Investigating cybercrime

Oerlemans, J.J.

7 Applying undercover investigative methods online

This chapter aims to answer the fourth research question with regard to online undercover investigative methods (RQ 4c): *How can the legal framework in Dutch criminal procedural law be improved to adequately regulate online undercover investigative methods?* In this study, online undercover investigative methods are categorised as (1) online pseudo-purchases, (2) online undercover interactions with individuals, and (3) online infiltration operations. To answer the research question, the investigative method is placed within the Dutch legal framework and further analysed to determine whether the normative requirements of art. 8 ECHR for regulating investigative methods are fulfilled. In chapter 3, the normative requirements were identified as follows: (1) accessibility, (2) foreseeability, and (3) the quality of the law.

In chapter 4, the desirable quality of the law for online undercover investigative methods was formulated. Undercover investigative methods should be regulated in detail in statutory law with strong procedural safeguards to both ensure transparency in their application and prevent entrapment from taking place. 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 as protected by art. 6 ECHR. 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 that the art. 6 ECHR may be equated with art. 8 ECHR requirements. The Dutch legislator does recognise that interferences with the right to privacy take place when undercover investigative methods are applied and the requirements of art. 8(2) ECHR apply. This strengthens the argument to transpose the similar requirements derived from case law of art. 6 ECHR to the normative requirements derived from art. 8 ECHR.

Brief description of the Dutch legal framework for undercover operations

Before proceeding, it is important to examine the basics of the Dutch legal framework vis-à-vis undercover investigative methods. As explained in section 1.1, the Dutch IRT affair has been very influential in the regulation of (special) investigative methods in the Netherlands.[1] In the 1990s, law enforcement authorities took many liberties in deploying novel undercover

1 See also for an extensive analysis Blom 1998.

investigative methods to gather evidence in criminal investigations that were (mostly) related to drug crimes. The (secrecy surrounding the) utilisation of these undercover investigative methods and the use of authorised drug transports led to controversy in the Netherlands. The special parliamentary inquiry commission Van Traa was instated and delivered an extensive report regarding the use of these undercover investigative methods. The report included recommendations for new regulations. These recommendations eventually led to the Special Investigative Powers Act, which was adopted in 1999.[2]

With the implementation of this act in the DCCP in February 2000, the Dutch legislature created detailed regulations for, amongst other special investigative powers, the application of undercover investigative methods in Dutch criminal procedural law. The following undercover investigative methods were regulated as special investigative powers in the DCCP:

(1) The special investigative power to conduct a pseudo-purchase or pseudo-service (e.g., buying goods or providing services for evidence gathering purposes);
(2) The special investigative power for systematic information gathering (e.g., interacting with suspects while undercover); and
(3) The special investigative power for infiltration operations (e.g., undercover operations in criminal organisations).[3]

The Dutch legislator held that detailed regulations were necessary for these undercover investigative methods, because these methods (1) interfere with the rights and freedoms of the individuals involved in more than a minor manner and (2) endanger the integrity of criminal investigations.[4] The Dutch regulations for undercover investigative methods are illustrated in Figure 7.1 by plotting them on the scale of gravity for privacy interferences and accompanying quality of the law that is derived from art. 8 ECHR.

2 See section 1.1.

3 At the same time, many other special investigative powers were implemented in the Dutch criminal procedural legal framework. For an extensive analysis of these special investigative powers, see, for example, Buruma 2001, p. 33-130.

4 See *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 3 and 10.

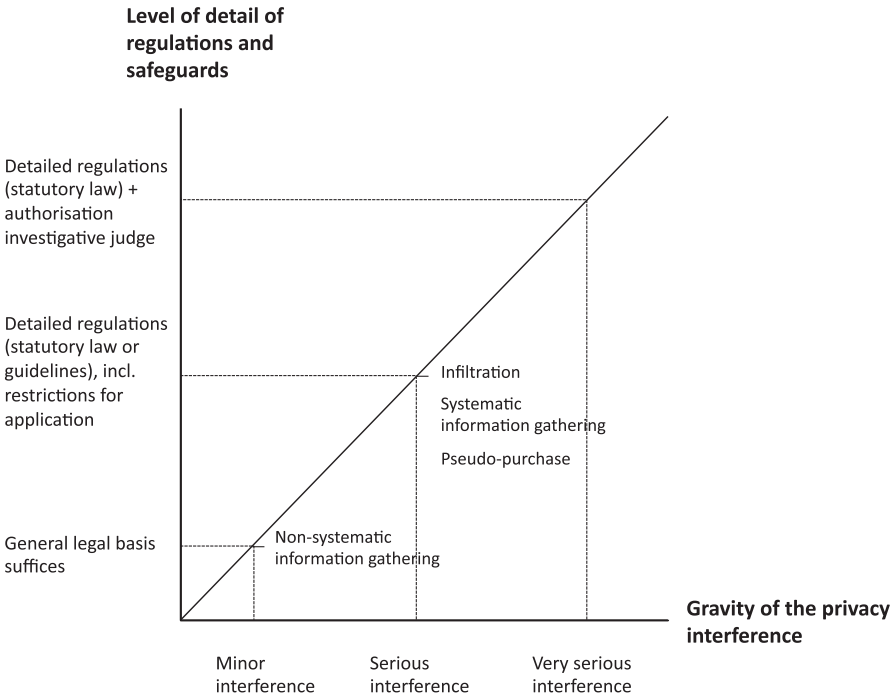

Figure 7.1: The Dutch scale of gravity for the regulation of undercover investigative methods.

Figure 7.1 illustrates how the level of detail and procedural safeguards for undercover investigative methods varies and depends on the gravity of the privacy interference which are different for each investigative method. It is worth noting that the Dutch legislature does not require a specific provision for all undercover investigative methods. Most notably, for non-systematic information gathering, the general legal basis in art. 3 of the Dutch Police Act may suffice. In this chapter, the Dutch legal framework for undercover investigative methods is thus tested with regard to accessibility, foreseeability, and the desired quality of the law.

