Investigating cybercrime

Oerlemans, J.J.

4 The right to privacy and digital investigative methods

This chapter aims to answer the third research question (RQ 3): *Which quality of law is desirable for the identified digital investigative methods?* The chapter is concerned with correctly identifying the interference with the right to privacy that takes place when the identified digital investigative methods are applied. Based on that interference, the desirable quality of law is formulated. Three steps are taken to answer RQ 3.

In the first step, ECtHR case law regarding investigative methods that are most similar to the identified digital investigative methods is analysed. As no specific case law is available with regard to the identified digital investigative methods, the case law of similar investigative methods is analysed to determine which type of regulations are required. The point of departure is that the basic structures of both digital investigative methods and their non-digital counterparts are comparable and that requirements for digital methods can be extrapolated from existing case law concerning non-digital methods. In accordance with that point of departure, the existing regulations for non-digital methods in Dutch law, which will be examined in the following chapters, can potentially provide a basis for regulating digital investigative methods. The aim is to determine whether Dutch law requires any amendments or additions to existing regulations, because of differences between digital and non-digital variants, which may bring with them that the existing bases are not adequate as they stand for digital variants.

In the second step, the gravity of the privacy interferences involved in the application of the distinct digital investigative methods is analysed. It is then determined whether the quality of the law that is required for counterpart non-digital investigative methods also 'fits' the digital investigative methods. Bearing in mind the restriction set forth in section 1.3, it should be recalled that this study does not examine desirable regulations for datamining techniques. However, the further processing of personal data once it is stored in police systems is taken into consideration, because they can influence both the gravity of the privacy interference and the appropriate quality of the law for the identified digital investigative methods. The scale of gravity for privacy interferences as presented in subsection 3.2.4 will be used to position the digital investigative methods accordingly. As explained in chapter 3, the ECtHR prescribes the detail of law and procedural safeguards for regulating the investigative methods, depending on the gravity of the privacy interference that takes place. The identified digital investigative methods interfere with the right to privacy in their own manner and should be placed at a specific point on the scale of gravity for privacy interferences to determine which quality of the law is appropriate.

In the third step, detected misalignments in the appreciation of the gravity of the privacy interference and quality of the law requirements derived from case law concerning counterpart investigative methods and that of privacy interferences caused by digital investigative methods are analysed to determine whether a different level of detail in regulations and different safeguards are desirable for the identified digital investigative methods. In the conclusion of the chapter, a table is provided that indicates which level of detail for regulations and procedural safeguards are desirable for the identified digital investigative methods. The results of this analysis provide the basis for determining (in chapters 5 to 8) whether the Dutch approach to regulating digital investigative methods is correct and meets the identified desired quality of the law for the investigative methods.

The structure of this chapter is based on the four investigative methods, each of which is examined in its own section. The structure is thus as follows: section 4.1 examines the gathering of publicly available online information; section 4.2 analyses the data production orders that are issued to online service providers; section 4.3 explores online undercover investigative methods; and section 4.4 examines hacking as an investigative method. Finally, section 4.5 presents a summary of the findings of the chapter.

4.1 Gathering publicly available online information

This section analyses the gravity of the privacy interferences that take place when law enforcement officials gather publicly available online information. Previously, the gathering publically available information in the course of criminal investigations was not a real issue, since the information-gathering capabilities of law enforcement authorities were limited to certain sources. However, the proliferation of publically available information online and the development of modern technologies that enable law enforcement authorities to gather and process large quantities of data have given rise to more intrusive privacy interferences (see WRR 2016).

ECtHR case law regarding counterpart investigative methods in this regard is examined in subsection 4.1.1. In subsection 4.1.2, the digital equivalents of these investigative methods are further analysed in their relation to the right to privacy. Subsection 4.1.3 then concludes the section by determining which quality of the law is *desirable* for the gathering of publicly available online information.

4.1.1 The right to privacy regarding similar investigative methods

The following subset of the digital investigative method was distinguished in chapter 2: (A) the manual gathering of publicly available online information, (B) the automated gathering of publicly available online information, and (C) observing the online behaviours of individuals. This subsection

examines case law with regard to similar investigative methods as compared to the gathering of publicly available online information.

The following investigative methods are considered similar to their digital counterparts: (A) the gathering of information from open sources, (B) the pre-emptive storage of personal information for law enforcement purposes, and (C) the visual surveillance of the behaviours of individuals in the physical world.

A The gathering of information from open sources

Open source information can be defined as information that anyone can lawfully obtain by request, purchase, or observation (cf. Eijkman & Weggemans 2012, p. 287).[1] An important case that reflects the privacy interference that takes place when open source information is gathered by law enforcement officials is the 2006 case of *Segerstedt-Wiberg and Others v. Sweden* (henceforth *Segerstedt-Wiberg*).[2] In this case, the Swedish Security Police collected information about individuals by (a) observing these individuals' public activities, (b) amassing newspaper articles about them, and (c) gathering public decisions taken about them by public authorities. The individuals involved complained to the ECtHR that storing this information in the Security Police files constituted an unjustified interference with their right to respect for private life.[3] The Swedish government contended that the information was publicly available and therefore questioned whether the information that was stored interfered with the right to respect for private life as protected under art. 8(1) ECHR.[4]

In the case of *Segerstedt-Wiberg*, the ECtHR decided that the storage of public information in the Security Police register and release of that information constituted an interference in the private lives of the individuals involved. The ECtHR emphasised that the fact that the data was public did not negate the interference, "*since the information had been systematically collected and stored in files held by the authorities.*"[5] The ECtHR also decided in other cases that "*public information can fall within the scope of private life where it is systematically collected and stored in files held by the authorities*".[6]

1 Eijkman & Weggemans refer to the National Open Source Enterprise, Intelligence Community Directive 301 of July 2006 for this definition.

2 ECtHR 6 June 2006, *Segerstedt-Wiberg and others v. Sweden*, appl. no. 62332/00.

3 ECtHR 6 June 2006, *Segerstedt-Wiberg and others v. Sweden*, appl. no. 62332/00, § 70.

4 ECtHR 6 June 2006, *Segerstedt-Wiberg and others v. Sweden*, appl. no. 62332/00, § 71.

5 ECtHR 6 June 2006, *Segerstedt-Wiberg and others v. Sweden*, appl. no. 62332/00, § 72.

6 See ECtHR 6 June 2006, *Segerstedt-Wiberg and others v. Sweden*, appl. no. 62332/00, § 72 with reference to ECtHR 4 May 2000, *Rotaru v. Romania*, appl. no. 28341/95, § 43. See also the case law with regard to the storage of information in police systems that does not concern public information: ECHR 26 March 1987, *Leander v. Sweden*, appl. no. 9248/81, § 48, ECtHR 4 May 2000, ECtHR 13 November 2012, *M.M. v. The United Kingdom*, appl. no. 24029/07, § 87 and ECtHR 17 December 2009, *Gardel v. France*, appl. no. 16428/05, § 58.

The ECtHR thus particularly test whether the information is (1) *systematically gathered* and (2) *stored in a police system* to determine whether an interference took place with the right to respect to private life. This test is also visible in other case law. For instance, the ECtHR found that no interference with the right to respect for private life takes place when law enforcement officials take pictures of an individual during a public demonstration, without storing that information in a police system (cf. De Hert 2005, p. 75).[7] The ECtHR clearly takes an individual's 'reasonable expectation of privacy' into consideration in its case law concerning the surveillance of individuals in their public lives.[8] The court has repeatedly stated in case law that *"a person who walks down the street will, inevitably, be visible to any member of the public who is also present"*.[9] The member of the public who is observing others can apparently also be a law enforcement officer. The fact that law enforcement officers use technological means, such as CCTV cameras, to monitor activities in a public scene does not make a difference, according to the ECtHR.[10]

When the information obtained from a public scene is *stored* in a police system, an interference with the involved individual's right to respect for private life takes place.[11] Case law of the ECtHR regarding the processing of stored recordings from CCTV images indicates that every step in the further processing of personal information once it is stored in police systems amounts to a more serious interference with the right to privacy (see Ölçer 2008, p. 284 and p. 292).[12] For example, in the case of *Peck v. The United Kingdom*, an individual who was 'in a state of distress' and wielding a knife was filmed by a CCTV camera.[13] These behaviours were filmed by a CCTV camera. Law enforcement officials then released to footage to a television

7 Citing ECommHR, *Pierre Herbecq and the Association Ligue des droits de L'homme v. Belgium*, Decision of 14 January 1998 on the applicability of the applications no. 32200/96 and 32201/96 (joined), Decisions and Reports, 1999, p. 93-98 in which the Commission finds that no privacy interference takes place when photographic equipment is used that does not record the visual data. See also ECtHR 31 January 1995, *Friedl v. Austria*, § 51-52.

8 ECtHR 25 September 2001, *P.G. and J.H. v. The United Kingdom*, appl. no. 44787/98, § 57. See also ECtHR 17 July 2003, *Perry v. The United Kingdom*, appl. no. 63737/00, § 38.

9 Idem.

10 ECtHR 25 September 2001, *P.G. and J.H. v. The United Kingdom*, appl. no. 44787/98, § 57. See also ECtHR 17 July 2003, *Perry v. The United Kingdom*, appl. no. 63737/00, § 38.

11 See, e.g., ECtHR 18 February 2000, *Amann v. Switzerland*, appl. no. 27798/95, § 65, ECtHR 4 May 2000, *Rotaru v. Romania*, appl. no. 28341/95, § 43, ECtHR 25 September 2001, *P.G. and J.H. v. The United Kingdom*, appl. no. 44787/98, § 59-60, ECtHR 28 January 2003, *Peck v. The United Kingdom*, no. 44647/98, § 62-63, ECtHR 17 July 2003, *Perry v. The United Kingdom*, appl. no. 63737/00, § 38 and 40-41, and ECtHR 17 December 2009, *Gardel v. France*, appl. no. 16428/05, § 62.

12 See also ECtHR 2 September 2010, *Uzun v. Germany*, appl. no. 35623/05, § 45: *"Further elements which the Court has taken into account in this respect include the question whether there has been compilation of data on a particular individual, whether there has been processing or use of personal data or whether there has been publication of the material concerned in a manner or degree beyond that normally foreseeable."*

13 See ECtHR 28 January 2003, *Peck v. The United Kingdom*, no. 44647/98, § 62.

show without informing and anonymising the individual involved.[14] It turned out the individual was contemplating to commit suicide. The ECtHR found that, in this case, the processing of personal information took place in a manner that could not be foreseen by the individual involved, which gave rise to a serious interference in his right to privacy.[15]

Required quality of the law

When deciding whether the storage of personal data obtained from public places amounts to an interference with the right to privacy, the ECtHR often refers to the Council of Europe's convention for the protection of individuals with regard to the automatic processing of personal data to discuss the required quality of the law.[16] Data protection regulations restrict the systematic collection and storage of personal information in police systems and can be considered as a framework representing the ECtHR's required quality of the law.

For instance, in the case of *Rotaru v. Romania*, the ECtHR specifically considered which restrictions were available in the domestic legislation of Romania with regard to the systematic collection and storage of personal data by law enforcement officials.[17] The court reviewed (1) which provisions were available concerning the individuals who were authorised to consult the stored files containing personal data and (2) whether provisions were available concerning the retention period of these files.[18] These restrictions were based on data protection regulations and can be considered as the required quality of the law for the gathering of personal data from open sources.

Storage of personal data v. processing of personal data

The difficulty with the case law of the ECtHR regarding the systematic gathering of information from open sources is that the ECtHR does not make a clear distinction between (a) the *storage of personal information* in police systems and (b) the *processing of personal information* by law enforcement officials (cf. De Hert 2005, p. 75). Since the storage of data in a police system is an interference, the question arises whether merely processing personal information taken from public sources (without storing it in a police file)

14 ECtHR 28 January 2003, *Peck v. The United Kingdom*, no. 44647/98, § 62.

15 See ECtHR 28 January 2003, *Peck v. The United Kingdom*, no. 44647/98, § 62-63.

16 Treaty of 28 January 1981, CETS no.108. See, e.g., ECtHR 18 February 2000, *Amann v. Switzerland*, appl. no. 27798/95, § 65, ECtHR 4 May 2000, *Rotaru v. Romania*, appl. no. 28341/95, § 43, ECtHR 25 September 2001, *P.G. and J.H. v. The United Kingdom*, appl. no. 44787/98, § 57 and ECtHR 17 December 2009, *Gardel v. France*, appl. no. 16428/05, § 27.

17 ECtHR 4 May 2000, *Rotaru v. Romania*, appl. no. 28341/95, § 43: "*Moreover, public information can fall within the scope of private life where it is systematically collected and stored in files held by the authorities*".

18 ECtHR 4 May 2000, *Rotaru v. Romania*, appl. no. 28341/95, § 57.

amounts to an interference with the right to private life. An example of this situation is when a law enforcement official takes a picture of an individual in a public place without storing the information in a police system. As explained above, it is likely the court will reason this surveillance measure is both not applied systematically and information is not stored in a police system. In that situation, no interference takes place with art. 8(1) ECHR.

However, data protection regulations within the European Union already apply when personal information is *merely processed* by law enforcement officials.[19] The application of these regulations do not require (1) the systematic collection and (2) the storage of personal information in a police system. For example, when law enforcement officials manually gather online information about a suspect by use of Google based on the suspect's name, data protection regulations apply. For instance, the investigative activity can only take place with a legitimate aim (such as gathering evidence in a criminal investigation). This means that data protection regulations apply earlier for many law enforcement authorities, i.e., all law enforcement authorities in the EU, than the ECtHR acknowledges. De Hert (2005) presents a more detailed discussion on this topic. It is important to realise that EU data protection regulations provide more protection to the individuals involved, because the threshold to apply these EU data protection regulations are lower than the one required by the ECtHR. This is illustrated in Figure 4.1, which is an adaptation of the scale of gravity for privacy interference and the required quality of the law in Figure 3.1.

19 See the Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23/11/1995 P. 0031 – 0050 and its proposed successor the Proposal for a regulation on the protection of individuals with regard to the processing of personal data and the free movement of such data (General Data Protection Regulation), 25 January 2012, COM(2012) 11 final 2012/001 (COD). See also with regard to data protection regulations for law enforcement authorities within the European Union: the proposal on the on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, COM(2012) 010 final 2012/0010 (COD).

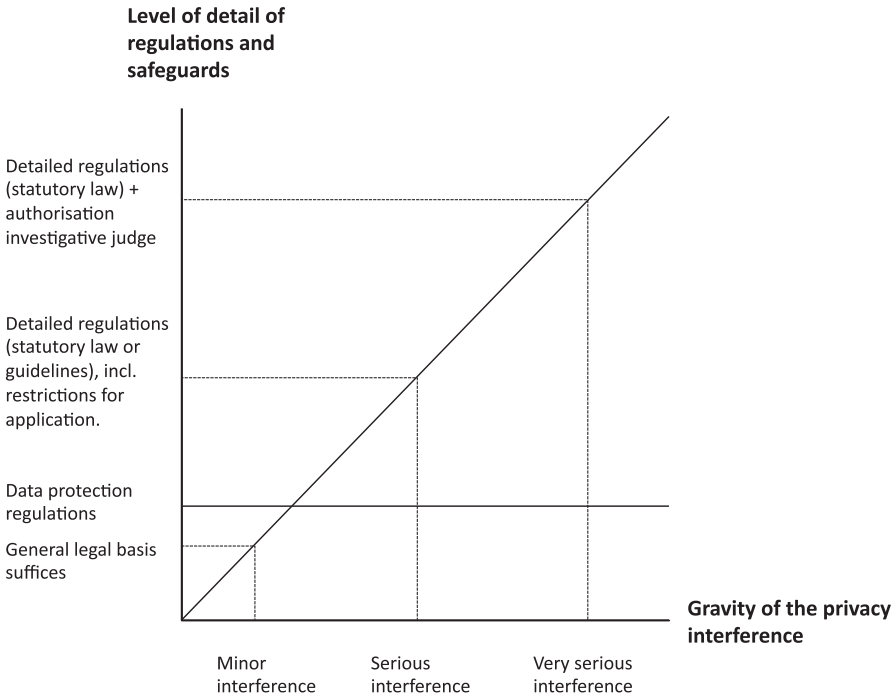

Figure 4.1: Scale of gravity for privacy interferences with accompanying quality of the law and data protection regulations.

