Investigating cybercrime

Oerlemans, J.J.

3 Normative requirements for investigative methods

The aim of this chapter is to answer the second research question (RQ 2): *Which normative requirements can be derived from art. 8 ECHR for the regulation of investigative methods?* The chapter is brief, as it intends only to provide a general overview of the normative requirements that apply for the regulation of investigative methods in domestic law.

To answer RQ 2, the relation between the right to privacy as defined in art. 8 ECHR and the regulation of investigative methods is analysed. Art. 8 ECHR provides for an overarching legal framework by imposing certain normative requirements for the regulation of investigative methods in the domestic laws of contracting States to the ECHR. These normative requirements are thus relevant for all contracting States to the ECHR.

The structure of this chapter is as follows. Section 3.1 analyses the scope of protection of the right to privacy as articulated in art. 8 ECHR. In section 3.2, the text of this article is examined to determine which conditions apply to legitimise privacy interferences caused by the use of investigative methods by law enforcement officials. As announced in chapter 1, although all aspects of art. 8 ECHR will be discussed, the focus of this study is on the requirements in this provision that determine how investigative methods should be *regulated* by law. The emphasis of the examination will thus lie in the examination of those aspects of art. 8 ECHR. This examination then serves as the basis for deriving the normative requirements for the regulation of investigative methods. Again, as explained in chapter 1, art. 8 ECHR and the accompanying case law of the ECtHR currently are not specifically oriented on 'the digital world', with case law on the relationship between treaty provisions and digital interferences being sparse. The normative framework examined in this chapter is thus general and mainly derived from case law concerning non-digital interferences. The requirements for digital interferences will be extrapolated from this framework and, in chapter 4, applied to digital investigations methods. The regulations in Dutch law upon which digital investigative methods are based in practice will be tested against these requirements in chapters 5 to 8. In section 3.3, the concept of 'the dynamic interpretation of the ECHR' that the ECtHR uses to interpret the convention rights is examined. In this light, the importance that art. 8 ECHR may have for the regulation of digital investigative methods in the (near) future is also considered. Finally, section 3.4 presents a summary of the chapter's findings.

3.1 The scope of protection under art. 8 ECHR

Art. 8 ECHR reads as follows:

"*1. Everyone has the right to respect for his private and family life, his home and his correspondence.*

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

Based on the text above, the right to privacy protects the following four aspects: (1) the right to respect for private life, (2) the right to respect for family life, (3) the right to respect for the home, and (4) the right to respect for correspondence. In a criminal investigation, the use of classical investigative methods, such as a house search and the interception of correspondence, interfere specifically with the right to respect for a *home* and *correspondence*. More novel investigative methods, such as the use of closed-circuit television cameras (hereinafter CCTV) or GPS beacons for surveillance purposes, interfere with the – more broadly formulated – *right to respect for private life* of art. 8(1) ECHR.[1] In its case law, the ECtHR has expanded the protection of art. 8 ECHR to encompass new investigative methods (cf. Ölçer 2008, p. 255).

The ECtHR deliberately does not provide an exhaustive definition of the right to respect for private life.[2] This allows the ECtHR to recognize and include new (types of) privacy interferences and interpret the right to privacy dynamically as a fundamental right. The case law shows the flexibility of art. 8 ECHR in light of both the development and use of new technologies in criminal investigations.[3]

1 See, e.g., ECtHR 28 January 2003, *Peck v. The United Kingdom*, no. 44647/98, § 57, 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: "*Article 8 is not limited to the protection of an "inner circle" in which the individual may live his own personal life as he chooses and to exclude therefrom entirely the outside world not encompassed within that circle. It also protects the right to establish and develop relationships with other human beings and the outside world. Private life may even include activities of a professional or business nature (…) There is, therefore, a zone of interaction of a person with others, even in a public context, which may fall within the scope of "private life"* (...)"

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

3 See further section 3.3 with regard to the dynamic interpretation of the ECHR.

Negative and positive obligations

The ECtHR interprets art. 8 ECHR (and other convention rights) in such a way that both 'negative' and 'positive' obligations follow from the right to privacy. Negative obligations require a State to refrain from interfering with convention rights, unless they can be legitimatised under the conditions stipulated in those convention rights. Positive obligations require a State to take the steps necessary to adopt reasonable and suitable measures to protect the rights of the individual (cf. Akandji-Kombe 2007, p. 7). The text of art. 8 ECHR itself suggests that only negative obligations follow from that article, as it states "there shall be no interference by a public authority with the right to privacy", except when the conditions stipulated in art. 8(2) ECHR are met. Positive obligations based on art. 8 ECHR are therefore an implicit construction of a convention right by the ECtHR itself. In the context of (digital) investigative methods, case law with regard to positive obligations that follow from art. 8 ECHR is scarce.