Structure of the chapter

This chapter is structured as follows. The three normative requirements of art. 8(2) ECHR are tested in separate sections, each of which discusses all three types of undercover investigative methods. To assess the accessibility and foreseeability of the Dutch legal framework with regard to the investigative methods, the same scheme of research is used as in chapters 5 and 6. That research scheme entails examining the following four sources of law: (A) statutory law, (B) legislative history, (C) case law, and (D) public guidelines. Thereafter, the requirements for regulations extracted from art. 8 ECHR in chapter 4 are compared to the Dutch legal framework. Based on the results of the analyses, recommendations are provided to improve the Dutch legal framework.

It thus follows that section 7.1 tests the *accessibility* of the Dutch regulations for online undercover investigative methods. Section 7.2 examines the extent to which online undercover investigative methods are regulated in a *foreseeable* manner in the Netherlands. Section 7.3 analyses whether the Dutch legal framework for online undercover investigative methods meets the *desired quality of the law*. Based on the analyses in sections 7.1 to 7.3, section 7.4 provides concrete proposals as to how Dutch criminal procedural law can be improved to adequately regulate online undercover investigative methods. Section 7.5 concludes the chapter by presenting a summary of its findings.

7.1 Accessibility

An accessible basis in law means that the individual involved has an adequate indication of which regulations apply to the use of investigative methods in a particular case.[5] Given the detailed regulations that have been created for undercover investigative methods in the Netherlands, it is expected that this normative requirement will be unproblematic in Dutch law. However, whether the examined legal sources in law also indicate the legal basis for the *online* application of undercover investigative methods in the Netherlands must be explored separately.

Subsections 7.1.1 to 7.1.3 examine the accessibility of the three types of online undercover investigative methods. Subsection 7.1.4 then presents conclusions regarding the investigative method's accessibility in Dutch law.

7.1.1 Online pseudo-purchases

An online pseudo-purchase entails the investigative method during which an undercover law enforcement official poses as a potential buyer of an illegal good or data in order to gather evidence of a crime. For example, law enforcement officials may buy stolen data, drugs, or weapons from vendors in online forums to collect evidence in a cybercrime investigation.[6] The accessibility of the legal basis for applying online pseudo-purchases as an investigative method is examined below with the previously mentioned research scheme.

A Statutory law

In Dutch criminal procedural law, (online) pseudo-purchases are regulated by the special investigative power for pseudo-purchase.[7] Art. 126i(1) DCCP reads as follows.

5 See subsection 3.2.2 under A.
6 See subsection 2.2.3 under C.
7 See art. 126i DCCP.

"In case of reasonable suspicion of a crime as defined in art. 67 DCCP, first paragraph, a public prosecutor can order, insofar it is in the interest of the investigation, a law enforcement official to:
a. buy goods from a suspect;
b. buy data from a suspect that is stored, processed or transferred by an automated device through the intermediary of public telecommunication network, or
c. provide services to a suspect."

The special investigative power thus indicates that law enforcement officials can buy goods or data in a criminal investigation as part of an online pseudo-purchase as an investigative method. The technological neutral manner the provision is articulated provides room to conduct a pseudo-purchase in an online context when this special investigative power is applied. These detailed regulations in the DCCP are thus considered accessible to the individuals involved.

It should be noted that the special investigative power in art. 126i(1) DCCP also authorises law enforcement officials to provide services to a suspect in a criminal investigation.[8] This application of the investigative method is not examined in this study, since the identified digital investigative method focuses on purchasing goods or data from a suspect in an online context.[9]

B Legislative history

The Special Investigative Powers Act mandated that the investigative method of a pseudo-purchase be regulated in detail as a special investigative power.[10] The explanatory memorandum to the act specifies that this special investigative power allows for the one-time application of a pseudo-purchase in a criminal investigation.[11]

In 1997, the Dutch legislature also stated for the first time that special investigative powers can be applied 'on the Internet'.[12] This position was reiterated in the explanatory memorandum to the Computer Crime Act II in 1999. Here, the Dutch legislator stated that undercover investigative methods can be applied 'in the digital world'.[13]

8 See art. 126i(1) DCCP under c.
9 This does not mean that the investigative method is not relevant. See, e.g., Rb. Haarlem 8 September 2011, ECLI:NL:RBHAA:2011:BS8878, in which an online pseudo-service was conducted by responding to an offer of a money mule recruiter on a chat website. Based on the examination of case law on rechtspraak.nl (a database for judgements that were uploaded by Dutch courts), it appears that case law with regard to pseudo-services in an online context is scarce.
10 In art. 126i DCCP and art. 126ij DCCP (see the statutory law as examined above under A).
11 See also *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 76.
12 In 1997, the Dutch legislature made clear that the special investigative powers for systematic information gathering and infiltration can be employed on the Internet in 'digital investigations' (*Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 29 and p. 55.
13 *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1998/99, 26 671, no. 3 (explanatory memorandum Computer Crime Act II), p. 36-37.

The Computer Crime Act II amended the special investigative power for pseudo-purchase in order to enable law enforcement officials to purchase *data* as part of a pseudo-purchase.[14] This was done because the special investigative power previously only enabled law enforcement officials to purchase a good – and not data – from an individual involved in a criminal investigation. The amendment enables law enforcement officials to conduct a criminal investigation by, for instance, purchasing stolen login credentials offered by individuals in an online black market.

Dutch legislative history thus does indicate which regulations apply to this investigative method in Dutch law.

C Case law

A large amount of case law indicates that the investigative method of a pseudo-purchase is applied relatively often in an online context.[15] This case law is further explored in subsection 7.2.1 to examine the foreseeability of the investigative method. The case law affirms that law enforcement officials use the special investigative power in art. 126i DCCP to apply online pseudo-purchases as an investigative method in practice.

D Public guidelines

The Guideline for Special Investigative Powers affirms the detailed legal basis in Dutch criminal procedural law for using a pseudo-purchase as an investigative method. It does not specifically state that the investigative method can be applied in an online context.

7.1.2 Online undercover interactions with individuals

Performing online undercover interactions with individuals as an investigative method can take place on many online platforms, including chat services, private messaging services, social media services, discussion forums, and black markets. With the right knowledge of internet subcultures, law enforcement officials can interact and build relationships with individuals using credible fake identities in order to gather evidence in criminal inves-

14 *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1998/99, 26 671, no. 3 (explanatory memorandum Computer Crime Act II), p. 37-39.

