation"[16].

In contrast to what I argued in 2012 (Oerlemans & Koops 2012, p. 45), I no longer think that this special investigative power provides the proper legal basis for the investigative method at hand. The investigative method of observation concerns gathering evidence in a criminal investigation by following a person or systematically observing his behaviours. As such, the method starts at a specific moment in time. *From that moment on*, information is gathered using the investigative method of observation. In contrast, the manual gathering of publicly available online information concerns the gathering of information that has been generated *in the past*. For that reason,

13 *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1998/99, 26 671, no. 3 (explanatory memorandum Computer Crime Act II), p. 36.

14 See also *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1998/99, 26 671, no. 3 (explanatory memorandum Computer Crime Act II), p. 36.

15 *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1998/99, 26 671, no. 3 (explanatory memorandum Computer Crime Act II), p. 36.

16 Emphasis added. The relevant requirements to apply the investigative method are examined in section 5.2. As explained in subsection 1.3.2, only the provision for ´classical investigations´ (in Title IV and IVA of the DCCP) are examined.

observation in the sense of art. 126g DCCP does not take place when this method is applied.[17]

To conclude, legislative history indicates on the one hand that the investigative method can be based on art. 3 of the Dutch Police Act and that the investigative method is restricted by data protection regulations. On the other hand, legislative history warns that the investigative method cannot be applied systematically on this basis, yet does not indicate which special investigative power can provide the appropriate legal basis for the investigative method.

C Case law

There is only *one* Dutch case available that explicitly deals with the legitimacy of the manual gathering of publicly available online information by law enforcement officials.[18] This case concerns a financial fraud investigation in 2004 in which a law enforcement official used 'Google Earth' to zoom in on the suspect's garden to ascertain whether the suspect had fraudulently acquired specific chairs and had them shipped to his home address instead of a company address. The investigating officer ascertained with the use of Google Earth that the two 'Bubble Club' chairs ordered were indeed located in the suspect's garden, which provided important evidence that the suspect had committed fraud.

The suspect's lawyer objected to the online evidence-gathering activity. He argued that the investigative method was unlawful, stating that the investigative act should have been based on a special investigative power regulated in the DCCP (although he did not specify which one), since the investigative method interferes with the right to privacy in more than minor manner.

The Court of The Hague disagreed with the suspect's lawyer, finding that the evidence-gathering activity only led to a minor interference with the individual's right to privacy. The activity could therefore be based on art. 3 of the Dutch Police Act.[19] The court also recalled the relevant legislative history and stated that online information cannot be 'systematically gathered and downloaded in police systems' upon the general legal basis of art. 3 of the Dutch Police Act. In this case, no systematic gathering of information had taken place in this case according to the court.

Thus, the only case that is available indicates that law enforcement officials can utilise Google Earth for evidence-gathering purposes based on art. 3 of the Dutch Police Act.

17 See also CTIVD 2014, p. 9 and p. 42.

18 Rb. Den Haag, 23 December 2011, ECLI:NL:RBSGR:2011:BU9409.

19 However, the judges did warn in their verdict that law enforcement officials are *"not allowed to systematically download information from the Internet and store it in police files"* on the legal basis of the description of the statutory duty of law enforcement officials to investigate crime. With this statement, the judges clearly refer to the legislative history cited above, in which this threshold is also mentioned.

D Public guidelines

The Guideline for the Special Investigative Powers of the Public Prosecution Service from 2014 only states that law enforcement officials are not required to issue data production orders to obtain information that is publicly accessible.[20] Data production orders are regulated as special investigative powers in Dutch criminal procedural law. These regulations are extensively analysed in chapter 6.

Within the guideline, the 'public part of the Internet' is provided as an example of information that is publicly accessible.[21] The guideline does not specify which other special investigative powers may apply in the context of gathering publicly available information. Here it is noteworthy that the guideline also does not differentiate between the (1) manual gathering of publicly available online information, (2) automated gathering of publicly available online information, and (3) the observation of online behaviours of an individual. The guideline also does not refer to any special investigative power that may provide a detailed legal basis for the systematic gathering of publicly available online information. It can be taken as a point of departure therefore that the Guideline for Special Investigative Powers implicitly holds that the gathering of publicly available online information can be based on art. 3 of the Dutch Police Act.

5.1.2 Automated gathering of publicly available online information

The automated gathering of publicly available online information differs from the manual gathering of such information in the sense that it involves using automated data collection systems. The accessibly of the regulations for the investigative method are examined below using the announced research scheme.

A Statutory law

The automated gathering of publicly available online information is not regulated in specific provisions of the DCCP. Again, the general legal basis in art. 3 of the Dutch Police Act may apply. As said, this is a general and broad provision and does not refer to any particular method.

Statutory law therefore does not provide a distinct explicit legal basis for the automated gathering of publicly available information.

B Legislative history

The explanatory memoranda of the Special Investigative Powers Act and the Computer Crime Act II both do not refer to this investigative method. The latter mentions that *law enforcement officials* can 'look around on the

20 *Stcrt.* 2014, no. 24442.

21 See section 2.10 in the Guideline for Special Investigative Powers.

Internet'.[22] However, this is different from the automated gathering of publicly available online information, which involves *software* collecting information automatically. However, in 2013, the Dutch government mentioned that the use of the 'iColumbo' automated online data collection system meets the Dutch Police Files Act's requirements for storing personal information about individuals in police systems.[23] This statement implies that the investigative method can be based on art. 3 of the Dutch Police Act and that the investigative method is only restricted by data protection regulations. As explained in subsection 2.2.2, the Dutch iColumbo system reportedly aims to provide *"an 'intelligent, automated, "near" real-time Internet monitoring service' for governmental investigators"*.[24]

Legislative history thus indicates that the investigative method can be based on art. 3 of the Dutch Police Act and that data protection regulations apply to the automated gathering of publicly available online information.

C Case law

No Dutch case law is available with regard to the automated gathering of publicly available online information as an investigative method.

D Public guidelines

The Guideline for Special Investigative Powers also fails to mention the automated gathering of publicly available online information as an investigative method. As explained under D in subsection 5.1.1, this guideline only specifies that no data production orders are required to obtain information from publicly accessible parts of the Internet.[25] The guideline does not differentiate between various types of gathering of publicly available online information.

The guideline therefore provides no indication of the legal basis for applying this investigative method.

5.1.3 Observation of online behaviours of individuals

Observing the online behaviours of individuals is an investigative method that takes place on publicly accessible places on the Internet, such as online forums, chat services and social media, insofar as anyone can observe that information. The observation of online behaviours of individuals starts at a

22 See *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1998/99, 26 671, no. 3 (explanatory memorandum Computer Crime Act II), p. 35 and subsection 5.1.1 under B.

23 See the memorandum 'Freedom and safety in the digital society. An agenda for the future' of 14 December 2013, 26 643, no. 298, p. 12.

24 See 'Deelprojectvoorstel, Ontwikkeling Real Time Analyse Framework voor het iRN Open Internet Monitor Network', 'iColumbo'. Available at http://www.nctv.nl/Images/deel-projectvoorstel-ontwikkeling-icolumbo-alternatief_tcm126-444133.pdf (last visited 23 December 2015).

25 See section 2.10 of the Guideline for Special Investigative Powers.

specific point in time and therefore does not entail the gathering of information from individuals that has been published in the past. As such, it differs from the investigative method of manual and automated gathering publicly available online information.[26] The accessibility of the legal basis for this investigative method is examined below using the announced research scheme.