However, the case of *K.U. v. Finland* is a noteworthy exception. In this case, the ECtHR determined that Finland had a 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.[4] The case of *K.U. v. Finland* involved a 12-year-old child whose picture and personal information was abused by an individual: the suspect used the child's information to place advertisements on the Internet stating that the minor wanted to explore sexual relationships. Paedophiles subsequently harassed the child. Finnish law enforcement officials started an investigation but were unable to obtain subscriber data from the online forum provider about the user who had placed the advertisement.[5] The ECtHR did not accept this situation and decided that States have a positive obligation to enable law enforcement authorities to obtain data from online service providers in order to identify internet users based on their IP address. The ECtHR stated that:

"*Although freedom of expression and confidentiality of communications are primary considerations and users of telecommunications and Internet services must have a guarantee that their own privacy and freedom of expression will be respected, such a guarantee cannot be absolute and must yield on occasion to other legitimate imperatives, such as the prevention of disorder or crime or the protection of the rights and freedoms of others.*"[6]

4 ECtHR 2 December 2008, *K.U. v. Finland*, appl. no. 2872/02.

5 The reason why law enforcement officials were unable to obtain subscriber data was that there was no investigative power available in Finnish law that provided law enforcement authorities with the authority to obtain subscriber data.

6 ECtHR 2 December 2008, *K.U. v. Finland*, appl. no. 2872/02, § 49.

In other words, the right to privacy under art. 8 ECHR can also lead to an obligation to protect individuals from privacy interferences by other individuals. For the purposes of this study, positive obligations such as those determined in *K.U. v. Finland* serve to confirm the necessity of the proper regulation of digital investigative methods in the current reality. At this time, computers and the Internet play a prominent role in society and creates a platform for crime, against which citizens must be protected. With the duty to protect in this positive sense, States must ensure that domestic law enforcement has the ability to apply the digital investigative methods necessary to an investigation. The negative duty to interfere only legitimately, brings with it that the necessary methods must be regulated in a manner compliant with art. 8 ECHR.

Negative and positive obligations can further be relevant in the context of another treaty concept invoked by the ECtHR, namely extraterritorial obligations. Based on these obligations, States can be held to treaty compliance even outside their own sovereign territory. Case law concerning obligations of States to respect treaty requirements in their actions abroad has been substantially developed.[7] In theory, it could be envisaged that a duty may exist for member States to protect their citizens against interferences on their own territory – through the Internet – by foreign agents acting from other jurisdictions, in or outside of Europe. Case law in this sense is, however, unknown to the author, so that it cannot be contended that such obligations can currently be based on the ECHR. This is not to say however that obligations such as these do not flow forth from rule of law requirements, such as those requiring legal certainty. Such obligations can be important in the context of the cross-border unilateral application of digital investigative methods that can interfere with the right to privacy of individuals who are located in a different State. This topic is revisited in chapter 9.

7 See, e.g., ECtHR 12 December 2001, *Banković and Others v. Belgium and Others*, appl. no. 52207/99, ECtHR 16 November 2004, *Issa and Others v. Turkey*, appl. no. 31821/96, ECtHR 12 May 2005, *Öcalan v. Turkey*, appl. no. 46221/99, ECtHR 7 July 2011, *Al-Skeini and others v. The United Kingdom*, appl. no. 55721/07, and ECtHR 27 October 2011, *Stojkovic v. Belgium and France*, *EHRC* 2012/23, m.nt. F.P. Ölçer. It is important to note that discussion exist about the extent to which the ECHR applies extraterritorially. See with regard to this discussion, e.g., De Schutter 2006 and King 2009. However, when digital investigative methods are applied by law enforcement officials from the investigating State, it is in my view clear that the ECHR protects the citizens that are affected by the application. It is irrelevant whether those individuals live on the territory of the investigating State or outside the territory of the investigating State. See Milanovic (2015, p. 97-99) for a similar reasoning in the context of (digital) mass surveillance measures.

3.2 Conditions to legitimise privacy interferences

When investigative methods are applied, an interference with the right to privacy may take place.[8] Art. 8(2) ECHR states that such a privacy interference is legitimate when the following three conditions are met: a legitimate aim is available (see 3.2.1), the interference is 'in accordance with the law' (see 3.2.2), and the interference is 'necessary in a democratic society' (see 3.2.3). In subsection 3.2.4, the relationship between the gravity of the privacy interference and the quality of the law is further discussed by explaining the workings of the 'scale of gravity' for privacy interferences.