Figure 4.1 illustrates how data protection regulations present a baseline for the quality of the law for the regulation of investigative methods that involve the processing of personal data. Data protection regulations can thereby restrict the application of investigative methods, even when even when the investigative method itself does not interfere with the right to privacy in a serious manner by art. 8 ECHR standards.

B The pre-emptive storage of personal information

In 2008, the ECtHR dealt with the legitimacy of the pre-emptive storage of personal information for law enforcement purposes in its case law.[20] The case of *S. and Marper v. The United Kingdom* is further below examined in order to determine the gravity of the privacy interference that takes place when information is pre-emptively stored in police systems. The quality of the law that the ECtHR finds appropriate for such an investigative method is also examined. The investigative method can be distinguished from open source information gathering under A, by the fact that this investigative

20 See ECtHR 4 December 2008, *S. and Marper v. The United Kingdom*, appl. nos. 30562/04 and 30566/04.

method regards to use of a database by law enforcement officials based on personal information that has been previously obtained and stored for later use for law enforcement purposes.

In the case of *S. and Marper v. The United Kingdom*, the pre-emptive storage of personal information in a police system concerned fingerprints and DNA materials that were taken from individuals following their arrest in the United Kingdom. These items were stored in a police system, which meant they could be used later in time for law enforcement purposes. When the applicants requested that the materials be deleted from the database, the government in the United Kingdom refused to do so. The case was eventually brought to the ECtHR.

To decide whether the storage of the data interfered with the applicants' right to privacy, the ECtHR took the following four factors into consideration: (1) the specific context in which the information at issue had been recorded and retained, (2) the nature of the records, (3) the way in which these records were used and processed, and (4) the results that could be obtained with the storage of the information.[21]

In its decision, the ECtHR determined that DNA materials should be seen as sensitive information, because they include details concerning an individual's health. In addition, DNA profiles derived from those materials provide a means for identifying genetic relationships between individuals as sensitive information. For these two reasons, the storage of the DNA materials was found to be an interference with the right to respect for private life as articulated as an object of protection in art. 8 ECHR.[22] With regard to the storage of fingerprints, the ECtHR concluded that the information is less sensitive than DNA materials. However, the fingerprints that were taken in criminal proceedings were permanently stored in a police database and regularly processed by automated means for criminal identification purposes, which amounted to an interference with art. 8(1) ECHR.[23]

Required quality of the law

With regard to the quality of the law, the ECtHR requires specific safeguards in the domestic legal frameworks of contracting States in order to avoid governmental abuse of the pre-emptive storage of sensitive materials. In *S. and Marper v. The United Kingdom*, the ECtHR required that (1) no more data is gathered than necessary for the investigation of specific crimes, (2) a specific

21 ECtHR 4 December 2008, *S. and Marper v. The United Kingdom*, appl. nos. 30562/04 and 30566/04, § 67.

22 ECtHR 4 December 2008, *S. and Marper v. The United Kingdom*, appl. nos. 30562/04 and 30566/04, § 72-75. The ECtHR also considered the storage of fingerprints – in connection with an identified or identifiable individual – in a police system as an interference with regard to the right to respect for private life. See ECtHR 18 April 2013, *M.K. v. France*, appl. no. 19522/09, § 32.

23 ECtHR 4 December 2008, *S. and Marper v. The United Kingdom*, appl. nos. 30562/04 and 30566/04, § 86.

retention period for the storage of personal data is in place (which is differentiated based on the seriousness of the offence), and (3) the involved individuals have the possibility to access and request deletion of the stored records.[24] It is noteworthy that these requirements are similar to those that generally apply to data protection regulations.[25]

An important consideration in the case of *S. and Marper v. The United Kingdom* is that the ECtHR emphasised that the *indiscriminate* pre-emptive storage of personal information also encompasses the collection of personal information from individuals who are not suspected of crime. This is deemed problematic by the ECtHR, because individuals who are not suspects must be presumed innocent and should not be subjected to governmental interferences in their private lives.[26] For that reason, the ECtHR carefully scrutinises the pre-emptive collection of sensitive information for law enforcement purposes in light art. 8 ECHR to decide whether the storage of information is proportionate considering the law enforcement aim (the prevention of disorder can crime) that is pursued.[27]

C Visual surveillance of the behaviours of individuals in the physical world

The case of *Segerstedt-Wiberg* is also relevant for the visual surveillance of individuals by law enforcement officials in the physical world; given that the information that can be obtained by observation in a public context is also considered as "open source information" (cf. Eijkman & Weggemans 2012, p. 287).[28] Other case law of the ECtHR concerning the surveillance of individuals in public places is also relevant.[29] Essentially, the ECtHR has made it clear in these cases that individuals who knowingly expose themselves to any other member of the public who can take notice of their behaviours in public are not necessarily protected by the right to respect for private life as meant in art. 8(1) ECHR.

24 ECtHR 4 December 2008, *S. and Marper v. The United Kingdom*, appl. nos. 30562/04 and 30566/04, § 103.

25 See, e.g., the Directive 95/46/EC of 24 October 1995 and the Proposal for a regulation on the protection of individuals with regard to the processing of personal data and the free movement of such data (General Data Protection Regulation), 25 January 2012, COM(2012) 11 final 2012/001 (COD).

26 ECtHR 4 December 2008, *S. and Marper v. The United Kingdom*, App. nos. 30562/04 and 30566/04, § 122. See also ECtHR 18 April 2013, *M.K. v. France*, appl. no. 19522/09, § 39.

27 ECtHR 4 December 2008, *S. and Marper v. The United Kingdom*, appl. nos. 30562/04 and 30566/04, § 99. See also ECtHR 18 April 2013, *M.K. v. France*, appl. no. 19522/09, § 28.

28 Eijkman & Weggemans refer to the National Open Source Enterprise, Intelligence Community Directive 301 of July 2006 for this definition.

29 ECtHR 25 September 2001, *P.G. and J.H. v. The United Kingdom*, appl. no. 44787/98, § 57. See also ECtHR 17 July 2003, *Perry v. The United Kingdom*, appl. no. 63737/00, § 38.

However, the ECtHR has also clarified in these cases that the right to private life in art. 8(1) ECHR provides for *"a zone of interaction of a person with others, even in a public context"*.[30] The background of this aspect of the right to privacy is that individuals must be able to engage in relationships with others – even in public – without arbitrary governmental interferences.[31] This statement seems to contradict the previous statement that no interference with the right to privacy takes place when information is obtained from a public place by the use of visual surveillance measures.

Nonetheless, here again the ECtHR considers it important that the information that is obtained from visual surveillance is also *stored in police systems* in order to speak of an interference with the right to respect for private life taking place.[32] The further processing of that information amounts to a more serious privacy infringement.[33]

Required quality of the law

With regard to the observation of an individual's movements in public, ECtHR case law has not required that specific procedural safeguards must be implemented in the domestic legal frameworks of contracting States. A general legal basis for using the investigative method may therefore suffice.

For instance, in the context of the use of GPS surveillance to monitor the movements of an individual and his accomplice in a car, the ECtHR found in the case of *Uzun v. Germany* that a general legal basis and authorisation by law enforcement officials to apply the investigative method were sufficient. Although the duration of the surveillance measure was not concretely restricted by statutory law, the proportionality principle that was applied by law enforcement officials ensured that this duration was sufficiently restricted.[34] However, when deciding on the legitimacy of the investigative method, the ECtHR did specifically take into consideration (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; and (4) the kind of remedy provided by the national

30 ECtHR 25 September 2001, *P.G. and J.H. v. The United Kingdom*, appl. no. 44787/98, § 56. See also e.g., ECtHR 17 July 2003, *Perry v. The United Kingdom*, appl. no. 63737/00, § 36, ECtHR 2 September 2010, *Uzun v. Germany*, appl. no. 35623/05, § 43, and ECtHR 21 June 2011, *Shimovolos v. Russia*, appl. no. 30194/09, § 64.

31 See, e.g., ECtHR 12 January 2010, *Gillian and Quinton v. The United Kingdom*, appl. no. 4158/05, § 61 and ECtHR 2 September 2010, *Uzun v. Germany*, appl. no. 35623/05, § 44.

32 See, e.g., ECtHR 25 September 2001, *P.G. and J.H. v. The United Kingdom*, appl. no. 44787/98, § 57. See also ECtHR 17 July 2003, *Perry v. The United Kingdom*, appl. no. 63737/00, § 38.

33 See, e.g., ECtHR 2 September 2010, *Uzun v. Germany*, appl. no. 35623/05, § 51-53.

34 See ECtHR 2 September 2010, *Uzun v. Germany*, appl. no. 35623/05, § 69-70. The court explicitly noted that surveillance with a GPS device is distinguished from other methods of surveillance that disclose more information person's conduct, opinions or feelings (see ECtHR 2 September 2010, *Uzun v. Germany*, appl. no. 35623/05, § 52).

law.[35] The ECtHR tested whether German law enforcement authorities took these factors into consideration in *concreto*, based on the circumstances at hand. It did not require detailed regulations in statutory law or guidelines for the investigative method. Instead, a general legal basis may suffice, as long law enforcement officials consider these factors when applying the investigative method. To a large extent, the manner in which these public surveillance measures are regulated in law is thus left to the discretion of contracting States to the ECtHR.

4.1.2 The right to privacy and gathering publicly available online information

The digital investigative method is distinguished in: (A) the manual gathering of publicly available online information, (B) the automated gathering of publicly available online information, and (C) observing the online behaviours of individuals.

These three digital investigative methods are further examined to identify the gravity of the privacy interference that takes place when they are applied. It is also examined whether, based on the gravity of the privacy interference, these digital investigative methods fit the framework developed in ECtHR case law for their counterpart methods examined above.

A Manual gathering of publicly available online information

On the one hand, the investigative method of the manual gathering of publicly available online information is similar to the gathering of information from open sources that discussed in subsection 4.1.1. The similarity is that both investigative methods concern evidence-gathering activities with regard to personal information that is publically available. In its most elementary form, the manual gathering of publicly available online information takes place when a law enforcement official looks for information about an individual on the Internet by typing key words into an internet search engine, such as Google.com.[36]

On the other hand, the manual gathering of publicly available online information that takes place today is very different from the gathering of data from open sources that takes place offline. The interference with the right to privacy when the method is applied online to open sources takes place in a different context. The following three reasons are identified in relation to why the collection of publicly available information online interferes with the right to privacy in a different manner its non-digital counterpart.

35 See, e.g., ECtHR 2 September 2010, *Uzun v. Germany*, appl. no. 35623/05, § 63 and ECtHR 21 June 2011, *Shimovolos v. Russia*, appl. no. 30194/09, §68.

36 See subsection 2.2.2 under A1 for a more extensive description of the investigative method.

(1) The Internet allows law enforcement officials to collect information on a much *greater scale* than before (cf. WRR 2016, p. 40). The large amounts of information about an individual that may nowadays be available online, should be taken into consideration when determining the gravity of the privacy interference (cf. Koops 2013, p. 663). The information can also be particularly sensitive, because pictures, opinions, feelings, and political views of individuals can be gathered from publicly accessible online sources (such as web forums and social media websites).
(2) Computers and the Internet make it possible to collect information *globally* and then to *conveniently* store relevant parts of it in a police system for evidence purposes. The information gathering can take place across State borders and is not as labour-intensive as before. Furthermore, the costs associated with storing and processing information continue to decrease (cf. WRR 2016, p. 41).
(3) Computers and the Internet make it possible for law enforcement officials to *process the collected information* in order to gain better insights into the private lives of individuals. Computers can help law enforcement officials to 'interpret' collected data by making an automatic selection and visualising the gathered data (cf. Koops 2013, p. 662). For example, law enforcement officials can gain insight into an online network of individuals by examining their friendship connections on social media websites.

Gravity of the privacy interference
It has been pointed out above that the ECtHR interprets the right to privacy *dynamically* and *evolutively* according to *present-day standards*. When technological developments are taken on board, it should be concluded that the gravity of privacy interference has increased when publicly available information is gathered manually.

At the same time, a mitigating factor for the gravity of the privacy interference that the ECtHR may take into consideration is that – to a large extent – the information is often 'knowingly exposed' by the individuals involved. The ECtHR may therefore take a person's reasonable expectation of privacy into consideration when deciding on the gravity of the privacy interference that may take place when law enforcement officials collect such information.

Alignment with the existing required quality of the law
The analysis of case law related to offline gathering of publicly available information subsection 4.1.1 indicates that the ECtHR only speaks of a privacy interference when information is systematically gathered and stored in police systems. It is possible that in an online context, law enforcement officials gather information sooner in a systematic manner than in an offline context. The reason is that more information and more diverse (and possibly sensitive) information is readily available on publicly available sources. However, one can nevertheless argue that *merely processing* publicly available online information that has been manually obtained in a single internet

search in itself does not necessarily interfere with the right to privacy as meant in art. 8(1) ECHR (cf. O'Floinn & Ormerod 2011, p. 777 and Koops 2013, p. 659).

Considering the increased amounts and broader diversity of information that is available online nowadays and the development of data protection regulations in the EU however, the position of the ECtHR (based on investigative methods that were applied in an offline context) should no longer hold. It would appear to instead be more appropriate for the ECtHR to recognize the possibility that online gathering of publicly available information is intrinsically more likely to interfere with privacy in a graver manner and this gravity will fluctuate depending on the type of information at issue. The ECtHR should consider to adopt the more modern data protection regulations, which apply when information is processed by law enforcement officials. These data protection regulations restrict the evidence gathering activity even when no information is stored in a police system and seem to be sensitive to the alternate context of publicly available sources in the digital world.

B Automated gathering of publicly available online information

Automatic data collection systems pre-emptively gather information from relevant online sources every day. This automated gathering of publicly available online information is an investigative method that can aid law enforcement officials by making relevant information available to them. In addition, these automated systems can process the collected information and present the officials with more relevant results (including quick visualizations of the information).[37]

Gravity of the privacy interference

A privacy interference clearly takes place when automated data collection systems are used. The storage of information in itself interferes with the right to privacy as articulated in art. 8 ECHR.[38]

The factors developed in the case of *S. and Marper v. The United Kingdom* for DNA and fingerprints are helpful for determining the gravity of the privacy interference when automated gathering of publicly available online information is at issue. These factors, which are elaborated on in subsection 4.1.1 (under B), include: (1) the specific context in which the information at issue has been recorded and retained, (2) the nature of the records, (3) the way in which these records are used and processed, and (4) the results that may be obtained with the storage of the information.[39] In the case of

37 See subsection 2.2.2 under A2.

38 Providers of commercial data collection systems already download and further process publicly available online information every day in order to provide the best search results for their clients.