15 See Rb. Den Haag 10 July 2008, ECLI:NL:RBSGR:2008:BD7012 (online pseudo-purchase of soft drugs on a Dutch website), Rb. Roermond 4 March 2009, ECLI:NL:RBROE:2009:BH4757 (online pseudo-purchase of suspected stolen goods at the online marketplace Marktplaats.nl), Rb. Zutphen, 28 January 2011, ECLI:NL:RBZUT:2011:BP2308 (online pseudo-purchase of illegal weapons), Rb. Haarlem 8 September 2011, ECLI:NL:RBHAA:2011:BS8878 (online pseudo service by responding to an offer of a money mule recruiter on a chat website), Rb. Oost-Brabant 6 May 2013, ECLI:NL:RBOBR:2013:BZ9467 (online pseudo-purchase of illegal fireworks), Rb. Overijssel, 24 February 2014, ECLI:NL:RBOVE:2014:884 (online pseudo-purchase of illegal fireworks), Rb. Rotterdam 8 May 2014, ECLI:NL:RBROT:2014:3504 (online pseudo-purchase on the drug trading website Silk Road), and Rb. Overijssel, 18 April 2016, ECLI:NL:RBOVE:2016:1323 (online pseudo-purchase of ivory from endangered species).

tigations (cf. Siemerink 2000b, p. 145 and Petrashek 2010, p. 1528).[16] The accessibility of the legal basis for using online undercover interactions with individuals as an investigative method is examined below utilising the announced research scheme.

A Statutory law

Dutch statutory law only provides a detailed legal basis for *systematically* performing undercover interactions with individuals as an investigative method within a criminal investigation. Art. 126j(1) DCCP reads as follows.

"In case of reasonable suspicion of a crime, a public prosecutor can, insofar it is in the interest of the investigation, order a law enforcement official as meant in art. 141(b) DCCP, to systematically gather information about the suspect, without being recognisable as a law enforcement official."

The text of the special investigative power thus indicates that a law enforcement official can systematically gather information about the suspect, without being recognisable as a law enforcement official. The text itself does not suggest that the investigative method includes the undercover *interactions* with individuals, but it does not exclude this option either. An accessible legal basis is therefore provided for the systematic application of this investigative method. The special investigative power in art. 126j(1) DCCP does not mention the investigative method can be applied in an online context. However, the text does not exclude the possibility either.

From the system behind the regulation of investigative methods in Dutch criminal procedural law (see the introduction to chapter 5), it follows that the basis for undercover interactions with individuals is derived from either (1) the description of the statutory duty of law enforcement officials to investigate crime set forth in art. 3 of the Dutch Police Act or (2) the above-mentioned special investigative power for systematic information gathering.[17]

B Legislative history

The Dutch legislature explicitly mentioned in its explanatory memoranda to the Special Investigative Powers Act and the Computer Crime Act II that the special investigative power for systematic information gathering can also be applied on the Internet.[18] The explanatory memorandum to the Special Investigative Powers Act explains that law enforcement officials who systematically gather information about a suspect *actively interfere* in that suspect's

16 See subsection 2.2.2 under C.

17 See (1) art. 3 Dutch Police Act 2012 in combination with 141-142 DCCP and (2) art. 126j DCCP.

18 See *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 34. See also *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1998/99, 26 671, no. 3 (explanatory memorandum Computer Crime Act II), p. 37.

life. Their activities go beyond mere observation or listening in on conversations.[19] This description meets the digital investigative method of undercover online interactions with individuals that are involved in a criminal investigation. Dutch legislative history thus provides an indication of the applicable regulations for applying this investigative method in an online context.

C Case law

Until 10 December 2015, no Dutch case law provided an indication of the applicable legal basis for the investigative method of online undercover interactions with individuals. However, on that date, the Court of The Hague provided the first judgment in the Netherlands about the appropriate legal basis for a specific application of this investigative method and affirmed that the special investigative power of systematic information gathering can be applicable to undercover online interactions with individuals involved in a criminal investigation.[20] The facts of the case are further considered in subsection 7.2.1 to illustrate the scope of the investigative method and the manner in which the investigative method can be applied.

D Public guidelines

The Guideline for Special Investigative Powers of the Public Prosecutors Service from 2014 does not discuss the *online* application of the investigative method that involves undercover interactions with individuals in a criminal investigation.

However, it does state that the legal basis for applying this investigative method in the physical world is derived from either (1) the statutory duty of law enforcement officials to investigate crime in art. 3 of the Dutch Police Act or (2) the special investigative power for systematic information gathering. Furthermore, the guideline specifies how the investigative power is to be differentiated from other special investigative powers that regulate other undercover investigative methods. The guideline explains that the special investigative power differs from systematic observation in the sense that the systematic information gathering is not limited to the following or observing the behaviours of an individual, but also authorises a law enforcement to *actively interfere* in the life of the individual involved to gather evidence.[21]

7.1.3 Online infiltration operations

Infiltration operations are similar to undercover interactions with individuals. However, the former are distinguished in this study by the fact that undercover agents involved in these operations are authorised (to a certain

19 *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 35.

20 Rb. Den Haag, 10 December 2015, ECLI:NL:RBDHA:2015:14365, m.nt. J.J. Oerlemans, *Computerrecht* 2016, no. 2, p. 113-124.

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

extent) to *participate* in a criminal organisation. This may entail, for instance, participating in a criminal organisation that is active within an online black market. Infiltration operations have in common with a pseudo-purchase that a(n) (authorised) crime can be committed during their application.

The accessibility of the legal basis for applying an online infiltration operation as an investigative method is examined below using the announced research scheme.

A Statutory law

In Dutch criminal procedural law, infiltration operations are regulated by the special investigative power for infiltration. Art. 126h(1) DCCP reads as follows.

"In case of reasonable suspicion of a crime as defined in art. 67 DCCP, first paragraph, which considering its nature or cohesion with other crimes committed by the suspect seriously interfere with the legal order, a public prosecutor can, insofar the interest of investigation demands it, order a law enforcement official as meant in art. 141(b) DCCP to participate in or provide services to a group of persons that are reasonably suspected of committing or plotting crimes".