Although all three conditions can be pertinent to the evaluation of compliance of national law with art. 8 ECHR, the second condition being 'in accordance with the law', is particularly important for the regulation of investigative methods *in abstracto*. As this last aspect is the focus of the study, the second requirement will be examined thoroughly. In contrast, the other two conditions for legitimising privacy interferences under art. 8 ECHR, namely having a legitimate aim and being necessary in a democratic society, do not play a central role in this research. It is not to say that they are never relevant. The condition that privacy interferences must be necessary in a democratic society can be important in particular, as it requires a balance between privacy interferences and legitimate aims. The test whether an interference is necessary in a democratic society is generally conducted *in concreto*, based on the facts of a specific case, rather than when regulating the investigative methods *in abstracto* in legislation. However, for particularly intrusive investigative methods, such as those that involve mass surveillance or hacking as an investigative method, the 'necessary in a democratic society' condition may play an important role.[9] Zuiderveen Borgesius and Arnbak (2015) rightfully pose the question whether it is desirable that all privacy interferences can be legitimised by 'proceduralising' them in legalisation. Legislatures should also take the scope of an investigative method into account and decide at which point an investigative method can no longer be considered 'necessary in a democratic society'. The three conditions for legitimising privacy interferences are further examined below.

---

8 It is important to realise that not necessarily all investigative methods interfere with the right to privacy as defined in art. 8 ECHR. For example, the ECtHR has considered that no interference with the privacy takes place when law enforcement officials take a photo of an individual at a public demonstration. See ECtHR 25 September 2001, *P.G. and J.H. v The United Kingdom*, appl. no. 44787/98, § 58 with reference to ECtHR 31 January 1995, *Friedl v. Austria*, § 51-52.

9 It is possible the ECtHR will decide on the legitimacy of these mass surveillance measures in one of the following cases: ECtHR 4 September 2013, *Big Brother Watch and Others v. The United Kingdom,* appl. no. 58170/13, ECtHR 11 September 2014, *Bureau of Investigative Journalism and Alice Ross v. The United Kingdom,* appl. no. 62322/14, and ECtHR 20 May 2015, *Human Rights Organisations v. The United Kingdom*, appl. no. 24960/15. In the same sense, the (total) absence of a legitimate aim behind a legal provision of an investigative method may also offend the requirements of art. 8 ECHR.

3.2.1 A legitimate aim is available

The first condition is that *a legitimate aim* must be available when investigative methods are used that interfere with the right to privacy. In the context of criminal investigations, the legitimate is often 'the prevention of disorder or crime' (cf. Krabbe, p. 160 in: Harteveld 2004). In practice, States rarely encounter problems in arguing and demonstrating that a 'legitimate aim is pursued' when investigative methods are used that interfere with the right to privacy in criminal investigations. Instead, the ECtHR often focuses on the other two conditions, i.e., whether the interferences are 'in accordance with the law' and 'necessary in a democratic society', to determine whether a particular privacy interference is legitimate (cf. Gerards 2011, p. 133).

3.2.2 In accordance with the law

The second condition is that interferences with the right to privacy that are caused by the use of investigative methods are '*in accordance with the law*'. The ECtHR uses a broad interpretation of the term 'law'. According to the ECtHR, the law concerns both (a) written law, including published guidelines for the application of investigative methods, and (b) unwritten law, such as settled case law.[10]

In its case law, the ECtHR has stipulated that the regulation of investigative methods must fulfil the following three requirements in order to be considered 'in accordance with the law': (1) *accessibility*, (2) *foreseeability*, and (3) a certain *quality of the law*.[11] In this study, these three requirements are thus considered as the *normative requirements* for the regulation of investigative methods based on art. 8 ECHR. They are further examined below.

A Accessibility

The first requirement for the regulation of investigative methods is 'accessibility', which means that the law gives an 'adequate indication' concerning which regulations apply for using investigative methods in a given case (cf. Greer 1997, p. 10).[12] The applicable statutory law, case law, or guidelines for

10 See, e.g., ECtHR 24 April 1990, *Kruslin v. France*, appl. no. 11801/85, §28 and *Huvig v. France*, app. no 11105/84, § 29 and ECtHR 2 August 1984, *Malone v. The United Kingdom*, appl. no. 8691/79, §66. See also ECtHR 26 April 1979, *Sunday Times v. The United Kingdom*, appl. no. 6538/74, § 49, and ECtHR 12 May 2000, *Khan v. The United Kingdom*, appl. no. 35394/97, § 27.

11 It should be noted that in case law, the ECtHR does not always strictly divide these three requirements in this order. In certain cases, the ECtHR only tests the foreseeability of the law, which is then considered as part of the required quality of the law. See, e.g., ECtHR 2 September 2010, *Uzun v. Germany*, appl. no. 35623/05, § 60.