39 ECtHR 4 December 2008, *S. and Marper v. The United Kingdom*, appl. nos. 30562/04 and 30566/04, §67 and §119.

S. and Marper v. The United Kingdom, the ECtHR found that the indiscriminate collection of information about individuals is a measure that seriously interferes with the right to privacy of the individuals involved.[40] When automated data collection systems are used, an indiscriminate collection of information about individuals also takes place. Developments in technology also make it possible to obtain an intricate picture of certain aspects of the private lives of the individuals involved.

However, the gathering of publicly available online information is not nearly as sensitive as the gathering and processing of DNA materials, as was the case in *S. and Marper v. The United Kingdom*. As DNA material can reveal details concerning an individual's health and genetic relationships with others, they are considered to contain particularly sensitive information.[41] In contrast, publicly available online information need not be as sensitive as this type of information whilst individuals often knowingly expose information on the Internet by themselves. For that reason, the automated gathering of online information is possibly considered not as privacy intrusive as the system that was in place in the case of *S. and Marper v. The United Kingdom*.

Nonetheless, large amounts of information are gathered by automated data collection systems and processed to obtain detailed insights into the lives of the individuals involved. In *S. and Marper v. The United Kingdom*, the ECtHR warned that the potential benefits of the extensive use of "modern technology" for law enforcement purposes should be carefully balanced against private life interests.[42] This warning should be kept in mind when articulating the desirable quality for the law of the investigative method of automated gathering of publicly available online information. In addition, in both investigative methods information is indiscriminately pre-emptively stored in police systems for law enforcement officials, which necessitates a strict test of the quality of the law.

Alignment with the existing required quality of the law

The investigative method that concerns the non-digital collection of personal information in *S. and Marper v. The United Kingdom* and the automated gathering of publicly available online information are both intrusive, but they interfere with the right to privacy in different manners.

However, the data protection principles that were applied in the *S. and Marper v. The United Kingdom* case may essentially also be appropriate for the automated gathering of online information. In addition, given that the preemptive collection of information may involve (a large number of) a third

40 ECtHR 4 December 2008, *S. and Marper v. The United Kingdom*, appl. nos. 30562/04 and 30566/04, §120.

41 ECtHR 4 December 2008, *S. and Marper v. The United Kingdom*, appl. nos. 30562/04 and 30566/04, § 72-75.

42 See ECtHR 4 December 2008, *S. and Marper v. The United Kingdom*, appl. nos. 30562/04 and 30566/04, §112: *"The Court considers that any State claiming a pioneer role in the development of new technologies bears special responsibility for striking the right balance in this regard."*

party, about whom information is also gathered, a heightened proportionality test also appears to be appropriate here.[43] The legislative requirements for the pre-emptive collection of personal data as framed in *S. and Marper v. The United Kingdom* may therefore also be suitable for the pre-emptive collection of publicly available online information.

C Observing online behaviours of individuals

Law enforcement officials can also observe the online behaviours of individuals on publicly accessible places on the Internet. For instance, law enforcement officials can observe an individual's public posts to online platforms such as social media services, online forums, and chat services.[44] The observation concerns online behaviours that take place in real-time, not those that occurred in the past. For the gathering of information that took place in the past, the investigative method of the manual gathering of publicly available online information is applied.

Gravity of the privacy interference

The privacy interference that takes place when law enforcement officials observe an individual's online behaviour is comparable to the interference when they use visual surveillance to observe an individual's movements in public life. The ECtHR has made it clear in case law that as part of the right to privacy, individuals must be able to engage in relationships with others – even in public – without the interference of the government.[45] There is no reason to assume that this aspect of the right to privacy would not apply to the behaviours of individuals in online environments.

The factors provided by the ECtHR for determining the gravity of the privacy interference when behaviours are observed also appear suitable for an online context. These factors are as follows: (1) the nature, scope, and duration of the possible measures; (2) the grounds required for ordering the measures; (3) the authorities competent to permit, carry out, and supervise the measures; and (4) the kind of remedy provided by the national law.[46] The ECtHR does not require detailed regulations for the investigative method. A general legal basis may thus suffice, as long the factors are used in practice when law enforcement officials apply the investigative method.

43 As explained in the introduction to section 3.2, the test whether the interference is 'necessary in a democratic society' is still relevant.

44 See subsection 2.2.2 under A3.

45 See, e.g., ECtHR 12 January 2010, *Gillian and Quinton v. The United Kingdom*, appl. no. 4158/05, § 61 and ECtHR 2 September 2010, *Uzun v. Germany*, appl. no. 35623/05, § 44.

46 See ECtHR 2 September 2010, *Uzun v. Germany*, appl. no. 35623/05, § 63. These procedural safeguards are repeated in ECtHR 21 June 2011, *Shimovolos v. Russia*, appl. no. 30194/09, §68.

Alignment with the existing required quality of the law
An important difference between observing the behaviours of individuals online and observing them in the physical world is that in an online context law enforcement officials can quickly learn about public behaviours that occurred *in the past* (cf. Oerlemans & Koops 2012, p. 46). For example, they can observe statements that individuals are currently making on social media or internet forums as well as look up statements that these individuals made in the past. In that way, much more information is available to law enforcement officials compared to when, for instance, they observe the movements of an individual in the physical world.

In addition, observing the online behaviours of an individual appears more straightforward, since the investigative method can be automated and does not require the law enforcement officials to physically move from one place to another. This investigative method is thus different in nature from its counterpart in the physical world.

Nevertheless, it is still not likely that the ECtHR will regard the online observation as an intrusive investigative method that is comparable to when, for instance, the private communications of a person are secretly wiretapped.[47] The ECtHR will take the reasonable expectation of privacy of individuals into consideration when law enforcement officials gather information that is publicly available to anyone. Since the privacy interference that takes place when public behaviours are observed is not considered as particularly serious, the ECtHR is not expected to require more detailed regulations with specific procedural safeguards for the digital investigative method.

4.1.3 Desired quality of the law

This subsection determines the *desirable* quality of the law based on the gravity of the privacy interference that takes place when publicly available online information of individuals is collected in the three modalities discussed above. In general, it should be observed that much more 'open source' information is publically available on the Internet than in an offline context. The ability to collect information from individuals located anywhere in the world is also novel.

However, the privacy interference that takes place when the investigative methods discussed above are applied can generally be placed at the low end of the scale of gravity for privacy interferences. The main reason is that case law indicates that the ECtHR takes into consideration the fact that information is publicly available to anyone, including law enforcement authorities. Based on the examined case law concerning non-digital counterparts, it is not likely that the ECtHR will require detailed regulations with certain procedural safeguards for the gathering of publicly available online

47 See, e.g., ECtHR 2 September 2010, *Uzun v. Germany*, appl. no. 35623/05, §66.

information, so that more general bases may suffice. It was argued that, taking into consideration present-day standards, data protection regulations should be applicable to the processing of personal information.[48]

The desirable quality of the law depends on how the publicly available online information is gathered. The quality of the law that is in my view desirable for regulating the information-gathering methods is presented below.

A Manual gathering of publicly available online information

With regard to the manual gathering of publicly available online information, a general legal basis for applying the investigative method coupled with data protection regulations may suffice. As only a minor privacy interference takes place when this investigative method is applied, it can be placed at the left side of the scale of gravity. Therefore, a *general legal basis* suffices for the investigative method.

However, data protection regulations should already apply when personal information is *processed* by law enforcement authorities, and not just when personal information is *stored* in police systems. In its case law, the ECtHR often refers to a relatively old data protection treaty of the Council of Europe. Instead, the EU *data protection regulations* should be adopted by the ECtHR as a baseline of protection.[49] The legislation is already used by most law enforcement authorities within the EU and is applicable to the mere processing of personal information by law enforcement officials.

B Automated gathering of publicly available online information

A more serious privacy interference takes place in relation to the automated gathering of publicly available online information. The use of such a 'technically sophisticated system' and the fact that information is processed concerning individuals who are not suspected of a crime indicate that the ECtHR will at least require States to balance the privacy interests of the individuals involved with regard to the aim pursued by law enforcement authorities.

The result of that balancing test should be reflected in *detailed regulations in either statutory law or in public guidelines* issued by law enforcement authorities that restrict the automated gathering of publicly available online information. Data protection regulations can aid in creating those detailed regulations and determining adequate safeguards.

48 See also subsection 4.1.1 under A.

49 See Koops 2013, p. 662 for an extensive analysis of EU data protection regulations for law enforcement authorities with regard to the processing of publicly available online information.

C Observing online behaviours of individuals

The observation of online behaviours of individuals can likely be placed at the low end of the scale of gravity for privacy interferences, given that these behaviours can be observed by anyone. The ECtHR does not require detailed regulations in statutory law for the application of observation as an investigative method in the physical world. An important difference compared to its offline counterpart, is that during online observation, law enforcement officials can also quickly collect information regarding an individual's past behaviours. When information is collected from past behaviours, the investigative method of the manual gathering of publicly available online information is applicable. Online observation only concerns the monitoring of behaviours that start from a specific point in time.[50]

The gravity of the privacy interference that takes place when the investigative method is applied depends on the factors developed by the ECtHR in case law. The nature, scope, and duration of the investigative method will influence the gravity of the privacy interference. For example, a single observation of the online behaviours of individuals for a brief period is considered as a minor privacy interference.

With an increasing intensity of observation, the gravity of the interference and desirable quality of the law will change accordingly. Only detailed regulations for the investigative method can prescribe for law enforcement authorities to take account the factors provided above and articulate the grounds for ordering the measure and authorities that conduct the investigative method. Therefore, a *detailed legal basis in law in either statutory law or in public guidelines* is desirable for the investigative method.

4.2 Issuing data production orders to online service providers

This section analyses the gravity of the privacy interferences that take place when law enforcement officials collect information by issuing data production orders to online service providers.

Issuing a data production order to a telecommunication service provider is considered to be a similar investigative method to issuing such an order to an online service provider. Subsection 4.2.1 thus analyses case law with regard to telecommunication service providers. In subsection 4.2.2, data production orders that are issued to online service providers are further analysed in light of their interference with the right to privacy. Subsection 4.2.3 then concludes the section by determining which quality of the law is *desirable* for data production orders that are issued to online service providers.

50 See for a similar distinction CTIVD 2014, p. 9 and p. 42.

4.2.1 Privacy and data production orders issued to telecom providers

The ECtHR considers the registration and storage of the numbers dialled on a particular telephone and the time and duration of each call as an interference with the right to respect for private life and correspondence in art. 8(1) ECHR.[51]

In the case of *Malone v. The United Kingdom*, the ECtHR first noted that the records of metering information – in particular the numbers dialled on a telephone – are an integral part of communications.[52] Greer (1997, p. 12) explains that the practice of 'metering' consists of the recording of all numbers dialled from a particular telephone by the (U.K.) Post Office for U.K. law enforcement authorities. In the current study, such information is considered as 'traffic data'.

In case law, the ECtHR explicitly differentiates traffic data from content data. For instance, in the case of *P.G. and J.H. v. The United Kingdom*, the ECtHR noted that the data production orders issued to a telecommunication provider were strictly limited to numbers dialled from the suspect's flat between two specific dates.[53] The contents of communications can be understood as data with regard to the meaning or message conveyed by the communication, which is different from traffic data.[54] A more serious privacy interference takes place when law enforcement officials obtain content data.[55]

Gravity of the privacy interference

The above exaxmined case law indicates that the ECtHR does not regard the privacy interference that takes place when traffic data is collected as particularly serious. The privacy interference caused by the investigative method can be placed at the left side of the scale of gravity, indicating that between a minor interference with the right private life takes place.

Required quality of the law

In the case of *Malone v. The United Kingdom*, the ECtHR found that the domestic legislation with regard to the collection traffic data from telecommunication providers was not 'in accordance with the law', since no specific regulations were available concerning (1) the scope of the investigative method and (2) the manner in which the 'metering information could be obtained from telecommunications providers (cf. Greer 1997, p. 12).[56]

---

51 ECtHR 2 August 1984, *Malone v. The United Kingdom*, appl. no. 8691/79, § 84. See also ECtHR 25 September 2001, *P.G. and J.H. v. The United Kingdom*, appl. no. 44787/98, § 42.

52 ECtHR 2 August 1984, *Malone v. The United Kingdom*, appl. no. 8691/79, § 84.

53 ECtHR 25 September 2001, *P.G. and J.H. v. The United Kingdom*, appl. no. 44787/98, § 46.

54 See the explanatory memorandum Convention on Cybercrime, par. 209. See also subsection 2.2.2 under B.

55 See also ECtHR 25 September 2001, *P.G. and J.H. v. The United Kingdom*, appl. no. 44787/98, § 46.

56 See ECtHR 2 August 1984, *Malone v. The United Kingdom*, appl. no. 8691/79, § 87.

Seventeen years later, the ECtHR found in the case of *P.G. and J.H. v. The United Kingdom* that the UK Telecommunications Act and Data Protection Act of 1984 contain an accessible and foreseeable statutory provision for law enforcement authorities to obtain billing information by issuing data production orders.[57] However, that legal basis only detailed the provision that processors of the traffic data were not liable when they disclosed information to law enforcement authorities in a criminal investigation (cf. Ölçer 2008, p. 294). The ECtHR was not persuaded by the defendant's argument that (more) detailed regulations were required for the investigative method.[58]

4.2.2 Privacy and data production orders issued to online service providers

This subsection examines the gravity of the privacy interferences that take place when data production orders are issued to online service providers. It is also considered whether the case law regarding the application of data production orders that are issued to telecommunications providers and the required quality of the law align with the examined digital investigative method. In chapter 2, data production orders that are issued to online service providers were distinguished in the following types of data: (A) subscriber data, (B) traffic data, (C) other data, and (D) content data.

As explained in subsection 2.2.1, this categorisation of data is partly derived from the categorisation made in the Convention on Cybercrime. States that have ratified this convention are obliged to introduce a differentiation in the legal protection of data production orders *"in accordance with its sensitivity"*.[59] According to the convention's explanatory memorandum, this implies that the substantive criteria and procedures that to apply the investigative power may vary according to the sensitivity of the data.[60]

Indeed, different types of data production orders issued to online service providers interfere with the right to privacy in different ways. These particular interferences with the right to privacy as articulated in art. 8 ECHR are further examined below.

A Subscriber data

The collection of subscriber information from online service providers by law enforcement officials interferes with the right to respect for private life. The reason is that the information is secretly gathered from online service providers and stored in police systems. The examined case law has shown that an interference takes place with the right to privacy when personal information from individuals is systematically gathered and stored in a police system.

57 ECtHR 25 September 2001, *P.G. and J.H. v. The United Kingdom*, appl. no. 44787/98, § 45.
58 ECtHR 25 September 2001, *P.G. and J.H. v. The United Kingdom*, appl. no. 44787/98, § 47.
59 Art. 15 Convention on Cybercrime.
60 Explanatory memorandum Convention on Cybercrime, par. 31.