These specific regulations provide an indication of the legal basis for this investigative method, because it enables law enforcement officials (under stringent conditions) to participate in or provide services to an organised crime group.

B Legislative history

In its explanatory memorandum to the Special Investigative Powers Act in 1997, the Dutch legislator explicitly stated that the special investigative power for infiltration can also be applied 'on the Internet'.[22] This statement was repeated in the explanatory memorandum to the Computer Crime Act II in 1999.[23] The Dutch legislator noted in its explanatory memorandum to the earlier act that the special investigative power is considered necessary given that the investigative method enables law enforcement officials to infiltrate a criminal organisation to both collect evidence about the crimes that the organisation is committing (or preparing to commit) and gain insights into its modus operandi.[24] Dutch legislative history thus provides an indication regarding the legal basis for this investigative method.

22 See *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 29.

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

24 See *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 28.

C Case law

Case law that involves the use of infiltration as a special investigative power in an online context is rare in the Netherlands. *One* available case specifies that the special investigative power for infiltration has been used on the Internet.[25] The details of this case are further examined in subsection 7.2.3 in order to analyse the scope of the investigative method and the manner in which the investigative method is applied in practice.

D Public guidelines

The Guideline for Special Investigative Powers does not specify that infiltration operations can also be applied in an online context. It instead merely repeats legislative history by specifying the legal basis for the special investigative power for infiltration.[26]

7.1.4 Section conclusion

The accessibility of the Dutch legal framework in criminal procedural law with regard to online undercover investigative methods can be assessed based on the analyses conducted in subsections 7.1.1 to 7.1.3, the results of which are presented below.

The online undercover investigative method are in their application similar to the application of undercover investigative method in the physical world (although they are applied in a different context). In order words, the investigative methods match and do not require regulations in special provisions in the DCCP.

Performing a pseudo-purchase as an investigative method is regulated as a special investigative power in Dutch law. Dutch legislative history and case law make it clear that this special investigative power for pseudo-purchase can also be applied in an online context. For that reason, the Dutch legal basis for this investigative method is considered *accessible*.

The systematic application of interacting with individuals in an undercover capacity is regulated by the special investigative power for systematic information gathering in the DCCP. It follows from the Dutch system for regulating investigative methods in criminal procedural law that the non-systematic application of this investigative method can be based on the statutory duty of law enforcement officials to investigate crimes set forth in art. 3 of the Dutch Police Act. Dutch legislative history and case law make it clear that the special investigative power can also be applied in an online context. For that reason, the Dutch legal basis for the investigative method is considered *accessible*.

25 See Rb. Midden-Nederland 9 October 2014, ECLI:NL:RBMNE:2014:4790 and ECLI:NL:RBMNE:2014:4792.

26 See section 2.6 and 2.9 of the Guideline for Special Investigative Powers.

Infiltration operations are regulated by the special investigative power for infiltration in the DCCP. Legislative history and case law make clear that the special investigative power can also be applied in an online context. Therefore, the legal basis in the DCCP for this investigative method is considered *accessible*.

7.2 Foreseeability

A legal framework that is foreseeable prescribes with sufficient clarity (1) the scope of the power conferred on the competent authorities and (2) the manner in which an investigative method is exercised.[27] The analysis in section 7.1 has shown that Dutch law provides a detailed legal framework that indicates which legal basis applies to the identified digital investigative methods. With the corresponding regulations, the Dutch legislature aimed to provide an accessible and foreseeable legal framework that enables the individuals involved in undercover operations to foresee when and how undercover investigative methods can be applied.[28] The analysis below determines whether that objective is achieved in terms of foreseeability.

Subsections 7.2.1 to 7.2.3 examine the foreseeability of all three types of online undercover investigative methods. Subsection 7.2.4 then presents conclusions regarding the foreseeability of this investigative method in Dutch law.

7.2.1 Online pseudo-purchases

The foreseeability of the regulations for applying online pseudo-purchases as an investigative method is examined below using the announced research scheme.

A Statutory law

The special investigative power that regulates pseudo-purchases in detail in art. 126i DCCP indicates the scope of the investigative method and the manner the special investigative power is applied by stating the requirements that Dutch law enforcement officials must meet to purchase goods or data from a suspect. The investigative power can only be applied in the interest of criminal investigations involving crimes as defined in art. 67(1) DCCP, after authorisation is obtained from a public prosecutor.[29]

27 See subsection 3.2.2 under B.

28 *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 10.

29 See art. 126i(1)DCCP.

The special investigative power also explicitly incorporates the prohibition of entrapment in art. 126i(2) DCCP.[30] The prohibition of entrapment also restricts the scope of the investigative method and the manner the investigative method can be applied. The Netherlands essentially has the same understanding of entrapment as the ECtHR. In 1991, the Dutch Supreme Court made it clear in the *Tallon* case that Dutch law enforcement authorities must ensure that 'a civilian does not commit a crime that would not have been committed without the intervention of law enforcement authorities'.[31] As noted in subsection 4.3.1, the ECtHR also requires that an offence would have been committed without the intervention of law enforcement authorities (cf. Ölçer 2014, p. 16).[32] An undercover operation should therefore remain 'essentially passive'. Law enforcement authorities should merely 'join' criminal acts that have already commenced and not instigate them.[33] Whether entrapment has taken place is decided on a case-by-case basis.

Statutory law itself thus provides on indication regarding the scope of the investigative method and the manner in which the investigative method is applied.

B Legislative history

The explanatory memorandum to the Special Investigative Powers Act specifies the manner in which this investigative can be applied in the physical world. The legislative history states that the special investigative power allows law enforcement officials to commit crimes, such as purchasing a weapon, as part of a criminal investigation.[34] The explanatory memorandum states explicitly that the special investigative power does not authorise a law enforcement official to sell an illegal good and then arrest the purchaser.[35]

---

30 Art. 126i(2) DCCP reads as follows: "*The investigating law enforcement official that applies the order shall not bring a suspect to commit other offences than those that he intended to commit*".