12 See, e.g., ECtHR 26 April 1979, *Sunday Times v. The United Kingdom*, appl. no. 6538/74, § 49, ECtHR 12 May 2000, *Khan v. The United Kingdom*, appl. no. 35394/97, § 26, ECtHR 3 April 2007, *Copland v. The United Kingdom*, appl. no. 62617/00, § 46, and ECtHR 10 March 2009, *Bykov v. Russia*, appl. no. 4378/02, § 76.

a certain investigative method must be publicly available. Secret guidelines set by law enforcement authorities in relation to the application of investigative methods are thus not considered as accessible law.[13]

B Foreseeability

The second requirement for the regulation of investigative methods is 'foreseeability', which means that the law must indicate with sufficient clarity (1) the scope of the power conferred on the competent authorities and (2) the manner in which the investigative method is exercised (cf. Gerards 2011, p. 128). In addition to written law and unwritten (case) law, relevant preparatory work for the legislation and publicly available guidelines are also taken into consideration in order to determine whether the law is sufficiently foreseeable in light of art. 8 ECHR (see Ölçer 2008, p. 292).[14]

The ECtHR has explained multiple times that it considers the 'essential object of protection' of art. 8 ECHR to "*protect the individual against arbitrary action by the public authorities*".[15] This is an important statement in relation to the foreseeability requirement in art. 8(2) ECHR. The foreseeability requirement stipulates that both (1) the scope of the power conferred upon the competent authorities and (2) the manner in which the investigative method is exercised must be clear to the individuals involved. If these two conditions are not met, individuals are subjected to an arbitrary interference by governmental authorities in their private lives. The foreseeability requirement in art. 8 ECHR thus offers *legal certainty* to the individuals who are involved in criminal investigations (cf. Krabbe, p. 165 in: Harteveld 2004). Legal certainty about the conditions and the manner in which investigative methods are applied is in turn a key element of the rule of law.[16] By imposing legal constraints on governmental officials in their activities, an uncontrolled and arbitrary application of coercion by the government is avoided. That is not to say that legality is the only requirement of the rule of law.[17]

13 See, e.g., ECtHR 23 September 1998, *Petra v. Romania*, appl. no. 27273/95, § 38.

14 See, e.g., ECtHR 24 March 1988, *Olsson v. Sweden*, appl. no. 10465/83, §62 and ECtHR 24 May 1988, *Müller and Others v. Switzerland*, appl. no. 10737/84, §29.

15 See, e.g., ECtHR 26 December 1992, *Niemietz v. Germany*, appl. no. 13710/88, § 31 and ECtHR 27 October 1994, *Kroon and Others v. The Netherlands*, appl. no. 18535/91, § 31.

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

17 Tamanaha (2004) distinguishes a formal definition of the rule of law and a substantive definition of the rule of law. In the formal definition, governmental officials and citizens are bound by and act consistent with the law. In the substantive definition, fundamental rights, democracy, and concepts such as 'human dignity' are also taken into account. After all, the fact that governmental officials are bound by the law, does not say anything about the content of the law. See for an extensive analysis, e.g., Tamanha 2004, p. 91-101.

C Quality of the law

The third requirement for the regulation of investigative methods is a sufficient 'quality of the law'. The ECtHR has clarified in its case law that investigative methods that interfere with fundamental rights cannot be expressed in a legal framework 'in terms of an unfettered power' that is conferred on law enforcement authorities.[18] The ECtHR can subsequently specify (1) the level of detail of the regulations and (2) the minimum procedural safeguards that must be implemented in the domestic legal frameworks of contracting States to the ECHR (cf. Gerards 2011, p. 129). These detailed regulations and procedural safeguards in domestic law aim to counterbalance the risk of abuse of power by the government (cf. Krabbe, p. 167 in: Harteveld 2004).[19]

3.2.3 Necessary in a democratic society

As a third condition for legitimising privacy interferences, art. 8(2) ECHR requires that the legitimate aim being pursued by a government when applying investigative methods that interfere with the right to privacy of citizens must be '*necessary in democratic society*'. To determine whether this condition is met, the ECtHR tests whether the inference with the right to privacy (1) corresponds to a 'pressing social need' and (2) is 'proportionate to the legitimate aim pursued'.[20] In doing so, the ECtHR essentially examines whether a fair balance is met between (1) the interference with the right to privacy of the involved individual on the one hand and (2) the necessity to use the privacy infringing investigative method on the other hand (see Gerards 2011, p. 140).