Gravity of the privacy interference
Subscriber data consists of a limited set of information and does not reveal information about the communications themselves. For these reasons, the privacy interference of obtaining subscriber data is considered less serious than the privacy interferences involved when traffic and content data is obtained by using data production orders.[61]

Alignment with the existing required quality of the law
Based on the case law with regard to data production orders that are issued to telecommunication providers, the ECtHR requires an accessible and foreseeable legal basis for a data production order.[62] The case of *P.G. and J.H. v. The United Kingdom* does not indicate that particularly detailed regulations in statutory law or guidelines are required to obtain data from telecommunications by using data production orders.[63]

It may be added here that it follows from the examined case of *K.U. v. Finland* in section 3.1 of chapter 3 that States have the positive obligation to implement legislation that makes it possible to obtain identifiable data, i.e., subscriber data, from online service providers for the prevention of disorder and crime.[64] Following the decision of the *K.U. v. Finland* case, either detailed regulations in statutory law or a more general legal power that authorises law enforcement officials to obtain subscriber data from online service providers must therefore be available in the domestic regulations of contracting States of the ECHR.

B Traffic data
In the case of *P.G. and J.H. v. The United Kingdom,* the traffic data concerned the numbers that a suspect had dialled from his telephone during a specific period of time. According to present-day standards, the privacy interference that takes place when traffic data is obtained from online service providers may be considered as more serious than the fixed telephone situation as discussed in by the ECtHR in *P.G. and J.H. v. The United Kingdom*. The first reason is that traffic data today also encompasses *location data* (see B.1). The second is that *internet traffic data* consists of information other than traffic data concerning communication by telephone (see B.2). The gravity of the privacy interferences caused by data production orders with regard to these two types of data and their alignment with the required quality of the law are further examined below.

B.1 Location data
The following example illustrates the privacy interference that can take place when location data is obtained from a telecommunication service pro-

61 This will be further argued and illustrated in this subsection under B and D.
62 ECtHR 25 September 2001, *P.G. and J.H. v. The United Kingdom*, appl. no. 44787/98, § 45.
63 See subsection 4.1.1
64 ECtHR 2 December 2008, *K.U. v. Finland*, appl. no. 2872/02.

vider and further processed for law enforcement purposes. In 2012, I sent a data access request to my own telecommunications provider in order to obtain access to information that the provider had stored for law enforcement purposes.[65] The information, which was provided to me in an Excel file,[66] included location data that depicted the location of the telephone antennae to which my mobile telephone (with internet access) had been connected. I plotted the location of the telephone antennas on a map using publicly available online tools in order to visualise what this data can reveal.[67] The location data was also combined with the time and date that the mobile phone had been connected to the antennae, which were all part of the provided traffic data. All of the data pertained to a timespan of three days.

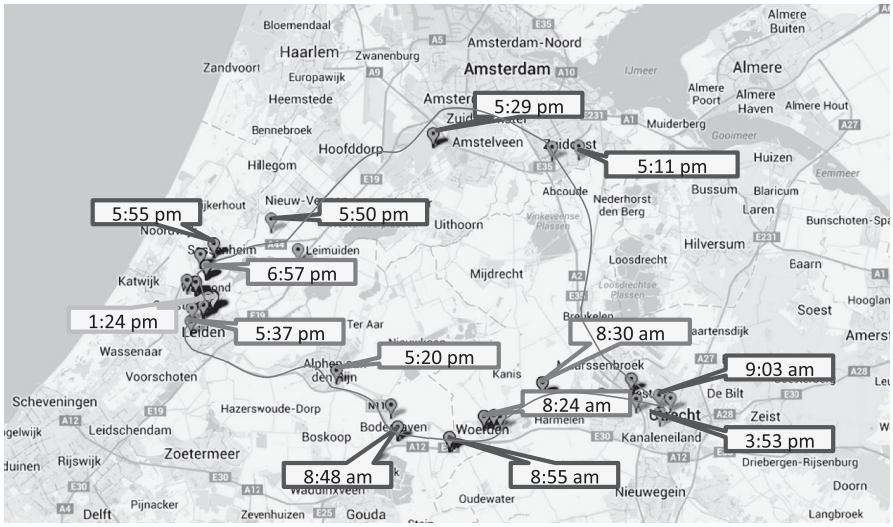

Figure 4.2: Representation of location data that can be derived from traffic data.

65 At the time, public telecommunication service providers were obliged by the Data retention act to retain traffic data relating to telephone data for 12 months and traffic data relating to internet data for 6 months. Subscribers have a right a right to access data under data protection regulations. I made use of this right. My data access request at my telecommunication provider aimed to find out what internet traffic data was retained by my telecommunications provider. See also J.J. Oerlemans, 'Leaving out notification requirements for data collection orders?', *LeidenLawBlog*, 17 October 2013. Available at: http://leidenlawblog.nl/articles/leaving-out-notification-requirements-for-data-collection-orders (last visited on 8 May 2014). The request was inspired by a German politician Malte Spitz, who also obtained access to his traffic data that was generated by mobile telephony. The politician used this information to illustrate the privacy infringement data retention obligations for telecommunication providers brings with (see 'Betrayed by our own data', *Die Zeit*, 26 March 2011. Available at: http://www.zeit.de/digital/datenschutz/2011-03/data-protection-malte-spitz (last visited 30 June 2014)).

66 The Excel file is available for review upon request at the author.

67 The provided location data was plotted on a map using the online service 'batchgeo'. Available at http://batchgeo.com/map/4db35deb53eb2727fb0f00b10e813087 (last visited on 25 June 2014).

Figure 4.2 clearly illustrates the insights into my private life that can be obtained using location data collected from my telecommunications provider. The dots on the map of Figure 4.2 illustrate the cell phone towers (32 in total) with which my mobile telephone was connected within the three-day period. The map also shows the time at which a connection was established between my telephone and the antenna on the cell phone tower. During those three days, I provided a cybercrime training course in the city of Utrecht. The map clearly shows how I took the train from Leiden Central Station to Utrecht Central Station and back. The thick line indicates the railroad track, which clearly runs between the dots that represent the cell phone antennae.

Gravity of the privacy interference

Figure 4.2 illustrates how location data can reveal an intricate picture of certain aspects of an individual's private life. With the information and a computer with an internet connection, a similar map can be created in 30 minutes. Thereby, an individual's movements can be made visible in a single glance. In addition, one can make an educated guess about this author's hometown by the number of dots around the city of Leiden on the map.

Telephone *traffic data* also consists of the calls made and received at specific times. Koops and Smits (2014, p. 141) point out that modern data processing techniques enable investigators to gain more insight into the personal lives of the involved individuals, even without taking notice of the 'contents' of information.[68] A detailed picture of certain aspects of an individual's private live can be obtained in particular when traffic data is collected over a longer period of time, combined with other information sources, and thoroughly analysed (cf. Koops & Smits 2014, p. 108-110).[69] These technological advancements must be taken into consideration when assessing the gravity of the privacy interference of investigative methods.

68 With reference to Hildebrandt & Gutwirth 2008 and Steenbruggen 2009, p. 56-57.

69 This observation is similar to the 'mosaic theory of privacy' that has been developed in the U.S. decision in the Maynard case (cf. Kerr 2013) (United States District of Columbia Circuit Court 6 August 2010, *United States v. Maynard*, 615 F.3d 544, (D.C. Cir. 2010). In the case of *Maynard*, a district court decided that the use of a GPS device to monitor the suspect's movements for a longer period of time amounted to a search that requires a warrant under the Fourth Amendment to the U.S. Constitution. Although the district court affirmed the U.S. doctrine that an individual's generally does not have reasonable expectation of privacy in public, the court found that the long-term observation of movements in the public amounts – taking in consideration the 'sum of its parts' – to a search that requires a warrant in the United States. Under the mosaic theory, a 'search' is perceived as a 'collective sequence of steps' rather than as individual steps (Kerr 2012, p. 313). As is illustrated in Figure 4.2, over time, the analysis of traffic information can reveal a 'mosaic of habits of an individual and relationships between individuals' (cf. Bellovin et al. 2014b, p. 556). Thus, the mosaic theory of privacy can help us understand how the analysis of traffic data – in particular location data – can seriously interfere with the right to respect for private life.

Alignment with existing required quality of the law

Considering the above analysis, it is clear that the processing of internet traffic data that has been obtained by data production orders issued to online service providers seriously interferes with the right to privacy. In the recent (2016) case of *Szabó and Vissy v. Hungary*, the ECtHR explicitly stated that "*the potential interferences with email, mobile phone and Internet services (…) attract the Convention protection of private life more acutely*".[70]

Given that greater privacy interferences takes place when traffic data is collected and processed by law enforcement officials today than in comparison to over than 15 years ago, it can be expected that more detailed regulations are now required for regulating data production orders. Existing ECHR requirements concerning traffic data obtained from telecommunications providers therefore misalign with the current reality of data production orders the regulations that follow from previous ECtHR case law with regard to data production orders issued to online service providers.

B.2 Internet traffic data

Internet traffic data consists of information other than telephone data. For example, it indicates at what time an internet connection is established and ended and which IP address the online service provider assigns to a device. This traffic data – which is also called 'session data' and 'logging data' – may be important for proving that a suspect used the Internet or a particular computer at a certain moment in time.[71]

Online service providers can also retain traffic information that reveals the 'destination IP address', which concerns the computer that an individual has connected with. That computer may be a server from an online service provider, such as an online storage provider, a social media service provider, or a webmail service provider. A destination IP address may therefore provide law enforcement officials with a lead to subsequently obtain private messages or other information from online service providers using data production orders.[72]

This analysis of the destination IP address also illustrates how difficult it can be to distinguish content data from traffic data. For instance, it is unclear whether (a) data with regard to search terms, (b) links to websites, (c) domain names, and (d) subject lines in private messages must be considered as content or traffic data (see Koops & Smits 2014, p. 93-106).[73] As a

70 ECtHR 12 January 2016, *Szabó and Vissy v. Hungary*, app. no 37138/14, § 53. It should be noted that it was also a factor that the investigative method involved the (potential) mass surveillance of telecommunications and not specifically a data production order to obtain traffic data from an online service provider. Nevertheless, the statement in my view indicates the collection of internet traffic data is deemed as privacy sensitive by the ECtHR.

71 See also subsection 2.2.2 under B.

72 How much information is available to law enforcement authorities depends on the type of service provider and the types of data that an online service provider retains.

73 With reference to Asscher & Ekker 2003, p. 104, Koops 2003, p. 77-78, Smits 2006, p. 416, Steenbruggen 2009, p. 56.

result, it is ambiguous whether these kinds of data are characterised as 'traffic data' or 'content data'. The collection and processing of (internet) traffic data clearly has the potential to seriously interfere with the right to respect for private life and correspondence as articulated as objects of protection in art. 8(1) ECHR.

Gravity of the privacy interference
Internet traffic information reveals at which point in time and for how long an individual made use of the Internet. The analysis in this subsection shows how traffic data and content data can be difficult to distinguish. Internet traffic data may indicate which websites an individual visited or which online services an individual used. The analysis of content data by law enforcement officials is a very serious interference with the right to respect to correspondence of individuals.

Alignment with the existing required quality of the law
As explained above with regard to the processing of location data, the ECtHR will consider the processing of internet traffic data as a serious interference with the right to privacy of individuals. It is expected the ECtHR will require detailed regulations for data production orders that are issued to obtain the data. In addition, the possibility that content data is obtained when these orders indicate that detailed regulations in statutory law is required for the investigative method.[74] Compared to the required quality of the law with regard to data production orders that are issued to telecommunication providers, a misalignment can be detected since the privacy interference is nowadays greater and more detailed regulations are expected to be required.

C Other data
The 'other data' category includes data that is not subscriber, traffic, or content data.[75] An example of this kind of data production order is the collection of profile information from online service providers, such as web forums or social media services.

An individual's online profile may, for instance, reveal that person's age, gender, interests, sexual orientation, and political affiliations. It may also include photographs that also reveal a person's race and possibly health conditions. The amount of information available depends on the amount of information an individual has disclosed to his social media provider on his private profile.[76]

74 See further under D.
75 See also subsection 2.2.2 under B.
76 If the information is publicly available, law enforcement officials can gather it and no data production orders are required.

Gravity of the privacy interference
The gathering and storage of personal information in the category of other data seriously interferes with the right to private life as defined in art. 8 ECHR. Profile information is, for instance, clearly more sensitive than subscriber information, due to the more sensitive type of information that often accompanies profile information and the potential variety of data. It can thus be argued that a serious privacy interference takes place when information from the 'other data' category is obtained from online service providers.

Alignment with the existing required quality of the law
Case law that deals with the collection of profile information using data production orders that are issued to online service providers is not available. However, the privacy interference that takes place appears to be more serious than the interference that results from collecting subscriber data. Since it is impossible to compare the privacy interference, and thus the required quality of the law, with the application of investigative methods that the ECtHR has decided on, a misalignment is clearly present.

D Content data
Content data can be defined as information that concerns the 'meaning or message' of communications.[77] In relation to online service providers, content data may take the form of private messages, including e-mails, which are sent between individuals who use a service; it may also include stored documents.[78] When content information is obtained from online service providers by the use of data production orders, there is no doubt that an interference takes place with the right to respect for private life and correspondence as protected by art. 8(1) ECHR.

Collecting private messages that are stored at online service providers can be compared with intercepting communications. In both cases, the meaning of messages in communications can be obtained. The ECtHR has made it clear in case law that the interception of telephone calls interferes with the right to respect for a person's private life and correspondence as protected in art. 8(1) ECHR.[79] As already mentioned in section 3.3, the ECtHR held in the case of *Copland v. The United Kingdom* that the interception of *electronic* communications concerning e-mail and information derived from the monitoring of personal internet usage also interferes with

77 Explanatory memorandum Convention on Cybercrime, par. 209. See also subsection 2.4.2.

78 Stored documents may be disclosed to law enforcement officials by cloud storage services, such as Google Drive of Microsoft's SkyDrive. See also subsection 2.2.2 under B.

79 See, e.g., ECtHR 6 September 1978, *Klass and Others v. Germany*, appl. no. 5029/71, § 41, ECtHR 24 April 1990, *Huvig v. France*, appl. no. 11105/84, § 25, ECtHR 30 July 1998, *Valenzuela Contreras v. Spain*, appl. no. 58/1997/842/1048, § 42, ECtHR 18 February 2000, *Amann v. Switzerland*, appl. no. 27798/95, § 44 and ECtHR 29 June 2006, *Weber and Saravia v. Germany*, appl. no. 54934/00, § 77.

the right to respect for private life and correspondence as protected in art. 8(1) ECHR.[80]

The collection of stored documents through data production orders is comparable to the search of an office or residence, during which law enforcement officials can seize documents (or a computer containing documents) for evidence-gathering purposes. The ECtHR considers a search in an office or residence undertaken by law enforcement authorities to be an interference with the right to respect for private life and a home as protected by art. 8(1) ECHR.[81] More recently, the ECtHR also specifically dealt with a situation in which law enforcement officials searched an office in order to seize computers and search documents stored therein for evidence-gathering purposes. As explained in subsection 2.4.2, in this study, this investigative method is called a 'computer search'. In case law involving computer searches, the ECtHR also found that the evidence-gathering activities interfered with both the right to home and correspondence as protected by art. 8(1) ECHR.[82] It can therefore be argued that the collection of *remotely* stored documents at online service providers interferes with the right to respect for home and correspondence as articulated as objects of protection under art. 8 ECHR (cf. Koops & Smit 2014, p. 141).[83]

Gravity of the privacy interference

The privacy interference that takes place when a data production order is issued to an online service provider to obtain content data is comparable to the privacy interference that occurs when electronic communications are intercepted. The reason is that in both cases, law enforcement officials secretly obtain information relating to the meaning or message of communications between individuals. The ECtHR regards the interception of communications as a serious privacy interference.[84] It requires detailed regulations with procedural safeguards for using the interception of communications as

80 See ECtHR 3 April 2007, *Copland v. The United Kingdom*, appl. no. 62617/00, §41-42.

81 See, e.g., ECtHR 26 December 1992, *Niemietz v. Germany*, appl. no. 13710/88, § 26, ECtHR 25 February 1993, *Funke v. France*, appl. no. 10828/84, § 48.