A Statutory law

For the observation of online behaviours, the legal basis for the special investigative power for systematic observation in art. 126g DCCP may be appropriate. As explained in section 5.1.1, this provision describes this evidence gathering-activity as *following a person* or *observing the behaviours of an individual*. This text does not restrict the investigative method to application in the physical world.[27]

However, the special investigative power only applies when the observation is *systematic* in nature. The *non-systematic* observation of behaviours of individuals can be based on art. 3 of the Dutch Police Act.

B Legislative history

In 1999, in the explanatory memorandum to the Computer Crime Act II, it was noted that the point of departure is that special investigative powers, such as systematic observation, can also be applied in the digital world.[28] It also stated that special investigative powers that are applied online must fulfil the same conditions as those that are applied in the physical world.[29] The explanatory memorandum of the Special Investigative Powers explicitly states that non-systematic observation can be based on art. 3 of the Dutch Police Act (then art. 2).[30] As a consequence, systematic online observation requires the special investigative power of systematic observation and the non-systematic online observation can be based on art. 3 of the Dutch Police Act.

Legislative history thus clearly indicates that the current regulations for observation in Dutch criminal procedural law also apply in an online context.

---

26 For a similar distinction, see p. 86-87 of the explanatory memorandum of the new bill for the Security and Intelligence Services Act and CTIVD 2014, p. 9 and p. 42.

27 The explanatory memorandum to the Special Investigative Powers Act explicitly states that the special investigative powers are formulated in a 'technological neutral manner' (see *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 55).

28 *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1998/99, 26 671, no. 3 (explanatory memorandum Computer Crime Act II), p. 36.

29 See also *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1998/99, 26 671, no. 3 (explanatory memorandum Computer Crime Act II), p. 36.

30 see *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 110.

C Case law

No case law that specifically addresses the observation of the online behaviours of individuals as an investigative method is available. A large amount of case law is available concerning observation in the physical world.[31] However, this case law does not indicate which legal basis applies to *online* observations, i.e., art. 3 of the Dutch Police Act or the special investigative power for systematic observation.

Case law therefore does not indicate the legal basis for the examined investigative method.

D Public guidelines

The Guideline for Special Investigative Powers specifies how the special investigative power for systematic observation can be distinguished from other special investigative powers.[32] This distinction is as follows. The investigative method of observation involves law enforcement officials *passively observing the behaviours* of an individual to gather evidence in a criminal investigation,[33] while undercover investigative methods entail law enforcement officials that *interact with an individual in an undercover capacity* to gather evidence.[34]

The guideline refers to legislative history to determine when observation becomes systematic (see subsection 5.2.3) and specifies the recommended procedure to make use of a special observation team to apply the special investigative power.

In contrast to legislative history, the guideline does not explicitly state that the investigative method can also be applied in an online context.

5.1.4 Section conclusion

The analysis above has shown that Dutch law does not distinguish between the various types of gathering of publicly available information as they have

31 When using the Dutch equivalents of the search terms 'systematic observation' and 'procedural defects' on the website www.rechtpraak.nl, 195 cases are available for analysis (on 23 July 2016). This website offers a large database of case law that is uploaded by Dutch courts. In most of these cases, the legal basis to use observation as an investigative method is contested by the suspect. After a thorough analysis, *none* of these cases concerns the online observation of individuals' behaviours.

32 See section 2.6 of the Guideline for Special Investigative Powers.

33 See also Oerlemans & Koops 2012, p. 43.

34 See also *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 35. See also Buruma 2001, p. 84-85 and Corstens & Borgers 2014, p. 506. The legislature emphasised in its explanatory memorandum to the Special Investigative Powers Act that the investigative method of 'systematic information gathering' implies 'more than just listening or observing'. See also *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 38 indicating the investigative method of 'systematic information gathering' must only be used when the undercover investigator *engages in a conversation* with a suspect.

been described as distinct categories in this study. In the explanatory memorandum to the Computer Crime Act II, reference is only made to the gathering of publicly available online information and the observation of online behaviours. In this study, a distinction is made between (1) the manual gathering of publicly available online information, (2) the automated gathering of publicly available online information, and (3) the observation of online behaviours of individuals.

With regard to the manual gathering of publicly available online information, the explanatory memorandum to the Computer Crime Act II indicates that the investigative method can be based on art. 3 of the Dutch Police Act. According to legislative history, a special investigative power must be applied for the 'systematic' gathering of publicly available online information. Given this, Dutch law can be considered *accessible* for this investigative method, in the sense that there is an indication of which legal basis applies. However, it remains unclear from the examined legal sources which special investigative power is applicable when the manual gathering becomes systematic.

Dutch legislative history indicates that the Dutch automated data collection system of 'iColumbo' can be based on art. 3 of the Dutch Police Act and that the use of the system is restricted by data protection regulations. Therefore, again there is an *accessible* legal basis for the automated gathering of publicly available online information.

With regard to the investigative method of observing online behaviours of individuals, the explanatory memorandum to the Dutch Computer Crime Act II and statutory law also provide an indication of what the legal basis is. The former is most concrete and makes it clear that the investigative method can be based either on (1) the description of the statutory duty of law enforcement officials to investigate crimes that is provided in art. 3 of the Dutch Police Act or (2) the special investigative power for systematic observation that is contained in art. 126g of the DCCP. The legal basis for applying this investigative method is therefore considered as *accessible*.

5.2 Foreseeability

The fact that an accessible legal basis exists however is only one of the requirements that flow forth from art. 8 ECHR for the regulation of investigative methods. That legal basis must also be foreseeable. A foreseeable legal framework is one that prescribes with sufficient clarity (1) the scope of the power conferred on the competent authorities and (2) the manner in which an investigative method is exercised.[35] As such, given that a relationship exists between the gravity of a privacy interference and the degree of detail in which the method at issue must be regulated, the foreseeability

35 See subsection 3.2.2 under B.

requirement is particularly important. It is in the context of this requirement that the balancing and fine-tuning of the interference and the detail of the regulation must be achieved.

The foreseeability of the Dutch legal framework for all three categories of gathering publicly available online information is examined in subsections 5.2.1 to 5.2.3. Subsection 5.2.4 then draws conclusions regarding the investigative methods' foreseeability in Dutch law.

5.2.1 Manual gathering of publicly available online information

This subsection examines whether the manual gathering of publicly available online information is regulated in a foreseeable manner by exploring the same legal sources used above.

A Statutory law

The analysis in subsection 5.1.1 has shown that the manual gathering of publicly available online information can be based on the general description of the duty of law enforcement officials to investigate crime in art. 3 of the Dutch Police Act, insofar as the investigative method is not applied in a systematic manner. When information is gathered in a systematic manner, a special investigative power should apply. However, the examined sources in law do not indicate which special investigative power should apply. In addition, the explanatory memorandum to the Dutch Computer Crime Act II does not elaborate on what determines the difference between systematic and non-systematic application of this investigative method. The scope of this investigative method thus remains unclear.

The general legal basis provided in art. 3 of the Dutch Police Act does not restrict this investigative method in a concrete manner. Law enforcement officials are authorised to apply investigative methods based on this legal basis in criminal investigations with regard to any crime. However, the explanatory memorandum to the Computer Crime Act II indicates that data protection regulations do restrict the investigative methods. Indeed, several authors emphasise that data protection regulations apply to this investigative method, even though it is not restricted by detailed regulations in criminal procedural law (cf. Koops 2012a, p. 32, Van der Bel, van Hoorn & Pieters 2013, p. 325, and Lodder et al. 2014, p. 73).[36]

36 Lodder et al. refer to opinion 03/2013 of the 'Article 29' Data Protection Authority Working Group of 2 April 2013, stating that: *"In this context, it is important to note that any information relating to an identified of identifiable natural person, be it publicly available or not, constitutes personal data. Moreover, the mere fact that such data has been made publicly available does not lead to an exemption from data protection law. The reuse of personal data made publicly available by the public sector, thus remains subject in principle to the relevant data protection law."* (at 10). See Koops et al. (2012, p. 41-43) with regard to data protection law and the collection of publicly available information from the Internet.