The ECtHR applies the test whether application of the investigation is 'necessary in a democratic society' *in concreto*. That means that the ECtHR takes into consideration the circumstances of the case at hand to determine if the privacy infringing measure of the government is proportionate to the legitimate aim pursued (cf. Ölçer 2008, p. 304). Hirsch Ballin (2012, p. 113) points out that the requirement of 'necessary in a democratic society' also implies an assessment of (1) the proportionality principle and (2) the subsidiarity principle. Law enforcement officials must thus continuously assess

18 See, e.g., ECtHR 2 August 1984, *Malone v. The United Kingdom*, appl. no. 8691/79, § 66-68, ECtHR 4 May 2000, *Rotaru v. Romania*, appl. no. 28341/95, § 55, ECtHR 11 October 2007, *Glas Nadezhda EOOD* and *Anatoliy Elenkov v. Bulgaria*, appl. no. 14134/02, § 46, ECtHR 12 June 2008, *Vlasov v. Russia*, appl. no. 78146/01, § 125.

19 For instance, the ECtHR emphasised in the case of *Malone v. The United Kingdom* that: *"the phrase "in accordance with the law" does not merely refer back to domestic law but also relates to the quality of the law, requiring it to be compatible with the rule of law, which is expressly mentioned in the preamble to the Convention"*. See ECtHR 2 August 1984, *Malone v. The United Kingdom*, app. no. 8691/79, §68.

20 See, e.g., ECtHR 26 April 1979, *Sunday Times v. The United Kingdom*, appl. no. 6538/74, § 67. ECtHR 25 March 1983, *Silver and others v. The United Kingdom*, appl. nos. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, and 7136/75, §97 and ECHR 26 March 1987, *Leander v. Sweden*, appl. no. 9248/81, §81.

whether the benefit of the application of an investigative method is reasonably balanced with the interference with fundamental rights that may take place (which reflects the proportionality principle) and whether there are no other – less infringing – investigative methods available to gather evidence (which reflects the subsidiarity principle) (cf. Hirsch Ballin 2012, p. 57). As already emphasised in the introduction to this section, this study focuses on whether the regulations of investigative methods are 'in accordance with the law' *in abstracto*. This study does not explore the balancing act described above for the identified digital investigative methods.[21]

The ECtHR typically grants contracting States to the ECHR a 'margin of appreciation' when evaluating whether a privacy infringing measure is necessary in a democratic society.[22] The term 'margin of appreciation' refers to the discretion that the ECtHR is willing to grant national authorities in fulfilling their obligations under the ECHR (see Greer 2000, p. 5). However, the more serious the privacy interferences caused by an investigative method, the more procedural safeguards the ECtHR will prescribe to contracting States to counterbalance the risk of abuse of power by governmental authorities. In such a case, contracting States to the ECtHR have a smaller margin of appreciation in regulating investigative methods that interfere with art. 8 ECHR.

3.2.4 The scale of gravity for privacy interferences

From the case law of the ECtHR, a 'scale of gravity' can be identified regarding the privacy interferences that are caused by the use of investigative methods (see Ölçer 2008, p. 293). Depending on the gravity of the privacy interference that takes place, the ECtHR requires more or less detailed law and procedural safeguards for regulating the investigative methods.[23] The working of this 'scale of gravity for privacy interferences' is illustrated in the Figure 3.1.

21 See also the introduction to section 3.2.

22 See, e.g., ECtHR 25 March 1983, *Silver and others v. The United Kingdom*, appl. nos. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, and 7136/75, §97 and ECtHR 4 December 2008, *S. and Marper v. The United Kingdom*, appl. nos. 30562/04 and 30566/04, §102.

23 See, e.g., ECtHR 25 September 2001, *P.G. and J.H. v. The United Kingdom*, appl. no. 44787/98, §46, ECtHR 4 December 2008, *S. and Marper v. The United Kingdom*, appl. nos. 30562/04 and 30566/04, §96, and ECtHR 26 October 2000, *Hasan and Chaush v. Bulgaria [GC]*, appl. no. 30985/96, §84.