82 See ECtHR 27 September 2005, *Petri Sallinen and Others v. Finland*, appl. no. 50882/99, § 71, ECtHR 7 October 2007, *Wieser and Bicos Beteiligungen GmbH v. Austria*, appl. no. 74336/01, § 45, and ECtHR 14 March 2013, *Bernh Larsen Holding AS and Others v. Norway*, appl. no. 24117/08, § 105.

83 Note that the ECtHR interprets the concept of a "home" broadly (cf. Krabbe in: Harteveld 2004, p. 156). The term 'home' can also extent to certain professional or business premises. See, e.g., ECtHR 26 December 1992, *Niemietz v. Germany*, appl. no. 13710/88, § 30, ECtHR 27 September 2005, *Petri Sallinen and Others v. Finland*, appl. no. 50882/99, § 70, and ECtHR 14 March 2013, *Bernh Larsen Holding AS and Others v. Norway*, appl. no. 24117/08, § 104.

84 See, e.g., ECtHR 2 August 1984, *Malone v. The United Kingdom*, appl. no. 8691/79, § 67, ECtHR 30 July 1998, *Valenzuela Contreras v. Spain*, appl. no. 58/1997/842/1048, § 46 and ECtHR 4 December 2015, *Roman Zakharov v. Russia*, appl. no. 47143/06, § 229.

an investigative method, in order to protect the individuals involved from arbitrary governmental interferences.[85]

The ECtHR requires the following procedures to be in place when (electronic) communications are intercepted: (1) the nature of the offences which may give rise to an interception order must be detailed; (2) a definition of the categories of people liable to have their telephones tapped must be available; (3) a restriction on the duration of telephone tapping must be set; (4) the procedure to be followed for examining, using, storing, and deleting the data obtained must be available; and (5) the precautions to be taken when communicating the data to other parties must be specified in the domestic legislation of a contracting State to the ECHR.[86] In the context of secret surveillance measures that involve the interception of communications, the ECtHR also considers it important that (6) the investigative method or surveillance measure is authorised by an independent authority, preferably a judge.[87]

With regard to computer searches, the ECtHR required in case law that detailed regulations with adequate procedural safeguards against abuse are available in the domestic laws of contracting States. For example, in the case of *Wieser and Bicos Beteiligungen GmbH v. Austria*, a law firm was searched and computers containing privileged documents were seized.[88] Here the ECtHR noted that it required in comparable cases that (1) the search was based on both a warrant issued by a judge and reasonable suspicion, (2) the scope of the warrant was reasonably limited, and – since the search took place in a lawyer's office – (3) the search is carried out in the presence of an independent observer to ensure that materials subject to professional secrecy were not removed.[89] In the case of *Wieser and Bicos Beteiligungen GmbH v. Austria*, the law enforcement officials did not follow the domestic procedures for computer searches.[90] The search was considered disproportionate and in violation of art. 8 ECHR, even though the domestic regulations were 'in accordance with the law'.

85 See, e.g., ECtHR 2 August 1984, *Malone v. The United Kingdom*, appl. no. 8691/79, § 67, ECtHR 30 July 1998, *Valenzuela Contreras v. Spain*, appl. no. 58/1997/842/1048, § 46 and ECtHR 4 December 2015, *Roman Zakharov v. Russia*, appl. no. 47143/06, § 229.

86 See ECtHR 24 April 1990, *Huvig v. France*, appl. no. 11105/84, § 34, ECtHR 30 July 1998, *Valenzuela Contreras v. Spain*, appl. no. 58/1997/842/1048, § 46, ECtHR 18 February 2000, *Amann v.* Switzerland, appl. no. 27798/95, § 76, ECtHR 29 June 2006, *Weber and Saravia v. Germany*, appl. no. 54934/00, § 95 and ECtHR 4 December 2015, *Roman Zakharov v. Russia*, appl. no. 47143/06, § 231.

87 See most notably ECtHR 4 December 2015, *Roman Zakharov v. Russia*, appl. no. 47143/06, § 257-267 with reference to ECtHR 26 April, *Dumitru Popescu v. Romania* (no. 2), appl. no. 71525/01, § 71.

88 ECtHR 7 October 2007, *Wieser and Bicos Beteiligungen GmbH v. Austria*, appl. no. 74336/01, § 8-10.

89 ECtHR 7 October 2007, *Wieser and Bicos Beteiligungen GmbH v. Austria*, appl. no. 74336/01, § 57.

90 ECtHR 7 October 2007, *Wieser and Bicos Beteiligungen GmbH v. Austria*, appl. no. 74336/01, § 63.

Alignment with the existing required quality of the law
The collection of stored private messages and stored documents from online service providers has been compared with case law regarding the interception of communications and computer searches. However, it is not clear whether the ECtHR also deems these investigative methods comparable with the collection of content data from online service providers. In my view, the seriousness of the privacy interferences and required quality of the law that can be deduced from this case law are also relevant for digital investigative methods. Case law with regard to the interception of communications and computer searches can therefore provide a good basis for regulating the examined digital investigative method.

4.2.3 Desired quality of the law

This subsection determines the *desirable* quality of the law based on the gravity of the privacy interference that takes place when data production orders are issued to online service providers.

In general, it should be observed that the gravity of the privacy interference that takes place when law enforcement officials obtain data from online service providers depends on the kind of data that is collected. It is also important to keep in mind that law enforcement authorities have the ability to obtain and combine different types of data. For instance, they may be able to collect financial data and internet traffic data from different online service providers and subsequently analyse that data in order to identify other individuals who may be relevant in a criminal investigation. It should be recalled here that the ECtHR considers the further processing of personal information as an increased interference with the right to privacy as defined in art. 8 ECHR. This factor should be taken into consideration when determining the desirable quality of the law.

The quality of the law that I view as desirable for regulating data production orders that are issued to online service providers is presented below. The four types of data are discussed separately.

A Subscriber data
With regard to subscriber data, the ECtHR likely does *not* regard the privacy interference as *particularly serious*. The first reason is that subscriber data consists of a limited set of data. The second is that subscriber data that is obtained from online service providers is not significantly different from subscriber data from telecommunication providers.

However, the desirable quality of the law should consist of *detailed regulations in statutory law* that stipulate under which conditions subscriber data can be obtained. A general legal basis in my view does not suffice, since the investigative method should be seen in connection with other (more intrusive) data production orders. This category of data should also be included in the detailed regulations for the investigative method.

B Traffic data

The collection of traffic data *seriously interferes* with the right to privacy of the individuals involved. Case law with regard to data production orders to obtain traffic data seems outdated. We no longer exclusively have telephone conversations using landlines. In addition, traffic data no longer only consists of the calls made and received coupled with date and time stamps. Today law enforcement officials can also collect location and internet-related traffic data from telecommunication providers, which can then be further processed to obtain a detailed picture of certain aspects of an individual's private life.

I therefore argue that *detailed regulations in statutory law* are desirable for the investigative method. The information is more intrusive than subscriber data, since traffic data consists of a broader category of data and is more sensitive in nature than subscriber data. As a procedural safeguard, I find the *authorisation of an investigative judge* desirable.

C Other data

The collection of other data through data production orders *seriously interferes* in the right to privacy of the individuals involved. Law enforcement officials are able to collect many different types of potentially sensitive data from online service providers, such as profile information from social media services. It is often unclear from the outset how much and what kind of information is going to be obtained.

Taking into account present-day standards, I argue it is desirable to implement *detailed regulations in statutory law* for the investigative method. As a procedural safeguard, the *authorisation of a higher authority* (such as a public prosecutor) is also desirable. Since the information can also encompass photographs of individuals who are attached to a (private) profile, *the authorisation of an investigative judge* is in my view also appropriate.

D Content data

When private messages are obtained, the collection of content data *seriously interferes* with the right to respect for private life and correspondence. The collection of content data can also interfere with the right to respect for home and correspondence when stored documents are gathered.

In my view, a *detailed legal basis in statutory law* is desirable for data production orders relating to content data. In addition, the *authorisation of an investigative judge* is in my view appropriate. That means that typically the request for a warrant to obtain the data is also restricted. For private messages, that restriction can be set by making it mandatory for data production orders to specify the relevant time period. For stored documents, filters from forensic software can be utilised to select the relevant documents for law enforcement authorities.

4.3 Applying online undercover investigative methods

This section analyses the gravity of the privacy interferences that take place when online undercover investigative methods are applied. The ECtHR has only developed case law with regard to the application of undercover investigative methods in the physical world. The application of undercover investigative methods on the Internet may or may not interfere with the right to privacy in a different manner.

To answer that question, the case law with regard to the application of undercover investigative methods in the physical world is first examined in subsection 4.3.1. Subsection 4.3.2 then examines the privacy interferences that take place when the digital counterparts of these methods are applied. Subsection 4.3.3 subsequently concludes the section by determining the *desirable* quality of the law for regulating undercover investigative methods.

4.3.1 The right to privacy and undercover investigative methods

In its case law regarding undercover investigative methods, the ECtHR usually determines whether an undercover investigative method interferes with the right to a fair trial, as defined in art. 6 ECHR.[91] Krabbe (in: Harteveld 2004, p. 144) explains this by arguing that the ECtHR often first considers art. 6 ECHR in cases where an applicant has protested against the legitimacy of an undercover operation. After the test with regard to art. 6 ECHR is conducted, the ECtHR does not consider it necessary to also test the legitimacy of the undercover operation under art. 8 ECHR.[92]

Case law of the ECtHR with regard to undercover operations and the right to privacy as articulated in art. 8 ECHR is scarce. The case of *Lüdi v. Switzerland* is an exception.[93] Here the ECtHR did consider whether interference with the right to privacy took place in the context of an undercover operation. In this case, an undercover agent bought drugs from Mr Lüdi as part of a 'pseudo-purchase' investigative method.[94] The facts are as follows. A Swiss law enforcement officer went undercover using the assumed name of 'Toni' and pretended to be a potential buyer of cocaine that was presumably being sold by Mr Lüdi. After meeting with Mr Lüdi three times, (undercover agent) Toni reported that Mr Lüdi had promised to sell him, as an intermediary, two kilograms of cocaine worth 200,000 Swiss francs.

91 See, e.g., ECtHR 9 June 1998, *Teixeira de Castro v. Portugal*, no. 44/1997/828/1034, ECtHR 5 February 2008, *Ramanauskas v. Lithuania*, appl. no. 74420/01 and ECtHR 4 November 2010, *Bannikova v. Russia*, appl. no. 18757/06.

92 Krabbe in: Harteveld 2004, p. 144, referring to ECtHR 12 July 1988, *Schenk v. Switzerland*, appl. no. 10862/84.

93 See ECtHR 15 June 1992, *Lüdi v. Switzerland*, appl. no. 12433/86.

94 See ECtHR 15 June 1992, *Lüdi v. Switzerland*, appl. no. 12433/86, § 9-13.

The suspect had also borrowed 22,000 Swiss francs from a third person for the purchase of cocaine or other narcotics. After arresting the suspect, the Swiss police searched his home and found traces of cocaine and hashish on a number of objects.[95]

With regard to the legitimacy of the undercover operation, the ECtHR found that no interference took place with the right to respect for private life. It reasoned that: *"Mr Lüdi must (…) have been aware from then on that he was engaged in a criminal act punishable under Article 19 of the Drugs Law and that consequently he was running the risk of encountering an undercover police officer whose task would in fact be to expose him."*[96] In other words, in the *Lüdi* case, the ECtHR seems to have adopted the approach that individuals who engage in criminal activities do not have a reasonable expectation of privacy, because they should be aware that undercover investigative methods could be used against them (cf. Ölçer 2008, p. 279). This would be a far-reaching approach, since it denies individuals involved in undercover operations from protection by art. 8 ECHR.[97] This aspect of the *Lüdi* case is critically analysed in subsection 4.3.3.

Gravity of the privacy interference

Since no other case law is available with regard to the privacy interference that takes place when undercover investigative methods are applied, it is not possible to determine the gravity of the privacy interference.

However, as mentioned in the introduction to this section, the ECtHR does test whether undercover investigative methods comply with the right to a fair trial. More specially, the ECtHR tests whether no entrapment has taken place. In the case of *Teixeira de Castro v. Portugal*, the ECtHR held that the right to a fair trial would be violated when law enforcement officials *"do not confine themselves to investigating criminal activity in an essentially passive manner, but exercise an influence such as to incite the commission of the offense"*.[98] Essentially, the ECtHR tests whether the offence would have been committed without the intervention of law enforcement authorities (cf. Ölçer

95 See ECtHR 15 June 1992, *Lüdi v. Switzerland*, appl. no. 12433/86, § 14.

96 ECtHR 15 June 1992, *Lüdi v. Switzerland*, appl. no. 12433/86, § 40-41. Note that the ECtHR does consider it an interference with the right to respect for correspondence as provided in art. 8 ECHR, from the point that law enforcement official records a conversation with the suspect during a criminal investigation. See, e.g., ECtHR 12 May 2000, *Khan v. the United Kingdom*, appl. no. 35394/97, § 26-28, ECtHR 8 April 2003, *M.M. v. the Netherlands*, no. 39339/98, § 29 and 79 and ECtHR 10 March 2009, *Bykov v. Russia*, appl. no. 4378/02, § 72.

97 The ECtHR may have been inspired by the U.S. doctrine on a 'reasonable expectation of privacy' in undercover operations. See subsection 9.4.2 for further analysis.

98 See ECtHR 9 June 1998, *Teixeira de Castro v. Portugal*, no. 44/1997/828/1034, § 38.

2014, p. 16). An undercover operation should remain 'essentially passive'.[99] Importantly, the ECtHR has articulated qualitative requirements for the domestic legal frameworks of contracting States to prevent entrapment from occurring and to ensure a fair trial.[100] These requirements are such that it is possible to transpose them to requirements for the *regulation* of undercover operations. Thus, although these requirements are based in art. 6 ECHR, they, or aspects of them, are similar to requirements that apply to interferences in the context of art. 8 ECHR. As such, it is taken as a point of departure in this study that the art. 6 ECHR may be equated with art. 8 ECHR requirements. The qualitative requirements that affect the regulation of undercover investigative methods themselves are further examined below.

Required quality of the law

In relation to the regulation of undercover investigative methods, it is important to note that the ECtHR required in the case of *Furcht v. Germany*: *"clear and foreseeable procedures for authorising investigative measures, as well as for their proper supervision"*.[101] The ECtHR thus requires (1) detailed regulations for undercover investigative methods and (2) the procedural safeguard of supervision for undercover investigative methods.

In addition, the ECtHR has repeatedly emphasised in case law that an investigative judge provides 'the most appropriate means' for supervising undercover operations.[102] Nevertheless, the ECtHR also accepts the supervision of a public prosecutor, insofar 'adequate procedures and safeguards' are available.[103] It does not concretely explain which procedures and safeguards are considered adequate. However, it is clear that the procedures for undercover operations must ensure transparency regarding the operations themselves and aim to prevent entrapment by law enforcement authorities.