31 See HR 4 December 1979, ECLI:NL:HR:1979:AB7429, *NJ* 1980, 356, m.nt. Th.W. van Veen. See also *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 31.

32 See ECtHR 4 November 2010, *Bannikova v. Russia*, appl. no. 18757/06, § 36-46 for an extensive test to determine whether police entrapment has taken place.

33 ECtHR 4 November 2010, *Bannikova v. Russia*, App. no. 18757/06, §43. See also ECtHR 23 October 2014, *Furcht v. Germany*, appl. no. 54648/09 § 50. To determine whether law enforcement authorities interfered in an active manner that led the suspect to committing the offence, the ECtHR takes the following four factors into consideration: (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 suspect's predisposition to the crime (see Ölçer 2014, p. 16 and ECtHR 4 November 2010, *Bannikova v. Russia*, appl. no. 18757/06, *EHRC* 2011/9, m.nt. Ölçer).

34 *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 34.

35 *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 34. It is noted in the explanatory memorandum that such an application will likely entail entrapment.

The explanatory memorandum to the Computer Crime Act II provides the example of a law enforcement official being able to purchase illegal software or child pornography in order to gather evidence in a criminal investigation.[36] Legislative history thus provides an indication about the manner in which this investigative method is applied.

C Case law

Case law indicates that Dutch law enforcement officials have used this special investigative power to purchase a wide variety of goods that were offered on the Internet. Examples of these goods include drugs, fireworks, weapons, stolen items, and even ivory obtained from endangered animal species.[37] It should observed here that a much greater amount of case law is available regarding this investigative method than for other digital investigative methods that are examined in this study. A report that evaluated the use of undercover investigative methods in the Netherlands also explicitly noted that the special investigative power for pseudo-purchase is often applied in an online context in criminal investigations (Kruisbergen & De Jong 2010, p. 216). Dutch case law thus provides a good indication about the manner in which this investigative method is practically applied in the Netherlands.

The cases show that before a pseudo-purchase is conducted, law enforcement officials contact (and thus interact undercover with) the suspect by e-mail, telephone, or an online private messaging system, in order to reach agreement to purchase the good. These cases have in common that the judges find that the application of the special investigative power of pseudo-purchase is appropriate in the situation that law enforcement officials first contacts the suspect that offers (illegal) goods on an online trading platform in order to purchase that good. The application of the special investigative power does not require that the goods are necessarily delivered to law enforcement officials; it applies as soon as the interaction with the suspect

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

37 See Rb. Den Haag 10 July 2008, ECLI:NL:RBSGR:2008:BD7012 (online pseudo-purchase of soft drugs on a Dutch website), Rb. Roermond 4 March 2009, ECLI:NL:RBROE:2009:BH4757 (online pseudo-purchase of suspected stolen goods at the online marketplace Marktplaats.nl), Rb. Zutphen, 28 January 2011, ECLI:NL:RBZUT:2011:BP2308 (online pseudo-purchase of illegal weapons), Rb. Oost-Brabant 6 May 2013, ECLI:NL:RBOBR:2013:BZ9467 (online pseudo-purchase of illegal fireworks), Rb. Overijssel, 24 February 2014, ECLI:NL:RBOVE:2014:884 (an online pseudo-purchase of illegal fireworks), Rb. Rotterdam 8 May 2014, ECLI:NL:RBROT:2014:3504 (online pseudo-purchase on the drug trading website Silk Road), and Rb. Overijssel, 18 April 2016, ECLI:NL:RBOVE:2016:1323 (online pseudo-purchase of ivory from endangered species). See also Landelijk Parket, 'Undercover onderzoek naar illegale marktplaatsen op internet', 12 February 2014, Landelijk Parket. Available at: https://www.om.nl/vaste-onderdelen/zoeken/@32626/undercover-onderzoek/ (last visited on 17 April 2015).

starts to purchase the good.[38] In two of the seven cases, law enforcement officials asked for authorisation of a public prosecutor too late in the operation, i.e., after the undercover law enforcement officials contacted the suspect or after the agreement to purchase the goods were made.[39]

D Public guidelines

The Guideline for Special Investigative Powers provides detailed information (more than for other investigative methods) about the scope of the special investigative power for pseudo-purchase and the manner in which this power is applied.[40] For example, it explains how law enforcement officials can use this special investigative power to (1) maintain their cover, (2) determine whether a suspect indeed offers an illegal good, and (3) determine the quality of the good (such as a drug) being offered.

The guideline also states that – although the explanatory memoranda to the Special Investigative Powers Act and the Computer Crime Act II do not restrict the investigative power to certain goods – it is not desirable to purchase particular goods. For instance, a public prosecutor cannot authorise the purchase of human organs as part of a pseudo-purchase. In 2011, a report of the Dutch national rapporteur on human trafficking mentioned that Dutch law enforcement authorities do not find it desirable to distribute child pornography on the Internet, as doing so perpetuates the psychological abuse of the minors involved.[41] Considering this, it can be argued that it is also not desirable to purchase child pornography since doing so can stimulate the 'child pornography market'. At the same time, however, purchasing child pornography on the Internet can be an important way to identify abused children and possibly obtain evidence about crimes that are being committing (e.g., child abuse and the distribution of child pornography).

7.2.2 Online undercover interactions with individuals

The foreseeability of regulations for online undercover interactions with individuals as an investigative method is examined below using the announced research scheme.

---

38 See, e.g., Rb. Roermond 4 March 2009, ECLI:NL:RBROE:2009:BH4757 (online pseudo-purchase of suspected stolen goods at the online marketplace Marktplaats.nl) with reference to HR 30 September 2003, ECLI:NL:HR:2003:AF7331, *NJ* 2004, 84 m.nt. Y. Buruma and and Rb. Oost-Brabant 6 May 2013, ECLI:NL:RBOBR:2013:BZ9467 (online pseudo-purchase of illegal fireworks).

39 See Rb. Roermond 4 March 2009, ECLI:NL:RBROE:2009:BH4757 and Rb. Oost-Brabant 6 May 2013, ECLI:NL:RBOBR:2013:BZ9467. The procedural defect was not sanctioned, because the suspect already offered the good on an online trading platform and law enforcement officials discussed the application of the investigative method with the public prosecutor.