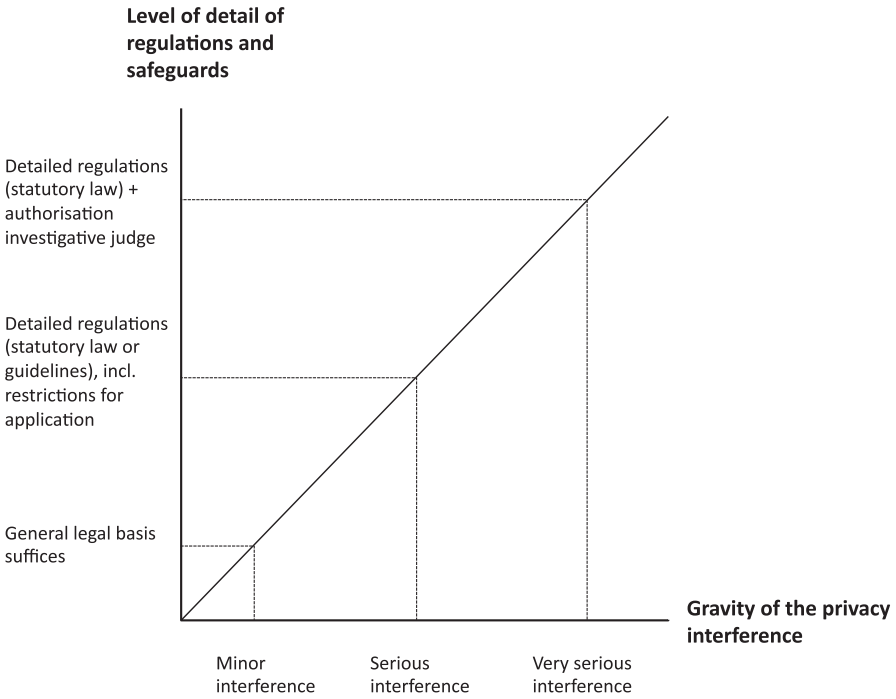

Figure 3.1: Workings of the scale of gravity for privacy interferences.

Figure 3.1 shows how investigative methods that interfere more heavily in the right to privacy generally require a more detailed legal basis in law with more procedural safeguards to protect the right to privacy of the individuals involved (cf. Krabbe, p. 166 in: Harteveld et al. 2004, Ölçer 2008, p. 290, and Gerards 2011, p. 129-130).[24] By requiring regulations that are more detailed with procedural safeguards for investigative methods that interfere with the right to privacy in a serious manner, the ECtHR aims to reduce the risk of abuse of governmental power.[25] The level of detail of the law and procedural safeguards, i.e., the quality of the law that is required for regulating the investigative methods thus depends on the gravity of the privacy interference that occurs when an investigative method is applied. From case law, the following level of detail and procedural safeguards for regulations are distinguished: (1) a general legal basis, (2) detailed regulations in statutory law or guidelines with restrictions for the investigative methods, or

24 The scale of gravity for privacy interferences is in this case presented on a 45 degree angle. However, the scale solely serves to illustrate a legal mechanism. It is not contented the privacy interference can be exactly measured and there is a linear relationship between the gravity of the privacy interference and the required quality of the law.

25 See, e.g., ECtHR 1 July 2008, *Liberty and Others v. The United Kingdom*, appl. no. 58243/00, § 62, ECtHR 2 September 2010, *Uzun v. Germany*, appl. no. 35623/05, § 61, and ECtHR 21 June 2011, *Shimovolos v. Russia*, appl. no. 30194/09, § 68

(3) detailed regulations in statutory law with the procedural safeguard of authorisation of an investigative judge.

To illustrate how this scale of gravity is used in case law, two examples of investigative methods that interfere with the right to privacy are presented below: one that interferes in a minor manner and one that interferes more seriously.

Minor interference

The *visual surveillance of an individual in a public place* is an investigative method that interferes with an individual's right to privacy in only a minor manner or, in certain circumstances, not at all.[26] An interference with the right to privacy does take place when personal information that is obtained through public surveillance measures is also *stored in police systems*. 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).[27] However, the investigative method of *the surveillance* of the behaviours of individuals *in public places* itself, does not – or only in a minor manner – interfere with the right to privacy in art. 8 ECHR. With regard to quality of the law, the ECtHR does not state that detailed regulations with procedural safeguards must be implemented in the domestic legal frameworks of member states to protect individuals from this type of governmental interference, even when the recorded information is stored in a police system. A general legal basis that authorises law enforcement officials to use visual surveillance as an investigative method may therefore be sufficient.[28]

Serious interference

The *interception of communications* is an investigative method that seriously interferes with the right to privacy of individuals. This investigative method can be placed at the far right of the scale of gravity for privacy interferences.[29] In relation to the interception of communications, the ECtHR has noted repeatedly that:

26 ECtHR 25 September 2001, *P.G. and J.H. v. The United Kingdom*, appl. no. 44787/98, § 58 with reference to ECtHR 31 January 1995, *Friedl v. Austria*, § 51-52.

27 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."*

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

29 See, e.g., ECtHR 24 April 1990, *Kruslin v. France*, appl. no. 11801/85 and *Huvig v. France*, app. no 11105/84, ECtHR 12 May 2000, *Khan v. The United Kingdom*, appl. no. 35394/97, and ECtHR 4 December 2015, *Roman Zakharov v. Russia*, appl. no. 47143/06.