---

99 See ECtHR 4 November 2010, *Bannikova v. Russia*, appl. no. 18757/06, §47. See also ECtHR 23 October 2014, *Furcht v. Germany*, appl. no. 54648/09 § 51. To determine whether law enforcement authorities interfered in an active manner that brought the suspect to committing the offence, the ECtHR takes into consideration the following four factors: (1) the reasons underlying the undercover operation; (2) the behaviour of the law enforcement authorities; (3) the existence of a reasonable suspicion that the suspect was involved in criminal behaviours; and (4) the predisposition to the crime of a suspect (see Ölçer 2014, p. 16, see also ECtHR 4 November 2010, *Bannikova v. Russia*, appl. no. 18757/06, *EHRC* 2011/9, m.nt. Ölçer).

100 See ECtHR 4 November 2010, *Bannikova v. Russia*, appl. no. 18757/06, § 48. In the case of *Bannikova v. Russia*, the ECtHR also noted that the need for transparency generally requires that undercover agents and other witnesses can be heard in court and be cross-examined by the defence, unless detailed reasons are provided for denying this right to questioning (ECtHR 4 November 2010, *Bannikova v. Russia*, appl. no. 18757/06, § 65).

101 ECtHR 23 October 2014, *Furcht v. Germany*, appl. no. 54648/09, § 53.

102 See 50 ECtHR 24 June 2008, *Milinienè v. Lithuania*, appl. no. 74355/01, § 39: *"Moreover it had been adequately supervised by the prosecution, even if court supervision would have been more appropriate for such a veiled system of investigation"*. See also ECtHR 4 November 2010, *Bannikova v. Russia*, appl. no. 18757/06, § and ECtHR 23 October 2014, *Furcht v. Germany*, appl. no. 54648/09, *EHRC* 2015/1, m. nt. Ölçer at 9.

103 ECtHR 4 November 2010, *Bannikova v. Russia*, appl. no. 18757/06, §50.

4.3.2 The right to privacy and online undercover investigative methods

This subsection examines the gravity of the privacy interferences that take place when undercover investigative methods are applied in an online context. It is also consided whether the case law regarding the application of undercover investigative methods in the physical world and required quality of the law align with the law that is required for the examined online application of the investigative method.

In chapter 2, online undercover investigative methods were categorised as: (A) online pseudo-purchases, (B) online undercover interactions with individuals, and (C) online infiltration operations. These three digital investigative methods are further examined below.

A Online pseudo-purchases

An online pseudo-purchase is an investigative method in which an undercover law enforcement official purchases a good or data that a suspect is offering on the Internet (e.g., in an online forum), in order to collect evidence in a criminal investigation or with the intention to arrest an individual upon delivery of the good or data.[104]

Gravity of the privacy interference

The case of *Lüdi v. Switzerland* indicates that the ECtHR does not consider the purchase of drugs offered by suspects as a privacy infringing activity.[105] However, as the analysis in subsection 4.3.1 has shown, the ECtHR does test whether the right to a fair trial as defined in art. 6 ECHR is violated in such situations. In particular, the ECtHR tests whether entrapment took place. The procedures and safeguards required to ensure a fair trial in connection with undercover investigative methods used in the physical world also apply in an online context, since the risk of entrapment exists here as well.

When a law enforcement official purchases a good or data from an individual in an online forum, that good or data is already being offered on the Internet to anyone who wants to purchase it. In such a situation, the risk of entrapment is small. It may also be argued that a minor privacy interference is taking place. The individual offering the good or data may feel betrayed after a transaction with a law enforcement official has been completed. However, the privacy interference remains limited due to the one-time application of the investigative method.

When the physical and online pseudo-purchase are compared, the major differences are that the online pseudo-purchases can be applied *anywhere in the world* and that both the buyer and the seller can (attempt to) remain *anonymous*. The latter can be done by using a nickname and avoiding reg-

104 See also subsection 2.2.2 under C.

105 ECtHR 15 June 1992, *Lüdi v. Switzerland*, appl. no. 12433/86, §40-41. See also, e.g., ECtHR 4 November 2010, *Bannikova v. Russia*, appl. no. 18757/06 and ECtHR 5 February 2008, *Ramanauskas v. Lithuania*, appl. no. 74420/01.

istration of the originating (public) IP address at the platform that provides the service. In addition, both the seller and the buyer can make use of webmail services that are offered through Tor, which help to hide the originating (public) IP address. In my view, online pseudo-purchases' two characteristics of (1) global reach and (2) anonymity do not significantly influence the intrusiveness of the digital investigative method of an online pseudo-purchase.[106]

Alignment with the existing required quality of the law
The above analysis indicates that the privacy interference that takes place when online pseudo-purchases are performed is non-existent from the perspective of the ECtHR. The risk of entrapment does exist in an online context, as it does in a physical world pseudo-purchase. However, in my view the risk is not greater in an online context. The detailed procedures and safeguards necessary to ensure a fair trial when this undercover investigative method is used in the physical world therefore align well with the application and required quality of the law when it is used in an online context.

B Online undercover interactions with individuals
Online undercover interactions with individuals to gather evidence as part of criminal investigations can take place on many internet platforms, such as chat services, online black markets, and social media services. With the right knowledge of internet subcultures, law enforcement officials can interact and build relationships with individuals under a credible, fake identity in order to gather evidence (cf. Siemerink 2000b, p. 145).[107] It is straightforward for undercover agents to create an 'online identity' (cf. Siemerink 2000b, p. 143). Law enforcement authorities can even prepare for online undercover investigations by creating many online identities – complete with pre-set profiles on social media websites – that can be used later in time. Due to the lack of physical proximity to the individual involved in the operation, an undercover agent is in no immediate risk of bodily injury if his cover is exposed (cf. Siemerink (2000b, p. 144).[108] Another interesting aspect of online undercover interactions as an investigative method is that law enforcement officials may be able to take over an account that is voluntarily provided by an individual who has either already interacted with suspects or has an interesting information position and cooperates with law enforcement authorities as an informant.[109] The gravity of the privacy interference that takes place in relation to this investigative method is considered below.

106 These characteristics do pose questions with regard to the territorial limitation of enforcement jurisdiction. These questions are addressed in section 9.4.
107 See also subsection 2.2.2 under C.
108 That is not to say that undercover law enforcement officials or informant are never subjected to a risk of bodily injury after an online undercover operation. Criminals may seek out an online undercover agent in order to punish that individual in the physical world.
109 See also subsection 2.2.2 under C.

Gravity of the privacy interference
Online undercover interactions can take place with individuals anywhere in the world and both participants – namely the undercover agent and the involved individual – can stay relatively anonymous. The individual who is targeted by the undercover operation cannot interpret certain communication signals (e.g., non-verbal[110] signals).

However, compared to undercover interactions with individuals in the physical world, online undercover investigative methods do not interfere more seriously in the private lives of the individuals involved. In the case of undercover interactions with individuals both in 'cyberspace' and 'meatspace',[111] undercover agents often gain the trust of individuals involved in the criminal investigation and develop personal relationships. When law enforcement officials mislead suspects in an undercover operation, those individuals will often feel betrayed after the operation (cf. Kruisbergen & De Jong 2010, p. 218). A privacy interference clearly takes place, given that personal relationships may be developed with the individual involved in this type of undercover operation. The privacy interference may be regarded as being greater than in an (online) pseudo-purchase, since the investigative method involves more than a one-time application.

Alignment with existing quality of the law
The individuals involved in online undercover interactions must be protected from an arbitrary governmental application of power and a mechanism must be in place to ensure that no entrapment by law enforcement officials takes place. During these online interactions with individuals, the same risk of entrapment arises as when the interactions take place in the physical world. In both cases, law enforcement officials must remain 'essentially passive' in the operation. The required existing quality of the law in the form of detailed regulations for the undercover investigative methods and articulated safeguards by the ECtHR with regard to the supervision of undercover operations (preferably by an investigative judge) therefore align well for application to the investigative method in an online context, in as far as entrapment may become an issue in the course of such operations.

C Online infiltration operations
Infiltration operations are similar to undercover interactions with individuals. The distinction is that the former includes the possibility that law enforcement officials can commit (authorised) crimes in order to maintain their cover and gain the trust of the targeted individuals in a criminal investigation (cf. Joh 2009, p. 166). In other words, in infiltration operations, law enforcement officials can *participate* in crime with other individuals in order

110 Obviously, 'verbal' is in this context interpreted as written text.
111 See for this comparison between cyberspace and meatspace, e.g., https://en.wikipedia.org/wiki/Real_life#Related_terminology (last visited 18 December 2015).

to gather evidence and gain access to that organisation's upper echelons (cf. Joh 2009, p. 167).[112]

Gravity of the privacy interference
The gravity of the privacy interference that takes place in online infiltration operations is similar to that of the investigative method of online interactions with individuals. However, in online infiltration operations, risks that endanger the *integrity* of criminal investigations are greater. A specific risk of infiltration operations is that undercover agents can 'go rogue' and commit unauthorised crimes, especially when civilians are used as undercover agents (cf. Kruisbergen & De Jong 2010, p. 130-131).[113] Law enforcement officials can also overstep their mandate and engage in unauthorised illegal activities.[114] The risk of entrapment is greater in the context of infiltration operations than in undercover interactions.

Alignment with the existing required quality of the law
Online infiltration operations can be characterised by their global reach and the possibility to participate in a criminal investigation while remaining relatively anonymous. The privacy interference that takes place in online infiltration operations is similar to that of the investigative method of online interactions with individuals and does not appear different to infiltration operations in the physical world. In online infiltration operations, the risks that endanger the integrity of criminal investigations and of entrapment are clearly present. In online infiltration operations, governmental agents or civilians are authorised to participate in a criminal organisation, which creates the risk that they will overstep their mandate. The required quality of the law in the form of detailed regulations for the investigative method and proper supervision, preferably by an investigative judge, therefore aligns well with the quality of the law for online infiltration operations.

4.3.3 Desired quality of the law

This subsection determines the *desirable* quality of the law based on the gravity of the privacy interference that takes place when online undercover investigative methods are applied.

First, a general comment must be made regarding the lack of case law for undercover investigative methods as they relate to art. 8 ECHR. As the analysis in subsection 4.3.1 has shown, the ECtHR indicated in the case of

112 See also subsection 2.2.2 under C.

113 This research is restricted to investigative methods that are applied by law enforcement officials. Therefore, this aspect is not elaborated upon in this study.

114 For example, in the Silk Road investigation (also described in subsection 2.3.3), an undercover law enforcement agent transferred bitcoins (a virtual currency) to himself without authorisation. See Reuters, 'US undercover agent jailed for six years for Silk Road Bitcoin theft', *BBC News*, 20 October 2015. Available at: http://www.bbc.com/news/business-34588568 (last visited on 12 May 2016).

Lüdi v. Switzerland that individuals do not have a reasonable expectation of privacy when a pseudo-purchase is applied as an investigative method. Therefore, for that undercover investigative method, no interference with the right to privacy as defined in art. 8 ECHR takes place. I disagree with that decision, as fundamental rights apply to anyone. From a principled viewpoint, it is does not make sense to exclude individuals subjected to undercover operations from protection against arbitrary governmental interferences. The protection of all individuals from the arbitrary use of governmental power is an essential component of the rule of law and human rights (cf. Joubert 1994, p. 21 and Corstens 1995, p. 547-548). Furthermore, as part of the presumption of innocence, law enforcement officials cannot decide in advance whether a person is a criminal and should be excluded from protection under art. 8 ECHR (cf. Joubert 1994, p. 21). It is unclear whether the ECtHR would repeat the reasonable expectation of privacy doctrine as developed in the *Lüdi* case today. In the more than 20 years that have followed the decision of *Lüdi*, the ECtHR has not again excluded the privacy interests of individuals in the context of undercover operations (cf. Krabbe in: Harteveld 2004, p. 153).[115] Since this case, the ECtHR has repeatedly dealt with the legitimacy of undercover investigative methods. Nonetheless, in these subsequent cases the ECtHR has focused on the right to a fair trial and the question of whether entrapment has taken place. In those cases, the ECtHR required detailed regulations with safeguards to ensure a fair trial and prevent entrapment by law enforcement officials. As explained above, the point of departure is that those requirements are similar to those set for interferences with privacy in the context of art. 8 ECHR.

Second, it is important to note that the analysis in subsection 4.3.2 has shown that although online undercover investigative methods are similar to their non-digital counterparts, they are not the same as undercover investigative methods in the physical world. They are different in the sense that online undercover operations have a global reach and can be conducted with the relative anonymity that the Internet offers to everyone. The opportunity to 'take over an account' of an individual who is already part of a criminal organisation or has a particular information position is unique to online undercover investigative methods. Nevertheless, when undercover investigative methods are applied in an online context, in my view the gravity of the interference to the right to privacy is not notably different from when they are applied in the physical world. Thus, whilst differences between digital and non-digital variants may have (more) bearing on issues

115 With the exception of the case of ECtHR 10 March 2009, *Bykov v. Russia*, appl. no. 4378/02, § 72, in which an undercover agent recorded a conversation with the suspect. In this case, the recording of the conversation with an undercover agent led to an interference with the right for private life under art. 8 ECHR. However, the privacy interference thus focused on the private recording, not the undercover interactions with the individual himself.

of misalignment in the context of other norms (such as that concerning entrapment in art. 6 ECHR), they are not substantial from the perspective of art. 8 ECHR.

The quality of the law that is in my view desirable for the regulation of the three identified online undercover investigative methods is presented below.

A Online pseudo-purchases

The gravity of the privacy interference that takes place when an online pseudo-purchase is applied is limited, due to the one-time application of the investigative method. However, the risk of entrapment is still present. The *detailed regulations in statutory law* that are already required by the ECtHR for undercover investigative methods are also desirable for the regulation of online pseudo-purchases as an investigative method. The ECtHR regards the involvement of an investigative judge as 'the most appropriate means' for supervising an undercover operation. However, considering the minor privacy interference and the entrapment risk involved, my view is that *the involvement of a public prosecutor* in supervising the application of this online undercover investigative method is appropriate and desirable.

B Online undercover interactions with individuals

The gravity of the privacy interference is greater when online undercover interactions with individuals are applied as an investigative method than when online pseudo-purchases are used. Law enforcement officials obtain more detailed knowledge about aspects of the private life of the individuals involved and the investigative method is applied for a longer period of time. The risk of entrapment can also be present when this digital investigative method is applied.

Therefore, I argue that both (1) a *detailed legal basis in statutory law* for the investigative method and (2) the *supervision of an investigative judge* as a procedural safeguard are desirable for regulating the investigative method.

C Online infiltration operations

The gravity of the privacy interference in the context of online infiltration operations is similar to when the investigative method of online undercover interactions is applied. However, the safeguards to prevent entrapment and help ensure transparency may be of greater importance in online infiltration operations. The reason is that in online infiltration operations, risks that endanger the *integrity* of criminal investigations and entrapment are more frequently present (cf. Ölçer 2014, p. 18). The quality of the law that is desirable consists of (1) a *detailed legal basis in statutory law* to apply to the investigative method and (2) the procedural safeguard of *an investigative judge* to supervise the online undercover investigative method.