B Legislative history

The explanatory memorandum to the Computer Crime Act II specifies the scope of the investigative method. To a certain extent, it also specifies the manner it is executed.

Essentially, legislative history indicates that law enforcement officials can (1) 'look around on the Internet', (2) download relevant information from a variety of sources, and subsequently (3) store that information in police databases as part of their statutory duty to investigate crime.[37] The aforementioned explanatory memorandum also states that law enforcement officials can mask their IP addresses and use pseudonyms in order to remain undetected in their evidence-gathering activities.[38]

However, as mentioned above, the legislative history does not clarify what determines when information is gathered in a 'systematic manner' and when the application of a special investigative power is appropriate.

C Case law

The case law analysis in subsection 5.1.1 showed that only one case specifically deals with the manual gathering of publicly available online information by law enforcement officials. This case showed that law enforcement officials can make use of Google Earth based on art. 3 of the Dutch Police Act, thus without being bound to the detailed frameworks that apply for specific special investigative powers. This case thus does not provide much information about the scope of the investigative method. For instance, it remains unclear whether it makes a difference (1) if information is gathered from social media services instead of Google Earth or (2) if law enforcement officials may utilise commercial 'intelligence' providers that collect publicly available online information based on art. 3 of the Dutch Police Act.

D Public guidelines

The Guideline for Special Investigative Powers does not provide an indication concerning the scope of the investigative method or the manner in which law enforcement officials are to apply it.

5.2.2 Automated gathering of publicly available online information

This subsection examines the foreseeability of the legal basis for the automated gathering of publicly available online information. In subsection 5.1.2, it became clear that only one letter to Dutch parliamentary members indicated that the investigative method can be applied on the basis of art. 3 of the Dutch Police Act and that data protection regulations apply to this investigative method. However, there are no sources in law that indicate

37 See *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1998/99, 26 671, no. 3 (explanatory memorandum Computer Crime Act II), p. 35-36.

38 See *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1998/99, 26 671, no. 3 (explanatory memorandum Computer Crime Act II), p. 35.

how Dutch law enforcement officials should interpret these regulations in concrete terms (cf. Lodder & Schuilenburg 2016, p. 152).

The research results show that there is a clear misalignment between current practice and the limited description of the gathering of publicly available online information in legislative history. The explanatory memorandum to the Computer Crime Act II only specifies that law enforcement officials may (1) 'look around on the Internet', (2) download relevant information from a variety of sources, and (3) store that information in police databases as part of their statutory duty to investigate crime.[39] In practice, commercial and public automatic data collection systems download publicly available online information for law enforcement purposes every day.[40] That information is subsequently analysed and presented to law enforcement officials in the most efficient manner possible.

Automated data collection activities thus significantly extend beyond 'looking around on the Internet' for evidence-gathering purposes. As argued in section 4.1, this investigative method seriously interferes with the right to privacy and requires detailed regulations in either statutory law or public guidelines. The lack thereof can be explained by the fact the examined legislative history dates back to 1999. However, given the technological developments since then and the reality that this method is used, detailed regulation is currently necessary.

5.2.3 Observation of online behaviours of individuals

In this subsection, the foreseeability of the legal basis for observing the online behaviours of individuals is further examined by exploring the same legal sources used above.

A Statutory law

The analysis in subsection 5.1.3 has shown that the investigative method of the observation of online behaviours of individuals can be applied either on the basis of art. 3 of the Dutch Police Act or the special investigative power for systematic observation in art. 126g DCCP. If the investigative method is not applied systematically, a law enforcement official can observe the online behaviours of individuals based on art. 3 of the Dutch Police Act. This means that the investigative method can then be applied in as part of criminal investigations related to all crimes. In contrast, when it is applied systematically, the special investigative power for systematic observation must be used.

The special investigative power for systematic observation regulates this investigative method in detail. It specifies that it can be applied in criminal investigations involving all types of crimes, insofar as the investiga-

39 See *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1998/99, 26 671, no. 3 (explanatory memorandum Computer Crime Act II), p. 35-36.

40 See subsection 2.2.2.

tive method is in the interest of the investigation. A public prosecutor must authorise the application of the special investigative power. Art. 126g DCCP also dictates that the special investigative power can only be applied for a maximum period of three months, which can be extended by another three months.[41]

Statutory law thus clearly describes the manner in which the investigative method should be applied, on two different legal bases. However, from statutory law alone it is not clear when (online) observation becomes 'systematic' in nature.

B Legislative history

The explanatory memorandum to the Special Investigative Powers Act specifies the scope of this investigative method by indicating when the method becomes systematic and the special investigative power for systematic observation is thus applicable.[42]

In 1996, the Dutch legislature formulated the following five factors for determining whether observation is systematic: (1) duration, (2) place, (3) intensity, (4) frequency, and (5) whether a technical device is used to observe an individual's behaviours.[43] These five factors – 'particularly in their combination' – indicate "*whether more or less complete insights are obtained about certain aspects of an individual's private life*" and thus if the investigative method is being applied systematically.[44]

Application in an online context

The aforementioned five factors are designed for the physical world, which means that it is challenging to apply them to an online context (cf. Koops 2012a, p. 42 and Koops 2013, p. 663-664). The legislature has to date not provided guidance as to how to apply them in the digital world. However, to a certain degree the factors can be applied to the digital context analogically, as detailed below.

The first factor, namely the *duration* of observation, can be applied in a digital world given that behaviours on the Internet can be observed for a specific period of time.

The second factor of the *place* from which a person's online behaviours are visible can also be applied to the Internet. For example, Dutch legislative history mentions that observing an individual visiting a brothel is a

41 See art. 126g DCCP. See also Corstens & Borgers (2014, p. 508) with regard to the legal basis in the DCCP for the application of the investigative method of observation in the physical world.

42 See *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 26-27.

43 *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 26-27. See also *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1998/99, 26 671, no. 7, p. 46.

44 *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 26-27.

more intrusive investigative activity than observing an individual walking down the street.[45] Similarly, in an online context, observing the online conversations of individuals on a chat service designed for conversations of a sexual nature may be more privacy sensitive than observing the online behaviours of individuals on a chat service that aims to bring hobbyists of Lego together.

The third factor, namely the *intensity* of the investigative method, may relate in a digital context to the amount and diversity of the information that is gathered (cf. Oerlemans & Koops 2012, p. 45). For example, law enforcement officials can simultaneously observe an individual's behaviours on three different publicly accessible sources, such as Twitter account, a chat channel, and an online forum.

The fourth factor of the *frequency* of the observation of the behaviours of individuals can also be applied in an online context. For example, law enforcement officials can observe the behaviours of individuals on social media at regular intervals.

It remains unclear how the fifth factor of *using a technical device* can be applied in an online context. One can question whether utilising a computer with an internet connection to conduct online monitoring qualifies as using a 'technical device'. The use of an automated system that 'monitors' an individual's behaviours and sends frequent updates to a law enforcement official could possibly be interpreted as a technical device.