"In view of the risk of abuse intrinsic to any system of secret surveillance, such measures must be based on a law that is particularly precise, especially as the technology available for use is continually becoming more sophisticated."[30]

Vis-à-vis the interception of communications, the ECtHR requires – as part of the required 'quality of the law' – that (1) the law is particularly precise and (2) procedural safeguards are implemented within legislation to protect the right to privacy of the individuals involved.[31] More particularly to the latter requirement, the ECtHR considers it important that the investigative method or surveillance measure is authorised by an independent authority, preferably a judge.[32]

It is important to understand the workings of the scale of gravity for privacy interferences and its relation with the regulation of digital investigative methods. Distinct digital investigative methods interfere with the right to privacy as articulated in art. 8 ECHR in their own manner. The ECtHR will thus place the privacy interference that takes place somewhere on the scale of gravity in order to determine the appropriate level of detail and procedural safeguards for each distinct investigative method. The requirements for regulating the identified digital investigative method are further examined in chapter 4.

3.3 Dynamic interpretation of the ECHR

Even though the ECHR was established and concluded within the framework of the Council of Europe in 1950, the treaty is by no means outdated. The reason is that the ECtHR uses '*dynamic, evolutive interpretation*', allowing it to take present-day standards and conditions into consideration. The ECtHR has repeatedly emphasised in its case law that the ECHR is *"a living instrument which should be interpreted according to present-day conditions"* (cf. Lawson & Schermers 1999, p. 50).[33] In subsection 3.3.1, two examples of the dynamic interpretation of convention rights are provided. Section 3.3.2

30 See, e.g., ECtHR 1 July 2008, *Liberty and Others v. The United Kingdom*, appl. no. 58243/00, § 62, ECtHR 2 September 2010, *Uzun v. Germany*, appl. no. 35623/05, § 61, and ECtHR 21 June 2011, *Shimovolos v. Russia*, appl. no. 30194/09, § 68.

31 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.

32 See most notably ECtHR 4 December 2015, *Roman Zakharov v. Russia*, appl. no. 47143/06, § 257-267 with reference to ECtHR 26 April 2007, *Dumitru Popescu v. Romania* (no. 2), appl. no. 71525/01, § 71.

33 Emphasis added by the author. The first case in which the ECtHR mentioned that the ECHR should be seen as a living instrument was in ECtHR, 25 April 1978, *Tyrer v. The United Kingdom*, appl. no. 5856/72 § 31. As Letsas (2013, p. 108) points out, the ECtHR 'very rarely' inquires what was thought be acceptable conduct when the ECHR was drafted or what specific rights the drafters of the ECHR intended to protect.

discusses the relevance of the interpretation method for the regulation of digital investigative methods.

3.3.1 Two examples of the dynamic interpretation of convention rights

The dynamic, evolutive interpretation of the convention rights articulated in the ECHR is clearly visible in case law. Two examples are provided to illustrate the evolutive interpretation with regard to convention rights and the Internet.[34]

First, the ECtHR has repeatedly stated in its case law that the Internet plays an important role in enhancing public access to and the dissemination of information, which are both part of the right to freedom of expression that is articulated in art. 10 ECHR.[35] This idea is clearly visible in the 2015 case of *Cengiz and Others v. Turkey*.[36] In this case, the ECtHR found that a blanket order to block YouTube affected the applicants' right to receive and impart information and ideas. This blanket blocking order thus violated the right to freedom of expression in art. 10 ECHR.[37]

Second, the dynamic, evolutive interpretation of convention rights is clearly visible in case law with regard to the right to privacy and the interception of communications by use of the Internet. At first, the ECtHR dealt with cases concerning the right to respect for private life and the right to respect for correspondence in relation to the interception of communications made by telephone. In 2007, the evolutive interpretation became clear when the ECtHR stated in the case of *Copland v. The United Kingdom* that *e-mails* and *information derived from the monitoring of personal Internet usage* are also protected under the right to respect for correspondence in art. 8 ECHR.[38] This second example illustrates that the dynamic, evolutive interpretation of convention rights can be particularly important for digital investigative methods, which often interfere in the right to privacy in new manners.

---

34 See also the report 'internet case-law of the European Court of Human Rights' of the Council of Europe (June 2015) for a more general and extensive overview of case law. Available at: http://www.echr.coe.int/Documents/Research_report_internet_ENG.pdf (last visited on 24 June 2016). See also the recently published factsheet of the ECtHR on 'new technologies' with a list of case law from June 2016. Available at: http://www.echr.coe.int/Documents/FS_New_technologies_ENG.pdf (last visited on 24 June 2016).

35 See, e.g., ECtHR 10 March 2009, *Times Newspapers Ltd (nos. 1 and 2) v. the United Kingdom*, appl. nos. 3002/03 and 23676/03, § 27, ECtHR 18 December 2012, *Ahmet Yildirim v. Turkey*, appl. no. 3111/10, § 48-49.