40 See most notably section 2.8 of the guideline.

41 See p. 164-165 of the 2011 report of the Dutch national rapporteur on human trafficking (Nationaal Rapporteur Mensenhandel (2011). Kinderpornografie – Eerste rapportage van de nationaal rapporteur. Den Haag: BNRM).

A Statutory law

The special investigative power for systematic information gathering in art. 126j DCCP states that law enforcement officials can 'systematically gather information about the suspect, without being recognisable as a law enforcement official'.[42] The wording of the special investigative power itself therefore does not restrict the scope of the investigative method, except in the sense that it refers to the *systematic* gathering of information about a suspect.

The special investigative power for systematic information gathering further specifies the requirements to apply this special investigative power, stating both that authorisation from a public prosecutor is necessary and that the investigative power can be used in criminal investigations regarding any type of crime.[43] This special investigative power can be applied for a maximum duration of three months.[44] The prohibition of entrapment is notably absent from the regulations associated with this special investigative power (cf. Ölçer 2014, p. 16). In contrast, the prohibition of entrapment is explicitly stated in the special investigative powers for pseudo-purchases and infiltration.[45] The explicit incorporation of the prohibition of entrapment clarifies the scope of the investigative method and the manner the investigative method can be applied, since it emphasises that entrapment is forbidden. The prohibition of entrapment is applicable nevertheless since it flows forth from art. 6 ECHR.

B Legislative history

Dutch legislative history provides more information regarding the scope of this investigative method and the manner in which the investigative method is applied.

As noted in subsection 7.1.2 under B, the explanatory memorandum to the Special Investigative Powers Act explains that law enforcement officials who systematically gather information about a suspect *actively interfere* in that suspect's life. Their activities go beyond mere observation or listening in on conversations.[46] The explanatory memorandum also states that the special investigative power for systematic information gathering is formulated in a technological neutral manner to enable law enforcement officials to conduct 'digital investigations'.[47]

The explanatory memorandum to the Computer Crime Act II also provides more information on the manner the special investigative power is applied. The legislative history states that that an undercover law enforcement official can interact with other individuals on the Internet in so-called

42 See subsection 7.2.1 under A.
43 See also subsection 7.1.2.
44 See art. 126j(2) DCCP.
45 See art. 126i(2) DCCP and art. 126h(2) DCCP.
46 *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 35.
47 See *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p 5.

'newsgroups'.[48] In such a situation, a law enforcement official actively participates in a newsgroup by posting messages.[49] The explanatory memorandum emphasises that the investigative power is only applicable when the investigative method is applied systematically.[50]

It should be noted that the explanatory memoranda to both the Special Investigative Powers Act and the Computer Crime Act II do not further indicate when the application of undercover interaction with other individuals as an investigative method becomes 'systematic' in nature. This is important to know, as crossing that line means that it is appropriate to apply the special investigative power for systematic information gathering. Insofar as the investigative method is not systematically applied, the general legal basis in art. 3 of the Dutch Police Act suffices, which is not restricted to any type of crime or duration.[51]

When an undercover law enforcement official interacts with a suspect online, it must be determined at which point in the undercover operation the investigative method becomes systematic in nature. Questions that must be answered in this regard include the following: What factors apply when determining whether the investigative method is applied systematically? Does systematic application depend on the frequency of the online interactions or perhaps the duration of the investigative method? Does it make a difference if conversations are held on a specific type of communications service, such as e-mail or a chat program? Are law enforcement officials allowed to take over accounts of co-operating informants and interact with individuals involved in criminal investigations through those accounts? Overall, many questions concerning the application of this special investigative power in an online context remain unanswered in legislative history. I therefore conclude that the scope of the investigative method is not sufficiently foreseeable in the sense that it is not clear when the application of the method is to be considered systematic.

---

48 See *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 34. Wikipedia aptly describes a 'newsgroup' as a *"repository usually within the Usenet system, for messages posted from many users in different locations. Newsgroups are discussion groups, and are not devoted to publishing news, but were when the internet was young. Newsgroups are technically distinct from, but functionally similar to, discussion forums on the World Wide Web"*. Available at: http://en.wikipedia.org/wiki/Usenet_newsgroup (last visited on 8 April 2015). Newsgroups are frequently utilised to distribute and download (often copyrighted) music and videos. Newsgroups still exist. However, music and video files are today more often distributed through online peer-to-peer services or music and video streaming services.

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

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

51 See also *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 115. However, one can argue that as part of the proportionality principle, undercover operations should *always* be restricted in duration.

C Case law

Only *one* case specifically deals with the appropriate legal basis when law enforcement officials gather evidence in a criminal investigation using undercover online interactions with individuals as an investigative method.[52] This case concerns a criminal investigation with regard to terrorist crimes, in which law enforcement officials used social media services to gather evidence about the suspects. The law enforcement officials created fake profiles on the social media service Facebook and then added themselves as 'friends' to the suspect's own online Facebook profile in order to learn more about the suspect and his activities.[53]

In its decision, the Court of The Hague first cites the relevant Dutch legislative history for the investigative method of systematic information gathering.[54] The court then takes a remarkable step by stating that the investigative methods of observation and information gathering are very similar.[55] In reality, the investigative methods are significantly different: the investigative power for systematic observation concerns the *passive monitoring* of people's behaviours, while the investigative power for systematic information gathering concerns *interacting with people* to gather evidence.[56] These special investigative powers do have in common that they only apply when the investigative method is being used *systematically*. However, the explanatory memorandum of the Special Investigative Powers only cites factors to determine when observation becomes systematic. As explained in subsection 5.2.3, these factors are (1) duration, (2) place, (3) intensity or (4) frequency, and whether (5) a technical device is used while observing an individual's behaviours.[57]

Nevertheless, in the judgment, the Court of The Hague used the same factors provided by the Dutch legislature to determine when observation becomes systematic in nature to determine when the information gathering becomes systematic in nature.[58] In my view, this can be explained by the fact that neither the Dutch legislator (in its legislation) nor the Dutch judiciary (in its consideration of earlier cases) has provided clarity as to when

52 See Rb. Den Haag, 10 December 2015, ECLI:NL:RBDHA:2015:14365.

53 See Rb. Den Haag, 10 December 2015, ECLI:NL:RBDHA:2015:14365, para. 5.1-5.40.

54 See Rb. Den Haag, 10 December 2015, ECLI:NL:RBDHA:2015:14365, para. 5.15-5.21.

55 In contrast to the application of the special investigative power for observation, the legislature provides no criteria for determining when application of the special investigative power for systematic information gathering is required. Cf. Melai and Groenhuijsen 2008, art. 126j DCCP, note 3.