The interpretation of these five factors by analogy provides some guidance for the manner in which the investigative method is applied. However, it is unclear whether these factors are indeed adequately 'translated' to an online context and in which manner they are interpreted by the Dutch Police and Public Prosecution Service in practice. The articulated factors in legislative history are abstract and leave ample room for interpretation by law enforcement officials and public prosecutors. Furthermore, it is possible that other factors, which are specifically related to (features of) (privacy on) the Internet should be involved in determining whether not a particular application of this method is systematic. This requires consideration by the legislator.

C Case law

As explained in subsection 5.1.3, no case law is available that specifically deals with the legal basis for observation as an investigative method in an online context. The only case law that is available regards the use of observation as an investigative method in the physical world. However, even this case law is highly divergent as to the questions of when observation in the physical world becomes systematic and the use of the special investigative

45 *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1997/98, 25 403, no. 7, p. 47.

power for systematic observation is thus required.[46] The case law simply repeats relevant parts of legislative history and does not provide further information regarding the application of the special investigative power in an online context, besides what can be deduced from the particular facts of a case.

D Public guidelines

The Guideline for Special Investigative Powers only specifies the manner in which the special investigative power for the systematic observation of the behaviours of individuals applies in the physical world.[47] It does not provide concrete information as to when application of the investigative method becomes systematic in nature, even in the physical world. Therefore, the guideline also does not provide clarification with regard to the difference between systematic and non-systematic application of observation in an online context.

5.2.4 Section conclusion

The foreseeability of the Dutch legal framework in criminal procedural law with regard to the gathering of publicly available information can be assessed using the analysis conducted in subsections 5.2.1 to 5.2.3. The results of this analysis are presented below.

The investigative method of the manual gathering of publicly available online information is not regulated in detail in Dutch criminal procedural law. Data protection regulations restrict the investigative method, but not in a concrete manner. In addition, legislative history indicates that a special investigative power is applicable when the investigative method is applied systematically. It is not clear, however, what the systematic gathering of online information entails and which special investigative power should be applicable. For that reason, the legal basis for this investigative method is considered *not foreseeable*.

With regard to the automated gathering of publicly available online information, no detailed regulations exist in Dutch law. The examined legislative history clearly has a different investigative method in mind than the current use of automated online data collection systems. Data protection regulations also provide no concrete interpretation of how these regulations apply for the automated gathering of publicly available online data. Given the absence of an indication of the scope of the investigative method in Dutch law and the manner it is applied, the legal basis for this investigative method is considered *not foreseeable*.

---

46 See, e.g., HR 29 March 2005, ECLI:NL:HR:2005:AS2752, HR 12 October 2010, ECLI:NL:HR:2010:BM4211 and Rb. Court of Limburg, 6 November 2013, ECLI:NL:RBLIM:2013:8519.

47 See section 2.2 of the Guideline for Special Investigative Powers.

The observation of the online behaviours of individuals can be based on art. 3 of the Dutch Police Act or the special investigative power for systematic observation. Statutory law, legislative history, and case law provide an indication of the scope of and the manner in which the investigative method is applied in the physical world. However, the five factors provided in legislative history for determining when observation becomes systematic were originally developed for observation in the physical world. Due to the lack of further guidance in case law or applicable guidelines, it remains unclear how these five factors are should be applied in an online context. The interpretation of these factors is currently at the discretion of law enforcement officials, who hopefully consult public prosecutors as to whether using the special investigative power for systematic observation is appropriate (cf. Oerlemans & Koops 2012, p. 46). Therefore, I conclude that the legal basis for the investigative method of observing the online behaviours of an individual is *not foreseeable*.

5.3 Quality of the law

Under the umbrella of the normative requirement regarding the quality of the law, the ECtHR can specify not only the level of detail required for the description of a power but also the minimum procedural safeguards that must be implemented vis-à-vis a particular method that interferes with the right to privacy. The detail that the ECtHR requires in the law and procedural safeguards depends on the gravity of the privacy interference that takes place.[48] This 'scale of gravity for privacy interferences' with regard to the gathering of publicly available online information is illustrated in Figure 5.1.

48 See subsection 3.2.2 under C.

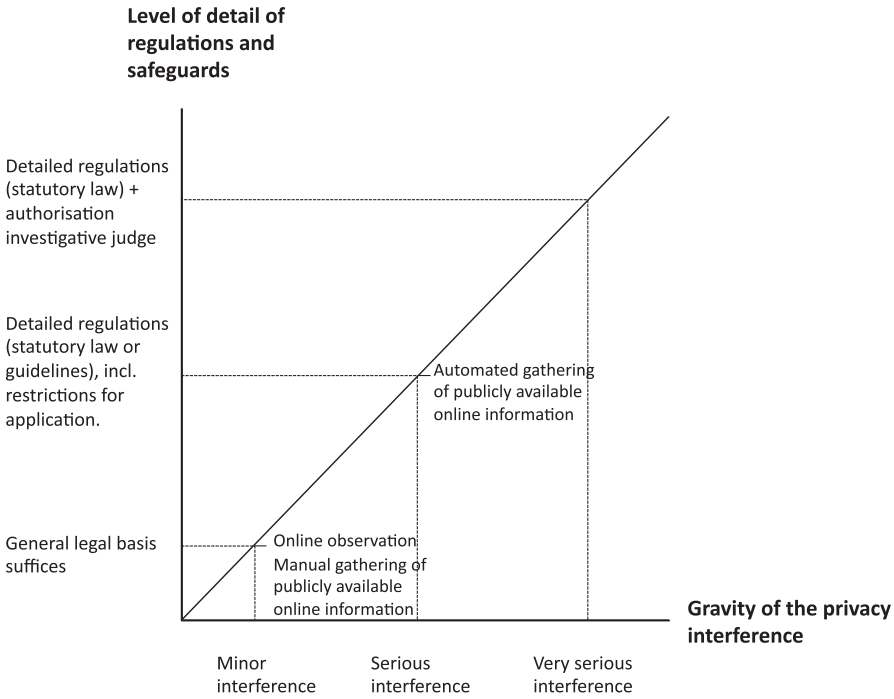

Figure 5.1: The scale of gravity for privacy interferences regarding the gathering of publicly available online information.

Figure 5.1 illustrates how it is likely that the ECtHR will not view the gathering of publicly available online information as a privacy infringing activity that merits detailed regulations in statutory law with stringent procedural safeguards. An important factor is that the information is publicly available to anyone and individuals can therefore expect that anyone, including law enforcement officials, can gather the information in a criminal investigation. However, data protection regulations restrict the evidence-gathering activity and require a minimum of protection to the individuals involved. In addition, the privacy interference is more serious when technologically advanced data collection systems are used, such as when publicly available online information is gathered automatically. In those circumstances, detailed regulations with procedural safeguards are desired as part of the quality of the law requirement.[49] Given the scale it deploys in case law, it may be expected that the ECtHR will also take this point of view. Of course, even if the ECtHR were not to set higher standards in this regard, the Dutch legal framework can require more detailed regulations with procedural safeguards for the different types of information gathering, based on higher standards derived from Dutch law.