4.4 Performing hacking as an investigative method

This section analyses the privacy interferences that take place when hacking is applied as an investigative method. As the ECtHR has not developed case law addressing this situation, an analogy with other investigative methods must be made.

The investigative methods of network and remote searches are comparable with the investigative method of a computer search. The case law concerning computer searches and the right to privacy is examined in subsection 4.4.1. The investigative method of using policeware is comparable with investigative methods involving the interception of electronic communications, more specifically using 'covert listening devices'. The case law with regard to the use of covert listening devices and the right to privacy is examined in subsection 4.4.2. In subsection 4.4.3, the privacy interferences that take place when hacking is performed as an investigative method are examined. Subsection 4.4.4 concludes the section by determining the *desirable* quality of the law for the regulation of hacking as an investigative method.

4.4.1 The right to privacy and computer searches

The gravity of the privacy interference that takes place in relation to computer searches is explored in this subsection by examining the relevant case law of the ECtHR. The investigative method is visualised in Figure 4.3.

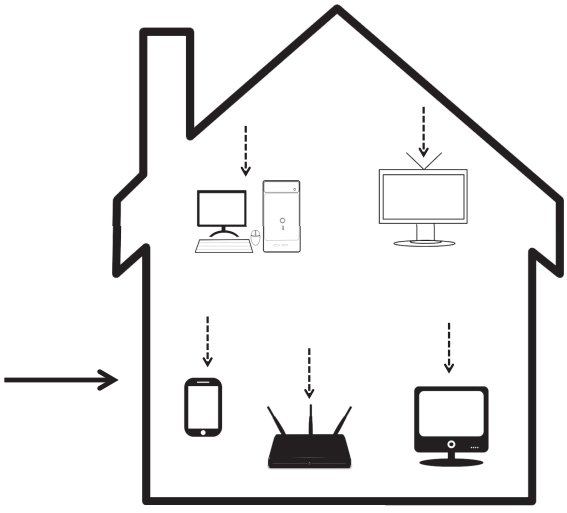

Figure 4.3: Simplified model of a computer search.

Figure 4.3 illustrates how a search can be conducted at a certain place, such as residence. During the search, law enforcement officials can subsequently seize (all types of) computers that may contain evidence that is relevant to

the criminal investigation. Figure 4.3 is called a simplified model of a computer search, because the initial search can also take place at any different place.

Gravity of the privacy interference

In the early 1990s, the ECtHR indicated in case law that a search in an office or residence by law enforcement officials is considered a serious interference with the right to respect for private life and home as protected by art. 8(1) ECHR.[116] In these cases, the concept of 'home' is interpreted broadly and the ECtHR has clarified that it can also encompass business premises.[117] Hacking as an investigative method and a search inside a residence are comparable as investigative methods, given that both involve an activity in which law enforcement officials gain access to a private place and can thereafter obtain intimate knowledge about individuals' private lives. Personal information such as documents, photos, and videos are now often stored digitally on computers instead of in physical boxes that are kept in certain places. When they use a search as an investigative method, law enforcement officials can gain access to a place and then seize items of interest – such as computers – for later analysis.

The ECtHR has recently started interpreting the right to privacy with regard to computer searches, i.e., when the search of a place results in computers being seized.[118] For example, in the case of *Prezhdarovi v. Bulgaria*, the individuals involved were suspected of using unlicensed software. Their computers were set up in a garage as part of a computer club.[119] In this case, the Bulgarian police conducted a search of the residence's garage without a judicial warrant. During this search, they seized computers that contained letters and other personal information about friends and clients of the suspects.[120] The ECtHR considered these investigative activities as an interference with the right to privacy as defined in art. 8 ECHR. In other case law with regard to computer searches, the ECtHR has explicitly noted that the search of a place and the seizure of computers amount to an interference with the right to respect for home and correspondence.[121] These interfer-

116 See, e.g., ECtHR 26 December 1992, *Niemietz v. Germany*, appl. no. 13710/88, § 26, ECtHR 25 February 1993, *Funke v. France*, appl. no. 10828/84, § 48.

117 See subsection 3.3.2.

118 See ECtHR 27 September 2005, *Petri Sallinen and Others v. Finland*, appl. no. 50882/99, § 71, ECtHR 7 October 2007, *Wieser and Bicos Beteiligungen GmbH v. Austria,* appl. no. 74336/01, § 45, ECtHR 3 July 2012, *Robathin v. Austria*, appl. no. 30457/06, § 51, ECtHR 14 March 2013, *Bernh Larsen Holding AS and Others v. Norway*, appl. no. 24117/08, § 105 and ECtHR 30 September 2014, *Prezhdarovi v. Bulgaria*, appl. no. 8429/05, § 41.

119 ECtHR 30 September 2014, *Prezhdarovi v. Bulgaria*, appl. no. 8429/05, § 12.

120 ECtHR 30 September 2014, *Prezhdarovi v. Bulgaria*, appl. no. 8429/05, § 21.

121 See, e.g., ECtHR 27 September 2005, *Petri Sallinen and Others v. Finland*, appl. no. 50882/99, ECtHR 7 October 2007, *Wieser and Bicos Beteiligungen GmbH v. Austria,* appl. no. 74336/01, ECtHR 3 July 2012, *Robathin v. Austria*, appl. no. 30457/06, ECtHR 14 March 2013, *Bernh Larsen Holding AS and Others v. Norway*, appl. no. 24117/08 and ECtHR 30 September 2014, *Prezhdarovi v. Bulgaria*, appl. no. 8429/05.

ences with the right to privacy can be considered as serious; more serious than, for instance, the surveillance by law enforcement officials of an individual in public. Considering the gravity of the privacy interference, more detailed regulations with specific procedural safeguards will be required for this investigative method. The required quality of the law for computer searches is further examined below.

Required quality of the law
It is emphasised here that the privacy interference that takes place when computers are seized and analysed is serious due to the large amounts of information that are nowadays stored on computers (cf. Groothuis & De Jong 2010, p. 280 and Conings & Oerlemans 2013, p. 26). The ECtHR requires the following quality of the law for computer searches.

In case law with regard to computer searches, the ECtHR has clarified that it strongly prefers the involvement of an investigative judge. For instance, in the case of *Prezhdarovi v. Bulgaria*, the court found it especially important that adequate judicial review was not available. Nevertheless, in the words of the ECtHR: *"the absence of a prior judicial warrant may be counterbalanced by the availability of a retrospective judicial review"*.[122] In *Prezhdarovi v. Bulgaria*, the ECtHR also pointed out that the scope of a search-and-seizure operation should be limited to relevant information.[123]

When evaluating the case law with regard to computer searches, in my view the essential safeguard that the ECtHR requires is a *"meaningful judicial scrutiny of the search and seizure"* of computers.[124] This safeguard can be interpreted as a requirement for authorisation of an investigative judge that is limited in scope to relevant information.

4.4.2 The right to privacy and the use of covert listening devices

The ECtHR has also made it clear in case law that using covert listening devices to intercept private communications amounts to an interference with the right to respect for private life.[125]

Gravity of the privacy interference
The ECtHR regards the privacy interference that takes place when covert listening devices are used as serious, similar to the privacy interference that takes place when communications are obtained through the interception of

122 ECtHR 30 September 2014, *Prezhdarovi v. Bulgaria*, appl. no. 8429/05, § 46. The ECtHR also noted in the case of *Petri Sallinen* (§ 89) that it was *"struck by the fact that there was no independent or judicial supervision."*

123 See ECtHR 30 September 2014, *Prezhdarovi v. Bulgaria*, appl. no. 8429/05, § 49. See also, e.g., ECtHR 3 July 2012, *Robathin v. Austria*, appl. no. 30457/06, § 48.

124 ECtHR 30 September 2014, *Prezhdarovi v. Bulgaria*, appl. no. 8429/05, § 50.

125 See, e.g., ECtHR 12 May 2000, *Khan v. The United Kingdom*, appl. no. 35394/97, § 25, ECtHR 31 May 2005, *Vetter v. France*, appl. no. 59842/00, and ECtHR 8 March 2011, *Goranova-Karaeneva v. Bulgaria*, appl. no. 12739/05, § 44.

communications.[126] The case law for the latter has already been examined in subsection 4.2.2 under D.

Required quality of the law
With regard to the quality of the law, the ECtHR specifically requires that the regulations that enable the interception of communications with covert listening devices are *particularly precise.* This is done to prevent an arbitrary governmental interference from taking place in the private lives of individuals.[127]

For example, in the case of *Khan v. The United Kingdom*, the ECtHR clarified that it requires that the law is *"sufficiently clear in its terms to give individuals an adequate indication as to the circumstances in which and the conditions on which public authorities are entitled to resort to such covert measures"*.[128] In this case, the investigative method was based on an internal guideline of the U.K. Home Office that authorised the investigative activities. The ECtHR made clear that it required statutory laws regulating the investigative method regarding the use of covert listening devices.[129] As such, the U.K. Home Office's internal guideline was not of sufficient quality.

In the case of *Goranova-Karaeneva v. Bulgaria*, the ECtHR further considered that the following four safeguards are appropriate for the use of covert listening devices: (1) a warrant describing the intended operation; (2) a restriction on the duration of the operation; (3) the possibility of a review to challenge the obtained evidence; and (4) the existence of procedures for preserving the integrity and confidentiality of the materials obtained through covert surveillance as well as for eventually destroying these materials.[130] With regard to the procedural safeguards for the regulation of the investigative method itself, (1) the warrant requirement and (2) a restriction on the duration of the investigative method are thus particularly important.

4.4.3 The right to privacy and hacking as an investigative method

This subsection analyses the gravity of the privacy interference when hacking is applied as an investigative method. It also considers whether the case law concerning the counterpart investigative methods examined above and their corresponding quality of the law requirements align with hacking as an investigative method.

---

126 See ECtHR 31 May 2005, *Vetter v. France*, appl. no. 59842/00, § 26 and ECtHR 8 March 2011, *Goranova-Karaeneva v. Bulgaria,* appl. no. 12739/05. Although case law does not explicitly states this, the required detailed regulations with specific procedural safeguards that are tested by the ECtHR indicates that the ECtHR views the privacy interference as serious.

127 See ECtHR 31 May 2005, *Vetter v. France*, appl. no. 59842/00, § 26.

128 ECtHR 12 May 2000, *Khan v. The United Kingdom*, appl. no. 35394/97, § 26.

129 ECtHR 12 May 2000, *Khan v. The United Kingdom*, appl. no. 35394/97, § 27. See also ECtHR 25 September 2001, *P.G. and J.H. v. The United Kingdom*, appl. no. 44787/98, § 38.

130 ECtHR 8 March 2011, *Goranova-Karaeneva v. Bulgaria,* appl. no. 12739/05, § 49-50.

Hacking as an investigative method is an umbrella term that encompasses different investigative methods that have in common that law enforcement officials *remotely access a computer system* (cf. Oerlemans 2011, p. 891). In this study, hacking as an investigative method comprises the following investigative methods: (A) network searches, (B) remote searches, and (C) the use of policeware on computers.[131] These methods are further examined below.

A Network searches

A network search is conducted when law enforcement officials are conducting a search of a place and find a computer that potentially contains evidence. In such a situation, law enforcement officials seize the computer and use it while it is still on, which enables them to gain access to interconnected devices and computers. As explained in subsection 2.4.3, a network search is also considered as a type of hacking as an investigative method in this study, because law enforcement officials can gain remote access to a computer system (of which the suspect is not necessarily aware) when a network search is performed. The investigative method is visualised in Figure 4.4. The reason Figure 4.4 is called a simplified model of a network search is that network searches can also take place in different places than a residence, such as inside an office and even inside a vehicle.

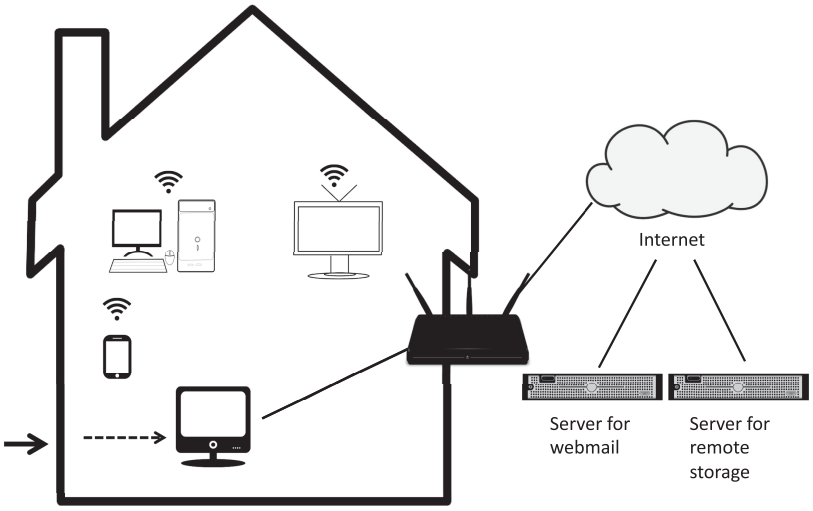

Figure 4.4: Simplified model of a network search.

Figure 4.4 illustrates how a network search is conducted at a certain place, such as a residence. Using a computer that is still on, law enforcement can use a network search as an investigative method to access the contents

131 See subsection 2.4.3.

stored on interconnected computers, such as an external hard disc that is shared with an internal network or an e-mail server that is used by a company but located elsewhere. Using a network search as an investigative method can also enable law enforcement officials to gain access to an individuals' webmail or online storage account when they seize a running computer (cf. Conings & Oerlemans 2013).[132] The prevalence of 'apps' on smartphones with accompanying login credentials and cloud services makes it possible for law enforcement officials to extract login credentials and use that information to subsequently collect evidence by performing a network search (insofar the smartphone is not encrypted).

Gravity of the privacy interference

Network searches and computer searches have important similarities as they are both conducted during the search of a place and involve analysing data stored on a computer. However, unlike a computer search, a network search also enables interconnected computers to be searched. Similar to regular computer searches, network searches also seriously interfere with the right to respect for home and correspondence as provided by art. 8(1) ECHR, with the difference that information can be obtained that is stored outside the location the initial search is conducted.

Alignment with the existing required quality of the law

The ECtHR requires detailed regulations for computer searches, (preferably) with the supervisory involvement of a judge who can authorise the search or conduct a retrospective judicial review. Since the gravity of the privacy interference is very similar for the investigative methods of computer and network searches, the quality of the law that is required aligns well for these investigative methods.

B Remote searches

During a remote search, law enforcement officials remotely access a computer that is located at a certain location. A remote search is different from a network search in that law enforcement officials do not 'physically' conduct computer searches at a certain place; it can instead be conducted 'virtually' from the convenience of a law enforcement official's desk. Remote searches are visualised in Figure 4.5.

132 Law enforcement officials can obtain login credentials from programs at the seized computer or from cookies to access certain web services. Login credentials can also be obtained through informants or voluntarily provided by a suspect.