56 See, e.g., section 2.6 of the guideline for special investigative powers of 2014.

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

58 See Rb. Den Haag, 10 December 2015, ECLI:NL:RBDHA:2015:14365, para. 5.22.

information gathering becomes systematic.[59] More clarity about which factors apply is required to identify when the investigative method becomes systematic and the special investigative power for systematic information gathering applies.

With regard to the 'online befriending operation' on Facebook in the aforementioned case, the Court of The Hague decided that the special investigative power for systematic information gathering should have been applied before an online account was created on the Facebook social media service.[60] This particular case therefore suggests that the use of the special investigative power for systematic information gathering is appropriate for an 'online befriending operation' that requires the creation of an account on a social media service in order to view the contents of a private profile and engage in discussions with a suspect for a period of three months. The case thereby provides an indication of the scope of the investigative method by specifying when the special investigative power is appropriate and explaining how the investigative method can be applied in practice.

D Public guidelines

The Guideline for Special Investigative Powers provides a significant amount of information regarding the manner in which this investigative method is practically applied in an offline context. It mentions that the investigative method becomes systematic in nature when 'more or less complete insights are obtained about certain aspects of an individual's private life'.[61] When this criterion is not met, law enforcement officials can use the investigative method based on the statutory duty of law enforcement officials to investigate crime.

---

59 Dutch courts use different criteria to determine whether the investigative method is applied systematically in the physical world. These factors can be identified as follows: (1) the manner in which the information is acquired, (2) the duration of the operation, (3) the location the information is collected from, and (4) the level of intensity of misdirection that is involved (see, e.g., Rb. Dordrecht 30 May 2002, ECLI:NL:RBDOR:2002:AE3709, Rb. Zwolle, 11 February 2003, ECLI:NL:RBZWO:2003:AF4427, Rb. Oost-Brabant, 30 January, ECLI:NL:RBOBR:2015:461). Nonetheless, these criteria are used in an inconsistent manner by Dutch courts (see also Van der Bel 2015 Sdu Commentary for art. 126j DCCP, at D and Buruma and Verborg in: De Melai & Groenhuijsen 2008 for art. 126j DCCP, at 3).

60 See Rb. Den Haag, 10 December 2015, ECLI:NL:RBDHA:2015:14365, para. 5.27. In this case, the law enforcement official who carefully constructed the online identity of a jihadist on Facebook should have requested a public prosecutor to authorise the online undercover operation in an earlier stage and should have reported the operation more carefully. The lack of prior authorisation from a public prosecutor and sloppy reporting were not sanctioned by the judges. See Rb. Den Haag, 10 December 2015, ECLI:NL:RBDHA:2015:14365, para. 5.34-5.35 and 5.38-5.39. For my commentary regarding the case, see: Rb. Den Haag, 10 December 2015, ECLI:NL:RBDHA:2015:14365, m.nt. J.J. Oerlemans, *Computerrecht* 2016, no. 2, p. 113-124.

61 See also *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 26-27. This criterion is used to determine when observation as an investigative method becomes systematic in nature (see also subsection 5.2.3).

The guideline also indicates that when it is expected that law enforcement officials will systematically gather information from a suspect's surroundings using a false identity, it is appropriate to use a special police team to conduct the undercover operations.[62]

Finally, the guideline specifies how this special investigative power is different from other special investigative powers.[63] It explains that this special investigative power differs from the special investigative power for infiltration in the sense that in infiltration operations, law enforcement officials are authorised to commit crimes when participating in the criminal organisation.[64]

With regard to the *online* application of this special investigative power, it is relevant to know that the guideline provides no direction. This leaves many questions unanswered. Considering the opportunities that, for example, undercover operations on social media services provide to law enforcement officials, more explanation regarding the use of the special investigative power to systematically gather information in an online context seems appropriate. Due to this lack of information, the guideline does not – in my view – sufficiently indicate the scope of the investigative method when it is applied in an online context.

7.2.3 Online infiltration operations

The foreseeability of the regulations for online infiltration operations as an investigative method is examined below using the announced research scheme.

A Statutory law

The special investigative power for infiltration in art. 126h DCCP can be distinguished from the text of the special investigative power for systematic information gathering, in the sense that the special investigative power for infiltration focuses on *participating in* or *providing services to* an organised crime group.[65] The text of the special investigative power itself indicates the manner the investigative method is applies. It is notable that there is no such

62 In this respect, one can question whether these teams are fully equipped to perform online undercover operations, since they require knowledge about the relevant internet subcultures. However, this aspect is not further examined, as this study is not concerned with operational issues regarding the use of the investigative methods.

63 See section 2.6 of the guideline.

64 Confusingly, the guideline also states in section 2.7 that civilians under supervision of law enforcement authorities can deliver services to criminals, as long those services do not contribute the commission of the crime the suspect is suspected from.

65 The analysis in subsection 7.2.2 under D has shown that law enforcement officials can also provide services to a suspect using the special investigative power for systematic information gathering. The difference is that in infiltration operations, the service that is provided can facilitate the crime, whereas this is not possible when the special investigative power for systematic information gathering is applied.

thing as 'non-systematic' infiltration as an investigative method. As soon as the investigative method involves the participation or providing services to an organised crime group, the special investigative power of infiltration is applicable.

The special investigative power for infiltration further specifies stringent requirements that apply to this investigative power and therefore indicates the manner in which the investigative method is applied in practice.[66] The special investigative power for infiltration can only be applied in criminal investigations with regard to crimes as defined in art. 67 DCCP, that seriously infringe the legal order, and when necessary for furthering the investigation. A public prosecutor must authorise the use the special investigative power for infiltration.[67] The special investigative power also explicitly incorporates the prohibition of entrapment in art. 126h(2) DCCP. This provision further restricts the scope of the investigative method and the manner the investigative method is applied.