49 See section 4.1 of chapter 4.

Remember that in the Netherlands, investigative methods that interfere with the rights and freedoms of individuals in a minor manner and do not threaten the integrity of criminal investigation can be based upon art. 3 of the Dutch Police Act.[50] Art. 3 of the Dutch Police Act does not require permission of a certain authority and does not restrict the application investigative method to criminal investigations with regard to certain crimes. Recently, the Dutch Supreme Court reaffirmed this interpretation of the criminal procedural legality principle in relation to the regulation of investigative methods.[51] On 1 July 2014, the Supreme Court decided that law enforcement authorities can send 'stealth text messages' (text messages that an individual receives, but cannot see) in order to localise an individual.[52] The text messages are sent while the individual is under surveillance by use of a wiretap. The Supreme Court reasoned that these stealth messages can be sent to a mobile phone of an individual based on art. 3 of the Dutch Police Act, insofar – depending duration, intensity, and frequency of the application of the investigative method – law enforcement officials do not acquire a more or less complete picture of certain aspects of an individual's life. The Dutch Supreme Court did not further specify at which point the application of a special investigative power is merited. Using the same reasoning, the Supreme Court also decided that law enforcement officials can use a so-called IMSI-catcher (a device that registers connecting cell phones by acting as a cell phone antenna) based on art. 3 of the Dutch Police Act, in order to track individuals.[53]

These judgements can be critiqued in the sense that they affect the required quality of the law for the regulation of investigative methods.[54] The main problem is that Dutch law enforcement authorities were not clear beforehand about their policy concerning the use of stealth messages to localise individuals. According to an *internal* guideline, the use of stealth messages must be mentioned in a police report and a public prosecutor must

50 See the introduction of this chapter.

51 See HR 1 July 2014, ECLI:NL:HR:2014:1563 and ECLI:NL:HR:2014:1569 and HR 1 July 2014, ECLI:NL:HR:2014:1562.

52 HR 1 July 2014, ECLI:NL:HR:2014:1563 and ECLI:NL:HR:2014:1569.

53 See also HR 1 July 2014, ECLI:NL:HR:2014:1562, *NBSTRAF* 2014/206, m. nt. C.J.A. de Bruijn. The Supreme Court took into consideration the circumstances at hand using (1) the factors mentioned above, (2) the fact that the investigative method is mentioned in a police report, (3) the fact that a public prosecutor ordered the application of the investigative method, and (4) the fact the special investigative powers of wiretapping and systematic observation were applied.

54 See most notably Borgers 2015 and HR 1 July 2014, ECLI:NL:HR:2014:1562, NJ 2015/115, m.nt. P.H.P.H.M.C. van Kempen.

authorize the investigative method.[55] Such a policy should have been public beforehand and the application of the investigative method should be described in a police report. As explained before[56], it is essential for the rule of law that individuals know under which conditions and in which manner investigative methods are applied by law enforcement officials, even when they (arguably) interfere with the right to privacy in only a minor manner.[57] It becomes even more essential where there is doubt that a general legal basis such as art. 3 of the Dutch Police Act is sufficient and that the investigative method rather requires the application of a special investigative power. When a policy for investigative methods is public, lawyers can object to the practice at trial and members of parliament can ask questions or take action by suggesting legislation for use of the investigative method. The Dutch Supreme Court could have been more critical about the secrecy surrounding the use of stealth text messages as an investigative method.[58] Hopefully, the practice of Dutch law enforcement authorities regarding the use of stealth text messages and IMSI catchers in the past, is not a harbinger of the use of digital investigative methods by law enforcement authorities that are at the border of interfering with the rights and freedoms of individuals in "*more than a minor manner*".

Hereinafter, the quality of the Dutch legal framework with regard to the identified categories of gathering publicly available online information as an investigative method is compared to the desired quality of the law as determined in chapter 4 for this method in subsections 5.3.1 to 5.3.3. Subsection 5.3.4 then presents conclusions regarding the adequacy of the quality of the Dutch legal framework for the digital investigative method.

55 See J.J. Oerlemans, 'Onduidelijkheid over de inzet van 'stealth smsjes' in opsporingsonderzoeken', *Computerrecht* 2013/217. See also the answers to parliamentary questions by Berndsen-Jansen and Schouw on 17 September 2013, about the article that law enforcement authorities unlawfully send stealth text messages to mobile phones to track suspect and the answers to parliamentary questions by Gesthuizen, Kooiman, Berndsen-Jansen and Schouw on 9 May 2014, about the use of stealth messages by law enforcement authorities for investigative purposes.

56 See subsection 3.2.2.

57 See similarly Borgers 2015, who argues that these kinds of judgments can lead to legal uncertainty for both law enforcement officials and citizens involved.

58 See also HR 1 July 2014, ECLI:NL:HR:2014:1562, NJ 2015/115, m.nt. P.H.P.H.M.C. van Kempen. Borgers (2015) suggests that the Surpreme Court could also prescribe more stringent conditions, such as authorisation of a public prosecutor (instead of taking it into account as a condition to decide on the legitimacy of the investigative method based on art. 3 of the Dutch Police Act).

5.3.1 Manual gathering of publicly available online information

The analysis in section 4.1 determined that the privacy interference that takes place when law enforcement officials manually gather publicly available online information is not likely to be considered as a serious interference by the ECtHR. As the information is publicly available, individuals can expect that anyone, including a law enforcement official, can gather the information in a criminal investigation. However, a graver interference with the right to privacy as defined in art. 8 ECHR takes place when personal information is stored in police systems. As part of the desired quality of the law, it was suggested in section 4.1 that data protection regulations should apply to the mere processing of personal information. Whereas the ECtHR only regards the systematic gathering and storage of information from publicly available sources as an interference of art. 8 ECHR, I argued that it is more appropriate to apply EU data protection regulations as soon as publicly available (online) information is processed by law enforcement authorities. Processing personal information about individuals does not require the systematic gathering and the storage of information in a police system. For example, a manual search of information about an individual on the Internet triggers data protection regulations. In this way, the right to privacy of individuals is protected sooner than the ECtHR currently requires.

Application to the Dutch legal framework
The Dutch legislator appears to assume that art. 3 of the Dutch Police Act suffices as a legal basis (in combination with data protection principles), insofar as the investigative method is not applied in a 'systematic' manner. When the investigative method is utilised systematically, a special investigative power should be applied.

However, the Dutch legislature has failed to clarify what the 'systematic gathering of online information' entails and which special investigative power is applicable in that case. Whether a digital investigative method interferes with the right to privacy in a minor manner is furthermore difficult to determine.

On the one hand, the amount of information about individuals that is available on the Internet has greatly increased since the legal basis for the investigative method was created in Dutch law back in 1999 (cf. Koops 2013, p. 663). This indicates the investigative method should nowadays *per se* be considered as more intrusive.

On the other hand, the gathering of publicly available information from the Internet about individuals involved in a criminal case is part of regular police work and is similar to gathering information from physical 'open sources' that law enforcement officials use to support criminal investigations. As the analysis of this investigative method in light of art. 8 ECHR has shown, the ECtHR will factor an individuals' public disclosure of information and public availability into its consideration. These factors will likely diminish the gravity of the privacy interference that takes place, since it influences the reasonable expectation of privacy of individuals.