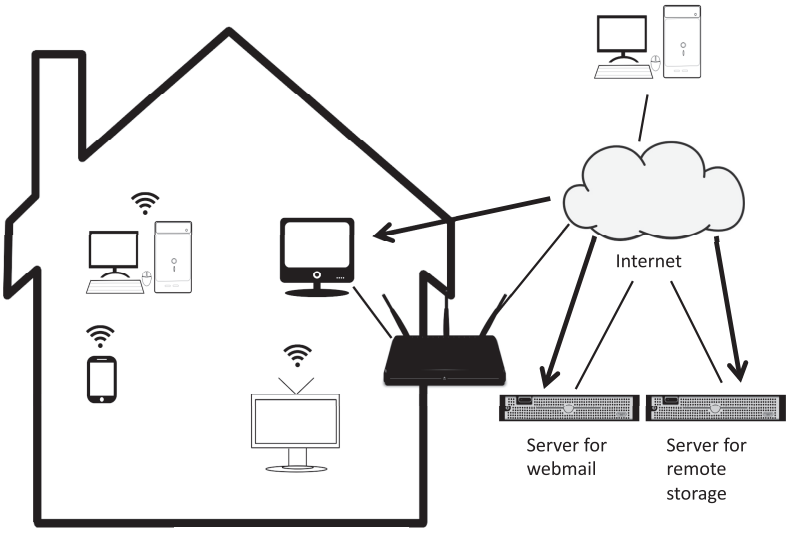

Figure 4.5: Simplified model of a remote search.

Figure 4.5 illustrates how a remote search distinguishes from computer searches and network searches. During a remote search, a computer is accessed remotely from a different computer through the Internet; not during a search at a place. An example of performing a remote search is when law enforcement officials log into a suspect's online account in order to search for information that is relevant to a criminal investigation.[133] The above model is simplified, because remote searches do not necessarily take place in computers located in the suspect's residence or in a suspect's webmail and online storage account.[134]

Gravity of the privacy interference

Remote searches clearly interfere with the involved individuals' right to respect for private life as meant in art. 8(1) ECHR (Oerlemans 2011, p. 898).[135] Based on the existing case law with regard to computer searches, it is expected that the investigative method will also interfere with the right to respect for home and correspondence.

The privacy interference that takes place during a remote search would be considered as serious by the ECtHR. During a remote search, law enforcement officials potentially gain access to sensitive information of individuals, such as photos, videos, and e-mails. I consider remote searches to be *more privacy intrusive* than computer searches, given that they are conducted

133 See also subsection 2.4.3 under B.

134 In addition, law enforcement officials will use anonymising services or techniques to obscure the origin of the hack.

135 See Groothuis & De Jong 2010, p. 280, Koning 2012, p. 49, and Koops et al. 2012b, p. 47.

covertly without presence of the suspect or other individuals. In contrast, the suspect is present when law enforcement officials physically search a place and seize a computer. In that situation, the suspect and perhaps even his lawyer can object to the seizure of certain data stored on computers. During a *remote* search, this is not an option.

Alignment with the existing required quality of the law
With regard to computer searches, in its case law the ECtHR prefers prior authorisation of an investigative judge to conduct the search. However, as argued above, remote searches should be considered more privacy intrusive than computer searches. For that reason, the required quality of the law for remote searches does not entirely align with the required quality of the law for regular computer searches.

The prior authorisation of an investigative judge should be regarded as a minimum requirement for remote searches. The ECtHR has repeatedly emphasised in other case law that investigative methods that are conducted covertly must be regulated in law in a 'particularly precise manner'.[136] Detailed procedures are required because applying the investigative methods in secret is accompanied by an increased risk of power being arbitrarily used, due to the diminished ability to control the investigative activity of a law enforcement authority.[137]

The required quality of the law for remote searches is thus likely to be (1) a detailed legal basis in statutory law and (2) prior authorisation from an investigative judge.

C The use of policeware
Before policeware can be utilised, law enforcement officials have to obtain remote access to a computer system that a suspect uses. The investigative method is visualised in Figure 4.6. The model of the use of policeware in Figure 4.6 is simplified, because law enforcement authorities will have to use their own ICT infrastructure to remain anonymous and exfiltrate the data from target computers in a secure manner. In addition, it is conceivable policeware is installed on different types of computers at any place (not only residences).

136 See ECtHR 29 June 2006, *Weber and Saravia v. Germany*, appl. no. 54934/00, § 93, ECtHR 1 July 2008, *Liberty and Others v. the United Kingdom*, appl. no. 58243/00, § 62, and ECtHR 2 September 2010, *Uzun v. Germany*, appl. no. 35623/05, § 61.

137 See, e.g., ECtHR 2 August 1984, *Malone v. The United Kingdom*, appl. no. 8691/79, § 67, ECtHR 24 April 1990, *Huvig v. France*, appl. no 11105/84, § 29, ECtHR 4 May 2000, *Rotaru v. Romania*, appl. no. 28341/95, § 55.

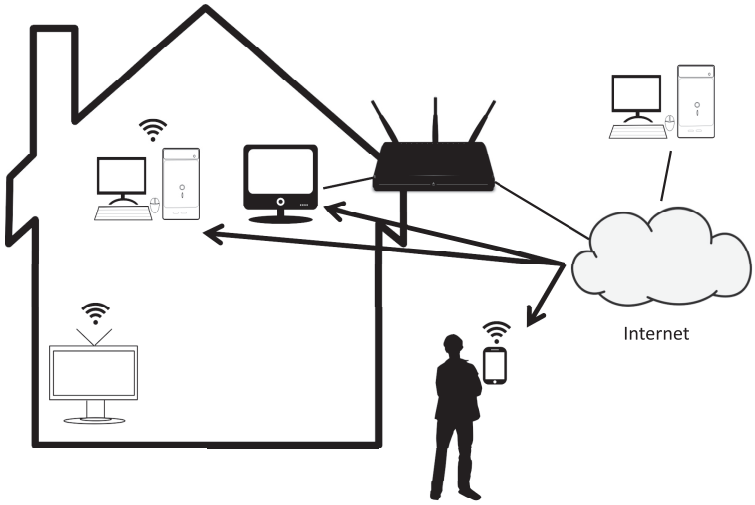

Figure 4.6: Simplified model for the use of policeware.

Figure 4.6 illustrates how law enforcement officials can remotely access any computer and install policeware regardless of their location. The use of policeware by law enforcement officials in criminal investigations interferes with the right to privacy in a different manner than network searches and remote searches. While these searches are focused on collecting certain information stored in a computer, policeware enables law enforcement officials *to monitor an individual's computer behaviours*. Policeware can enable law enforcement officials to take certain functions of a computer over for evidence-gathering purposes. For instance, they may be able to log keystrokes and turn a computer user's microphone on to intercept his communications. They can also take screen shots to see the activities of a computer user.[138]

Gravity of the privacy interference

The privacy interference that takes place when policeware is used is particularly serious. It can be placed at the far right of the scale of gravity for privacy interferences, given that the privacy interference is not restricted to looking at and copying private files (as is the case when a remote search is conducted). When policeware is used, law enforcement officials do not only gain covert remote access to a computer; they also *take over* the computer's functionalities. Essentially, law enforcement officials can 'spy' on a computer user's activities. This can take place quite literally by turning on a built-in camera without notifying the computer user. The use of policeware seriously interferes with the right with respect for private life, home, and correspondence as protected by art. 8 ECHR.

138 See also subsection 2.4.3 under B.

Alignment with the existing required quality of the law
The ECtHR already requires detailed regulations with strong procedural safeguards for the use of covert listening devices. Essentially, these safeguards consist of (1) a warrant requirement and (2) a restriction on the duration of the investigative method.[139] With regard to the required quality of the law, it is important to remember that in the last two decades the ECtHR has emphasised in its judgements with regard to the interception of (tele) communications that it is: *"essential to have clear, detailed rules on interception of telephone conversations, especially as the technology available for use is continually becoming more sophisticated"*.[140] This statement can also serve as a warning for States that detailed regulations will be required for the use of policeware as an investigative method.

The use of policeware with its many functionalities interferes with the right to privacy more intensely than when covert listening devices are utilised. Nevertheless, the same quality of the law appears appropriate, because the highest level of detail of regulations and procedural safeguards are reached. In that respect, the quality of the law for policeware aligns with the required quality of the law for covert listening devices. Considering the intrusiveness of the investigative method, it appears that legislatures should also critically assess which application of the use of policeware is still regarded as 'necessary in a democratic society'.

4.4.4 Desired quality of the law

This subsection determines the *desirable* quality of the law based on the gravity of the privacy interference that takes place when hacking is applied as an investigative method.

In general, hacking as investigative method allows law enforcement officials to access computers located anywhere in the world and gather potentially large and diverse amounts of information. The three types of hacking used as investigative methods all seriously interfere with the right to privacy. Therefore, a detailed basis in statutory law with strong procedural safeguards is required to regulate the digital investigative method.

However, the three relevant types of hacking as an investigative method interfere with the right to privacy in different ways. The detailed regulations with procedural safeguards should therefore be tailored to the specific investigative method. The desirable quality of the law for the identified types of hacking as investigative methods is discussed below.

---

139 See the analysis in subsection 4.4.2.

140 ECtHR 24 April 1990, *Kruslin v. France*, appl. no. 11801/85, § 33. See also ECtHR 24 April 1990, *Huvig v. France*, appl. no. 11105/84, § 32, ECtHR 25 March 1998, *Kopp v. Switzerland*, appl. no 13/1997/797/1000, § 72, ECtHR 30 July 1998, *Valenzuela Contreras v. Spain*, appl. no. 58/1997/842/1048, § 46, ECtHR 29 June 2006, *Weber and Saravia v. Germany*, appl. no. 54934/00, § 93 and ECtHR 4 December 2015, *Roman Zakharov v. Russia*, appl. no. 47143/06, § 229.

A Network searches

The use of a network search as an investigative method interferes with individuals' right to privacy in a similar manner to a computer search, as it also occurs in a place search during which computers are seized. The gravity of the privacy interference is considered serious and can be placed at the right end of the scale of gravity for privacy interferences. In recent case law with regard to computer searches, the ECtHR has made clear that it prefers the involvement of an investigative judge as a procedural safeguard.

Considering the gravity of the privacy interference that takes place when a network search is performed, I view a *detailed legal basis in statutory law* for the investigative method as desirable. As a procedural safeguard for the regulation of the investigative method, prior *authorisation of an investigative judge* is desirable. As part of the authorisation (warrant) to conduct a network search, the scope of the network search should be restricted in the request for the warrant.

B Remote searches

Remote searches interfere with the right to privacy in a more intrusive manner than network searches do. The reason is that remote searches are conducted covertly, whereas computer searches are conducted in the presence of the suspect. The covert use of this intrusive investigative method is accompanied by a risk of an arbitrary use of governmental power.

The privacy interference that takes place when remote searches are conducted is therefore considered particularly serious and placed on the far (right) end on the scale of gravity for privacy interferences. For that reason, a *detailed legal basis in statutory law* is in my view appropriate for the regulation of this investigative method. In addition, prior *authorisation of an investigative judge* is the desirable procedural safeguard. As part of the authorisation (warrant) to conduct a remote search, the scope and duration of the remote search should be restricted in the warrant.

C The use of policeware

The use of policeware can be considered the most privacy intrusive investigative method that is examined in this study. Policeware allows law enforcement officials to monitor the computer behaviours of individuals by taking over the functionalities of a computer system, which then enables them to 'spy' on that computer user's activities.

In this study, the use of policeware is placed on the farthest right of the scale of gravity for privacy interferences. Considering the intrusiveness of this investigative method, it should have a *detailed legal basis in statutory law* to prevent arbitrary governmental interferences in the private lives of the individuals involved. Based on case law with regard to computer searches and the use of covert listening devices by law enforcement authorities, I consider (1) prior *authorisation of an investigative judge* to use of policeware and (2) a *restriction on the duration and functionalities* of the use of policeware as desirable procedural safeguards.

4.5 Chapter conclusion

The aim of this chapter was to identify the desirable quality of the law based on art. 8 ECHR for the regulation of the identified digital investigative methods (RQ 3). To answer RQ 3, the gravity of the privacy interference that takes place when the identified digital investigative methods are applied was examined and the accompanying quality of the law was formulated.

The first step in doing so was to analyse case law concerning similar investigative methods in order to identify the gravity of the privacy interference and accompanying quality of the law that the ECtHR requires in relation to those non-digital counterparts. This provided a basis for comparison with digital investigative methods.

As second step, the digital investigative methods were examined in detail to determine how they interfere with the right to privacy as defined in art. 8 ECHR. Whether the required quality of the law of the counterpart investigative methods aligns with the digital investigative methods was also analysed. The analysis showed that the privacy interferences caused by the digital investigative methods of (1) the gathering of publicly available online information, (2) the issuing of data production orders to online service providers, and (3) hacking as an investigative method, (which have not been examined in case law of the ECtHR) significantly differ from those caused by their non-digital counterparts that *have* been examined in case law by the ECtHR. Generally, the amount and diversity of information that can be processed when these digital investigative methods are applied significantly affects the gravity of the privacy interference. In my view, only the quality of the law requirements developed in case law for undercover investigative methods already aligns with the quality of the law requirements that are appropriate for the application of online undercover investigative methods.

As a third step, the results of the analysis conducted in the second step were used to determine the desirable quality of the law for the investigative methods.

Summary of the gravity of the privacy interferences and the desired quality of law
The result of the analysis that was conducted in sections 4.1 to 4.4 is presented in Table 4.1. This table provides an overview of the gravity of the privacy interferences that take place when each of the identified digital investigative methods is applied and the corresponding recommended desirable quality of the law for regulating the identified digital investigative methods.

Investigative method	Gravity of the privacy interference	Desirable level of detail for the regulations	Desirable procedural safeguards
Gathering publicly available online information:			
A. Manual gathering of information.	A. Minor interference.	A. General legal basis in law may suffice.	A. None (although data protection regulations apply).
B. Automated gathering of information.	B. More serious interference.	B. Detailed legal basis in law in statutory law or public guidelines.	B. None (although data protection regulations apply).
C. Observation of online behaviours of individuals.	C. Minor interference.	C. Detailed legal basis in statutory law or public guidelines.	C. None (although data protection regulations apply).
Issuing data production orders:			
A. Subscriber data.	A. Minor interference.	A. Detailed legal basis in statutory law.	A. No specific procedural safeguards required.
B. Traffic data.	B. Serious interference.	B. Detailed legal basis in statutory law.	B. Authorisation from an investigative judge.
C. Other data.	C. Serious interference.	C. Detailed legal basis in statutory law.	C. Authorisation from an investigative judge.
D. Content data.	D. Particularly serious interference.	D. Detailed legal basis in statutory law.	D. Authorisation from an investigative judge.
Applying undercover investigative methods:			
A. Pseudo-purchases.	A. Minor interference.	A. Detailed legal basis in statutory law.	A. Supervision by a public prosecutor.
B. Online undercover interactions with individuals.	B. Serious interference.	B. Detailed legal basis in statutory law.	B. Supervision by an investigative judge.
C. Online infiltration operations.	C. Serious interference and increased risks regarding the integrity of investigations.	C. Detailed legal basis in statutory law.	C. Supervision by an investigative judge.
Performing hacking as an investigative method:			
A. Network searches.	A. Serious interference.	A. Detailed regulations in statutory law.	A. Authorisation from an investigative judge.
B. Remote searches.	B. Particularly serious interference.	B. Detailed regulations in statutory law.	B. Authorisation from an investigative judge.
C. The use of policeware.	C. Particularly serious interference.	C. Detailed regulations in statutory law.	C. Authorisation from an investigative judge and a restriction of the duration and functionalities of the use of policeware.

Table 4.1: Overview of the gravity of the privacy interferences caused by the identified digital investigative methods and the corresponding recommended desirable quality of the law.