36 See ECtHR 1 December 2015, *Cengiz and Others v. Turkey*, nos. 48226/10 and 14027/11.

37 See ECtHR 1 December 2015, *Cengiz and Others v. Turkey*, nos. 48226/10 and 14027/11. See also ECtHR 18 December 2012, *Ahmet Yildirim v. Turkey*, appl. no. 3111/10.

38 ECtHR 3 April 2007, *Copland v. The United Kingdom*, appl. no. 62617/00, § 41.

3.3.2 Relevance for digital investigative methods

The dynamic, evolutive interpretation of convention rights is an important concept for the regulation of digital investigative methods based on art. 8 ECHR. From this concept, it follows that the ECtHR does not only interpret convention rights based on the text of the ECHR itself or its historical meaning. Following the preamble of the convention, the "maintenance and further realisation of Human Rights and Fundamental Freedoms" is the aim to be pursued by the convention. The ECtHR interprets convention rights in order to realise this goal.

This 'teleological interpretation' of convention rights features in "virtually all judgements of the ECtHR", according to Senden (2011, p. 58). This means that the textual interpretation of convention rights can at times be 'overruled' by the ECtHR to ensure the protection of fundamental individual rights (see Senden 2011, p. 53). The ECtHR also uses the 'consensus method' and the 'principle of autonomous interpretation' to interpret convention rights according to their present-day standards. These methods of interpretation are further considered below.

The 'consensus method' means that the ECtHR compares the laws of contracting States to determine whether consensus on a certain issue can be found. If this consensus is found, the ECtHR can adopt an interpretation that is in line with this consensus (see Senden 2011, p. 67). For instance, if many contracting States require a warrant to conduct a computer search, the ECtHR may refer to that legislation and specify that a warrant is part of the required quality of the law according to present-day standards.

It can also occur that contracting States to the ECtHR take a restrictive interpretation of the scope of protection under art. 8 ECHR and provide their governmental investigative authorities with broad investigative powers, which the ECtHR may not deem to be desirable. In such a case, the ECtHR need not grant discretion, follow consensus, or assign decisive importance to what a respondent State considers an acceptable interpretation of standards in the circumstances at hand. The ECtHR then interprets the law *autonomously* (cf. Letsas 2013 in: Føllesdal, Peters & Ulfstei 2013, p. 108). Senden (2011, p. 78) explains that if the ECtHR were to take a different approach, it would be dependent on national classifications for the regulation of investigative methods, which would in turn undermine the ability of the ECHR to provide a minimum level of protection for human rights. In the context of the regulation of digital investigative methods, the autonomous interpretation of convention rights may allow the ECtHR to decide that it is desirable to expand the protection of the right to privacy to cover certain aspects of the right to privacy when digital investigative methods are applied. In addition, the ECtHR can also decide that certain regulations and procedural safeguards are required to adequately regulate digital investigative methods.

In brief, a dynamic reading of the ECHR provides the degree of flexibility necessary for the ECtHR to interpret convention rights in a rapidly changing environment (see Dzehtsiariou 2011, p. 1732). It also enables the ECtHR to both appraise interferences with convention rights when digital investigative methods are applied according to present-day standards and conditions and formulate any desirable regulations that it deems necessary.[39] The same is true of teleological and autonomous interpretation applied by the ECtHR. All contracting States to the ECHR must then meet the required quality of the law by implementing the normative requirements in their domestic legal frameworks.

3.4 Chapter conclusion

The aim of this chapter was to identify the basic framework containing the normative requirements for the regulation of investigative methods from art. 8 ECHR (RQ 2). To answer the research question of this chapter, (1) the scope of art. 8 ECHR, (2) the conditions as stipulated in art. 8(2) ECHR, and (3) the interpretative approaches of the ECtHR to convention rights were examined.

The analysis showed that investigative methods that interfere with the right to privacy must meet three conditions: (1) they must have a legitimate aim, (2) they must be in accordance with the law, and (3) they must be necessary in a democratic society. In relation to regulating investigative methods, the second condition of being '*in accordance with the law*' is most important. This second condition requires that the regulations for the investigative methods (1) are *accessible*, (2) are *foreseeable*, and (3) meet a certain *quality of the law*. Further in this study, these normative requirements are deployed as the framework against which the regulation of investigative methods should be tested.

In relation to the required quality of the law, it is important to note that the gravity of a privacy interference and the accompanying quality of the law are interpreted in conformity with present-day standards and conditions. When the gravity of a privacy interference that results from applying an investigative method changes due to technological developments, the required quality of the law should change accordingly. The gravity of privacy interferences and the accompanying desirable quality of the law for the identified digital investigative methods are further examined in chapter 4.

39 At the same time, in the context of the regulation of investigative methods, contracting States to the ECtHR may regard an autonomous interpretation of convention rights as a risk to their sovereign right to regulate governmental powers that are used for evidence gathering purposes in criminal investigations.