However, it is worrisome that some law enforcement officials seem to believe that publicly available online information can be gathered infinitely (see Koops 2012a, p. 32 and Lodder et al. 2014, p. 72-73).[59] In this respect, the bad track record of Dutch law enforcement authorities regarding upholding the Police Files Act is also troubling.[60] Restrictions to evidence-gathering activities are only meaningful in terms of the quality of the law, insofar as the restrictions are effectively enforced.[61]

5.3.2 Automated gathering of publicly available online information

The ECtHR has shown in case law that it is critical of law enforcement activities that involve a pre-emptive collection of personal information for law enforcement purposes. When publicly available online information is automatically gathered using data collection systems, a more serious interference with the right to privacy as defined in art. 8 ECHR takes place. In addition, the use a 'technically sophisticated system' and the fact that information is processed about individuals who are not suspected of a crime indicate that the ECtHR will set stricter standards in this context. In section 4.1.3, I argued that the result of the balancing test that should be conducted in this regard, also in terms of the requirements of a legitimate aim and the necessity of the method in a democratic society should be reflected in detailed regulations for the investigative method. Existing data protection regulations can aid in both creating these new regulations and determining further adequate safeguards.[62]

Application to the Dutch legal framework

In the Netherlands, no detailed regulations are available for the investigative method of automated gathering of publicly available information. Considering the intrusiveness of this method, one can argue that it should be regulated as a special investigative power. However, automated data col-

59 See also Harry Lensink & Gerard Janssen, 'Plaats delict: social media', *Vrij Nederland*, 18 April 2014. Available at: http://www.vn.nl/Archief/Justitie/Artikel-Justitie/Plaats-delict-social-media.htm (last visited on 10 June 2015).

60 See, e.g., the following press releases of the Dutch Data Protection Authority: 'Regionale politiekorpsen niet toegerust op nieuwe eisen gegevensbescherming CBP zal vervolgonderzoek doen bij individuele korpsen', 14 October 2008, 'Verwerking persoonsgegevens door regionale politiekorpsen Vervolgonderzoek CBP naar functioneren politie infodesks', 16 July 2009, 'Politie en opsporingsdiensten verzuimen privacyaudit uit te voeren', 19 July 2011 and Bart de Koning, 'Nieuws: de politie blijkt op grote schaal de wet te overtreden', *De Correspondent*, 8 December 2015. Available at: https://decorrespondent.nl/3734/Nieuws-de-politie-blijkt-op-grote-schaal-de-wet-te-overtreden/446202963008-90777447 (last visited on 4 January 2016).

61 In that respect, see also ECtHR 4 December 2015, *Roman Zakharov v. Russia*, appl. no. 47143/06, § 250-301. Although this case regards the more privacy-intrusive investigative method of the interception of communications, it makes it clear that the ECtHR finds it important that the safeguards against abuse are effective and thus applied in practice.

62 See the analysis in subsection 4.1.3 under B.

lection systems can also be used for public order purposes. A separate bill that regulates the general use of automated data collection systems by law enforcement officials appears more appropriate.

The Dutch legislature currently has no plans to create detailed regulations that restrict the automated gathering of publicly available online information. As mentioned in subsection 5.1.2, the use of the 'iColumbo' automated online data collection system meets the Dutch Police Files Act's requirements according to the Dutch legislator.[63] This point of view is remarkable, since the cited report by Koops et al. *did not* state that the system is in line with data protection regulations. The report only stipulated the conditions that the system has to comply with in order to meet data protection requirements (Koops et al. 2012a, p. 41-43). Serious concerns may thus be raised as to whether the Dutch regulations for automated data collection systems meet the desirable quality of the law.

The need for more detailed regulations for the automated gathering of publicly available online information for law enforcement purposes is also supported by the cases of *Digital Rights Ireland v. Ireland* and *Seitlinger, Tschohl et al. v. Kärtner Landsregierung* (hereinafter: *Digital Rights Ireland* and *Seitlinger*) of the Court of Justice of the European Union (hereinafter: CJEU) (cf. Lodder & Schuilenburg 2016, p. 152).[64] Case law of the CJEU is directly applicable to the Dutch legal framework and its decisions must be incorporated into Dutch law. Both cases are therefore briefly examined.

On 8 April 2014, the CJEU decided in the landmark cases of *Digital Rights Ireland* and *Seitlinger* that retaining telecommunication data is a form of personal data processing that interferes with the right to respect for private life and the right to data protection as defined in art. 7 and 8 of the CFR.[65]

In its decision, the CJEU refers to case law of the ECHR regarding interferences with the right to privacy that take place when personal data is stored in police systems.[66] The CJEU additionally takes into consideration that personal information is also retained about individuals who are not suspected of a crime (cf. Boehm & Cole 2014, p. 35-38).[67]

In the cases of *Digital Rights Ireland* and *Seitlinger*, the Advocate General also argued that the retention of personal data may also harm aspects of the rights to freedom of expression and information. The reason for this

63 See the memorandum 'Freedom and safety in the digital society. An agenda for the future' of 14 December 2013, 26 643, no. 298, p. 12. See also subsection 5.1.2.

64 CJEU 8 April 2014, C-293/12 (*Digital Rights Ireland v. Ireland*) and C-594/12 (*Seitlinger, Tschohl et al. v. Kärtner Landsregierung*).

65 CJEU 8 April 2014, C-293/12 (*Digital Rights Ireland v. Ireland*) and C-594/12 (*Seitlinger, Tschohl et al. v. Kärtner Landsregierung*), § 29.

66 See CJEU 8 April 2014, C-293/12 (*Digital Rights Ireland v. Ireland*) and C-594/12 (*Seitlinger, Tschohl et al. v. Kärtner Landsregierung*), § 35 referring to ECHR 26 March 1987, *Leander v. Sweden*, appl. no. 9248/81, § 48, ECtHR 4 May 2000, *Rotaru v. Romania*, appl. no. 28341/95, § 46, ECtHR 29 June 2006, *Weber and Saravia v. Germany*, appl. no. 54934/00, § 79.

67 CJEU 8 April 2014, C-293/12 (*Digital Rights Ireland v. Ireland*) and C-594/12 (*Seitlinger, Tschohl et al. v. Kärtner Landsregierung*), § 57-59. See also subsection 4.4.1.

is that the knowledge that a government continuously gathers information about its citizens may stifle individuals' behaviours.[68] This so-called 'chilling effect' often accompanies surveillance measures. The CJEU did not further address the interference with the freedom of expression, because it deemed doing so 'unnecessary' after its extensive analyses of art. 7 and 8 CFR.[69] However, in my view the chilling effect is indeed a factor that needs to be taken into consideration when regulating law enforcement authorities' usage of automated data collection systems.

Similar to the ECtHR, the CJEU carefully scrutinises whether the quality of the law for the regulation of investigative methods is proportionate considering the aim that is being pursued. In doing so, it notes that domestic regulations of data retention measures must impose a minimum of legislated safeguards to effectively protect personal data from both abuse and unlawful access to data by law enforcement authorities.[70] The CJEU finds that regulations must specifically consider three aspects, namely: (1) the vast quantity of data that is stored as a result of the Data retention directive, (2) the sensitive nature of that data, and (3) the risk of unlawful access to that data.[71] Interestingly, the CJEU remarks that "*the need for such safeguards is all the greater where, (…), personal data are subjected to automatic processing and where there is a significant risk of unlawful access to those data*".[72] This comment supports the view that detailed regulations should restrict the use of automated data collection systems by law enforcement officials.

5.3.3 Observation of online behaviours of individuals

An interference with the right to respect for private life takes place when law enforcement officials observe online public behaviours of individuals. The investigative method can likely be placed at the low end of the scale of gravity for privacy interferences, given that these online behaviours can be observed by anyone. However, in its case law, the ECtHR has developed the following factors for determining the gravity of the privacy interference and the quality of the law regulating it: (1) the nature, scope, and duration of the surveillance measures; (2) the grounds required for ordering them; (3) the authorities competent to permit, carry out, and supervise the measures;

68 AG Opinion to CJEU 8 April 2014, C-293/12 (*Digital Rights Ireland v. Ireland*) and C-594/12 (*Seitlinger, Tschohl et al. v. Kärtner Landsregierung*), § 53.

69 CJEU 8 April 2014, C-293/12 (*Digital Rights Ireland v. Ireland*) and C-594/12 (*Seitlinger, Tschohl et al. v. Kärtner Landsregierung*), § 70.

70 CJEU 8 April 2014, C-293/12 (*Digital Rights Ireland v. Ireland*) and C-594/12 (*Seitlinger, Tschohl et al. v. Kärtner Landsregierung*), § 54. These safeguards must be implemented in addition to the requirements of accessible and foreseeable law. The CJEU also refers to ECtHR case law, such as *S. and Marper v. The United Kingdom* and *Rotaru v. Romania*.

71 CJEU 8 April 2014, C-293/12 (*Digital Rights Ireland v. Ireland*) and C-594/12 (*Seitlinger, Tschohl et al. v. Kärtner Landsregierung*), § 66.

72 CJEU 8 April 2014, C-293/12 (*Digital Rights Ireland v. Ireland*) and C-594/12 (*Seitlinger, Tschohl et al. v. Kärtner Landsregierung*), § 55.

and (4) the kind of remedy provided by the national law for violations.[73] If contracting States of the ECtHR are to comply with these factors in their domestic legal frameworks, it appears logical that they regulate the investigative method in detail, incorporating these factors therein.[74]

Application to the Dutch legal framework

As explained in sections 5.1 and 5.2, the observation of the behaviours of individuals in public is viewed as a privacy-infringing activity in the Netherlands. However, the detailed legal basis with procedural safeguards is applicable in the DCCP only when the observation becomes systematic in nature. In my view, it is not necessary to require more stringent procedural safeguards in connection with systematic online observation (as opposed to systematic offline observation), such as the involvement of an investigative judge. The current requirement for a public prosecutor's order for the systematic observation of online behaviours of individuals is appropriate.

If the factors that the ECtHR already considers when it determines the gravity of a privacy interference and the quality of the law are taken into account, a detailed legal basis in statutory law appears appropriate for both the non-systematic and systematic application of this investigative method. The details concerning how individuals are observed in an online context could be regulated in a guideline for the Public Prosecution Service. The need for a guideline that explains in more concrete terms when the special investigative power to systematically observe individuals' (online) behaviours will be required is clear. The most recent study (2004) regarding the application of this investigative method concluded that it is unclear for law enforcement officials when the application of the special investigative power for systematic observation is required for this method even in the physical world (see Beijer et al. 2004, p. 36 and 59). With a lack of case law and direction in guidelines for law enforcement officials, I do not expect the *online* application of the investigative method to be any clearer in practice.

5.3.4 Section conclusion

The results of the analysis in subsections 5.3.1 to 5.3.3 with regard to the adequacy of the quality of the law of the Dutch legal framework conducted presented below.

The manual gathering of publicly available online information by law enforcement authorities is considered a privacy-infringing activity in the Netherlands. The Dutch regulations *meet the desired quality of the law*, since the investigative method is restricted by data protection regulations. However, Dutch law enforcement authorities must exert more effort to ensure

73 The 'kind of remedy' refers to a remedy for procedural defects in the investigation by law enforcement authorities. This criterion does not relate to art. 8 ECHR or the regulation of the investigative method itself and is therefore not further considered.

74 See subsection 4.1.2 under C and subsection 4.1.3 under C.

that data protection regulations effectively restrict evidence-gathering activities. At the moment, law enforcement authorities do not sufficiently apply these regulations.

The automated gathering of publicly available online information is not regulated in detail in the Netherlands. Case law of both the ECtHR and CJEU indicates that each court will carefully compare the need to collect information with the aim that is being pursued by gathering the data. The result of that comparison must be reflected in detailed regulations that concretely interpret requirements arising from data protection regulations. The Dutch Police Files Act is not tailored to this investigative method. As a result, the legal basis for the automated gathering of publicly available online information *does not meet the desired quality of the law* requirements

The observation of the online behaviours of individuals is considered a privacy-infringing activity in the Netherlands. A detailed provision in criminal procedural law, with the specific procedural safeguard of an order being required from a public prosecutor is only applicable when the investigative method is applied systematically. The Dutch legal framework with regard to the investigative method of the observation of the online behaviours *does not meet the desired quality of the law* requirements, due to ambiguity with regard to the question of when (online) observation as an investigative method becomes systematic in nature. A guideline should more concretely detail when a special investigative power is required for such observation.

5.4 Improving the legal framework

This section discusses how the DCCP can be improved in order to provide an adequate legal framework for the regulation of the investigative method of gathering publicly available online information. A legal framework is considered adequate when (1) it is accessible, (2) it is foreseeable, and (3) the desired quality of the law requirements are met. The results of the analysis regarding these normative requirements are summarised in Table 5.1.

Normative requirement	**Manual gathering of publicly available online information**	**Automated gathering of publicly available online information**	**Observing the online behaviours of individuals**
Accessible	✓	✓	✓
Foreseeable	✗	✗	✗
Meets the desirable quality of the law	✓	✗	✗

Table 5.1: Representation of the research results from sections 5.1 to 5.3 (✓ = adequate, ✗ = not adequate).

These research results are the basis for making suggestions for improving how the Dutch legal framework regulates each category of gathering publicly available online information. The improvements related to each investigative method are presented in the following subsections.

5.4.1 Manual gathering of publicly available online information

The Dutch legal framework for the manual gathering of publicly available online information is not considered foreseeable, due to its ambiguity with regard to how data protection regulations must be interpreted concretely in the context of the investigative method. In addition, the Dutch legislature has previously made a confusing statement that a special investigative power is required for the systematic information gathering of online information.[75]

Taking the desired quality of the law for this investigative method into account, I argued above that the general legal basis in art. 3 of the Dutch Police Act may suffice for the investigative method, in combination with data protection regulations. However, the data protection regulations themselves are not taken into sufficient consideration by Dutch law enforcement authorities and need to be applied more concretely.

In order to improve the investigative method's foreseeability and the quality of the law, it is recommended to create a guideline for the manual gathering of publicly available online information (*Recommendation 1*).[76] Dutch law enforcement officials can and should be provided with more guidance from the Dutch legislator or Public Prosecution Service with regard to the question as to how the manual gathering of publicly online information should be restricted. The guideline for 'internet investigations' prepared by municipal investigators can be used as an example in this regard.[77] Most notably, this guideline requires investigators to (1) consider whether it is necessary to look for information about the individual online and perform a proportionality test in relation to the crime at hand, (2)

75 In 2014, the Dutch Ministry of Security and Justice proposed a new special investigative power that allows law enforcement officials to 'systematically download online data' in criminal investigations of every crime, insofar as a legal order is obtained from a public prosecutor. See the discussion document regarding special investigative powers (6 June 2014), p. 59-60. Available at: https://www.rijksoverheid.nl/documenten/publicaties/2014/06/06/herziening-van-het-wetboek-van-strafvordering. However, in his letter of 30 September 2015 on the modernisation of the DCCP, the Dutch Minister of Security and Justice suddenly stated that the Dutch national police no longer desired a new special investigative power for the 'systematic collection of personal data from the Internet'. See the letter of 30 September 2015 regarding the modernisation of the DCCP, p. 88. Available at: https://www.rijksoverheid.nl/documenten/kamerstukken/2015/09/30/brief-aan-de-tweede-kamer-modernisering-wetboek-van-strafvordering-plus-contourennota (last visited on 3 May 2016). Since then, no legislative initiatives have been made to improve Dutch legislation regarding the gathering of publicly available online information.

76 Alternatively, the existing Guideline for Special investigative Powers can be amended to incorporate the investigative method.

77 See 'Protocol internetonderzoek door gemeenten'. Available at: https://cbpweb.nl/sites/default/files/atoms/files/protocol_internetonderzoek_door_gemeenten.pdf. The Dutch Data Protection Authority found the guideline appropriate in light of data protection regulations. See 'Besluit internetonderzoek door gemeenten', 17 April 2015. Available at: https://cbpweb.nl/nl/nieuws/besluit-internetonderzoek-door-gemeenten (last visited on 17 September 2015).

develop a search strategy – and thereby a basis for the police report – that includes which combination of key words and online sources they will use in their investigation, and (3) provide a police report that states the results of their online investigation. The guideline also restricts the investigative method in a concrete manner by posing a time limit on the gathering of publicly available information, after which law enforcement officials must obtain authorisation from a higher-ranking law enforcement official if they feel it is necessary to continue their search.

5.4.2 Automated gathering of publicly available online information

The legal basis for applying the automated gathering of publicly available online information is not 'in accordance with the law', since the normative requirements of foreseeability and the quality of the law requirements are not met. Detailed regulations should restrict this privacy-intrusive investigative method and protect the individuals involved. Case law of both the ECtHR and CJEU requires that States carefully test the necessity to collect information and the aim that is pursued by gathering that data.

The result of this test should be reflected in detailed regulations that minimise the risk that the data will be abused or unlawfully accessed and used. The Police Files Act is not tailored to this investigative method. The creation of detailed regulations in statutory law would force the Dutch legislature to think about the necessity and conditions for using automated data collection systems. These bodies should also engage in a broader debate about the use of commercial online data collection services by law enforcement authorities.

The detailed regulations themselves may be comparable to legislation that is already in place for CCTV camera surveillance in public places (*Recommendation 2*). It is likely that automated information-gathering systems will be used for public order purposes, as well as for gathering evidence in criminal investigations. The detailed regulations should at least specify (1) for which purposes and which crimes automated data collection systems can be utilised, (2) the retention period for the data, (3) the organisational and technical security measures for securing information, (4) which organisations individuals should approach should they wish to invoke their right to access and correct data, and (5) which remedies are available to the individuals involved when errors occur.

5.4.3 Observation of online behaviours of individuals

In the Netherlands, the observation of the online behaviours of individuals is based on either (1) the statutory duty of the law enforcement officials and public prosecutors to investigate crimes or (2) the special investigative power for systematic observation. However, it is currently unclear when the observation of individuals becomes 'systematic' in nature and hence when the special investigative power for systematic observation is required

as a legal basis. The factors with the accompanying explanation provided in legislative history in 1999, appear to be outdated. Whether the use of the special investigative power for systematic observation is appropriate is currently left to the discretion of law enforcement officials, who hopefully consult with public prosecutors (cf. Oerlemans & Koops 2012, p. 46). More clarity about the application of the investigative method is required for both law enforcement officials and the individuals involved.

The Dutch legislator or Public Prosecution Service should create more detailed regulations in a guideline that specifies under which conditions this investigative method can be applied (*Recommendation 3*). This guideline could interpret the factors provided in legislative history in an online context and thus indicate more concretely when the application of the special investigative power for systematic observation is appropriate. The Dutch legislator can also consider amending the special investigative power for systematic observation and specifying a time limit that defines when observation becomes systematic in nature. However, a downside of such a condition would be that a time limit does not consider the fact that this investigative method can be intrusive to the individuals involved when their online behaviours are observed from multiple sources or in particularly sensitive online contexts.

5.5 Chapter conclusion

The aim of this chapter was to determine how Dutch criminal procedural law should be improved to adequately regulate the investigative method of gathering publicly available online information (RQ 4a). To answer the research question, the Dutch legal framework regulating all three categories of the investigative method was investigated with regard to (1) accessibility, (2) foreseeability, and (3) the quality of the law.

In this study, the gathering of publicly available online information is subdivided into (1) the manual gathering of publicly available online information, (2) the automated gathering of publicly available online information, and (3) the observation of online behaviours. Law enforcement authorities have traditionally viewed the gathering of information from these 'open sources' as investigative methods that do not require detailed regulation in the form of 'special investigative powers' in criminal procedural law. However, a much larger amount of more diverse information is now publicly available on the Internet. The analysis in subsection 4.1.3 has shown that this investigative method – and especially the use of technologically advanced systems to collect and process personal data – should be subject to detailed regulations.

Subsection 5.5.1 summarises the results of the adequacy of the Dutch regulations for the investigative method in terms of the three normative requirements. The corresponding recommendations are presented in subsection 5.5.2.

5.5.1 Summary of conclusions

In section 5.1, an analysis regarding the accessibility of the legal basis for the investigative method was conducted. That analysis showed that Dutch law provides an adequate indication of the applicable regulations for the manual gathering of publicly available online information, the automated gathering of publicly available online information, and the observation of online behaviours.

The analysis in section 5.2 showed that none of the categories of gathering publicly available online information is regulated in a foreseeable manner in Dutch law. Data protection principles restrict the manual and automated gathering of publicly available online information. However, the way in which these data protection regulations restrict these particular investigative methods is unclear. In addition, the examples mentioned in legislative history, which includes the explanatory memorandum to the Computer Crime Act II of 1999, appear outdated. Today a larger amount of more diverse information about individuals is publicly available on the Internet. The Dutch legislature or Public Prosecution Service should indicate the scope of the manual gathering of publicly available online information more clearly in statutory law or guidelines. In addition, the Dutch legislature or Public Prosecution Service should explain how the factors provided in legislative history to determine when the investigative method observation becomes systematic in nature, apply in an online context and if necessary, design new determining factors tailor made for the online context. Finally, the Dutch legislature should discuss the desirability of automated data collection systems that are used to gather publicly available online information for law enforcement purposes. The scope of this investigative method and the manner in which it is used should be restricted in detailed regulations in statutory law.

The analysis in section 5.3 showed that only the manual gathering of publicly available online information meets the desired quality of the law. However, in the context of this method, Dutch law enforcement authorities must exert more effort to ensure that data protection regulations effectively restrict evidence-gathering activities. The current situation is that law enforcement authorities do not sufficiently apply these regulations. In order to meet the desired quality of the law for the automated gathering of publicly available online information, detailed regulations that reflect requirements from data protection regulations must be created. The observation of the online behaviours of individuals does not meet the desired quality of the law, due to ambiguity with regard to when (online) observation as an investigative method becomes systematic in nature. A guideline should detail more concretely when the special investigative power is required for observing the online behaviours of individuals. This reflection is continued in subsection 5.5.2.

5.5.2 Recommendations

Section 5.4 provided three recommendations to improve the Dutch legal framework for the gathering of publicly available online information as an investigative method. These recommendations followed the analysis of the adequacy of the Dutch legal framework based on the three normative requirements in section 5.1 to 5.3. The recommendations are as follows.

1. The Dutch legislator or Dutch Public Prosecution Service should create a guideline for the manual gathering of publicly available online information. This guideline can specify the scope of the investigative method, explain the manner in which the method should be applied in practice, and restrict the investigative method by specifying how the data protection regulations should be concretely fulfilled.
2. The Dutch legislator should create detailed regulations (statutory law) for the use of the automated gathering of publicly available online information as an investigative method that are comparable to the existing regulations for using CCTV cameras. These detailed regulations should also specify how data protection regulations should be concretely fulfilled.
3. The Dutch legislator or Public Prosecution Service should create more detailed regulations for the observation of online behaviours of individuals. A guideline could specify more explicitly under which conditions this investigative method can be applied and when the application should be considered systematic.