B Legislative history

The explanatory memorandum to the Special Investigative Powers Act extensively describes the regulation of infiltration as an investigative method in Dutch criminal procedural law.[68] This is unsurprising considering the events surrounding the IRT affair. Infiltration operations were one of the main investigative activities of law enforcement officials that led to the controversy in Dutch society concerning undercover operations. The Dutch legislature required legislation to regulate the use of undercover investigative methods, such as infiltration operations, in order to control the integrity of an investigation and protect the involved individuals' right to privacy.[69]

The explanatory memorandum to the Special Investigative Powers Act characterises this undercover investigative method as an undercover operation that entails *participating* in a criminal organisation.[70] The Dutch legislature noted that this special investigative power is considered necessary given that the investigative method enables law enforcement officials to infiltrate a criminal organisation to both collect evidence about the crimes it is committing (or preparing to commit) and gain insights into its modus

66 See subsection 7.1.3.

67 See art. 126h DCCP.

68 *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 28-33.

69 See *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 3 and 10.

70 See also *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 29. See also the 2014 letter of the Dutch Minister of Security and Justice to the Dutch Parliament about the difference in 'informants' and 'individuals infiltrating criminal investigations' (8 October 2014, number 571620).

operandi.[71] Law enforcement officials are authorised to commit crimes in an infiltration operation. For example, they do not have to obtain separate authorisation from a public prosecutor to perform a pseudo-purchase as an investigative power. The special investigative power for infiltration thus also authorises the application of a pseudo-purchase as an investigative method.[72]

With specific regard to use of this special investigative power in an *online context*, the Dutch legislature explicitly notes in explanatory memoranda of the Special Investigative Powers Act and the Computer Crime Act II that law enforcement officials can also (virtually) infiltrate networks of individuals who distribute child pornography through the Internet.[73] However, the previously mentioned report of the Dutch national rapporteur on human trafficking states that Dutch law enforcement authorities do not find it desirable to participate in these networks, as they must distribute child pornography in order to gain access.[74] Doing so will perpetuate the psychological abuse of the minors involved.[75]

Finally, the explanatory memorandum to the Special Investigative Powers Act states that law enforcement officials are not allowed to sell illegal goods or provide illegal services as part of an infiltration operation.[76] However, they are permitted to assist a criminal organisation by setting up a 'front store'. A 'front store' (also known as a 'storefront') is a shop that law enforcement authorities set up in order to facilitate certain activities of a criminal organisation (cf. Corstens & Borgers 2014, p. 518). Legislative history indicates that a front store can for instance facilitate the transport of goods or the conversion of currency for money laundering purposes, with the aim of gathering evidence in a criminal investigation.[77] The explana-

71 See *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 28.

72 See *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 33.

73 See *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 29. See also *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1998/99, 26 671, no. 3 (explanatory memorandum Computer Crime Act II), p. 36-37. The explanatory memorandum to the Computer Crime Act II also states on p. 37 that the special investigative power can be applied on the Internet, which means that law enforcement officials can participate in or facilitate a criminal organisation that is active on the Internet.

74 See p. 164-165 of the 2011 report of the Dutch national rapporteur on human trafficking (Nationaal Rapporteur Mensenhandel (2011). Kinderpornografie – Eerste rapportage van de nationaal rapporteur. Den Haag: BNRM).

75 See subsection 7.1.3 under D.

76 See *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 119 (with the exception of small amounts of drugs).

77 *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 31. With regard to the use of 'front stores', see also the Van Traa report (*Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1995/96, 24 072, nos. 10-11, p. 230 and 239-240).

tory memoranda to the Special Investigative Powers Act and the Computer Crime Act II do not cite any examples of the use of online front stores as part of the application of this special investigative power in an online context.[78] This raises the question of how using front stores translates to an online environment (cf. Siemerink 2000b, p. 143). In my view, it is also conceivable that Dutch law enforcement authorities could assist a criminal organisation with setting up a VPN connection as an anonymising service, while simultaneously wiretapping the connection to gather evidence.[79]

C Case law

Case law that deals with the legitimacy of the use of the special investigative power for infiltration in an online context is scarce. However, *one* case illustrates the scope of the investigative method and the manner in which the investigative method is applied.

In 2013, Dutch law enforcement officials *participated in an online drug-trading forum* as part of an online infiltration operation.[80] The criminal investigation focused on identifying the 'moderators' of a criminal online forum. Moderators generally manage the day-to-day affairs of a forum by scrutinising forum posts and forum users.[81] This particular drug-trading forum was only available through the Tor system and reportedly had 90,000 permanent users with an estimated monthly turnaround of nine million dollars. The moderators also sold drugs on the forum themselves.[82]

78 The explanatory memorandum to the Special Investigative Powers Act notes on p. 119 that the use of front stores is further regulated in internal guidelines.

79 See subsection 2.2.2, in which the 'DarkMarket-investigation' was described to illustrate an online infiltration operation. In that operation, an undercover agent worked himself up within an online forum that specialised in trading stolen credit cards. By providing a VPN service that was wiretapped by the FBI, U.S. law enforcement officials were able to gather evidence. See, e.g., Kim Zetter, 'TJX Hacker Gets 20 Years in Prison', *Wired*, 25 March 2010. Available at: https://www.wired.com/2010/03/tjx-sentencing/ (last visited on 20 February 2016).

80 See Rb. Midden-Nederland 9 October 2014, ECLI:NL:RBMNE:2014:4790 and ECLI:NL:RBMNE:2014:4792. The court cryptically explains that the suspects made use of a 'secured network' to 'anonymously' buy and sell drugs on online market places. The suspects likely made use of the Tor network to buy and sell drugs on hidden services, more specifically 'Black Market Reloaded' and 'Utopia'. See *ANP*, 'OM wil tot zeven jaar cel voor internetdealers', *Nu.nl*, 23 September 2014. Available at: http://www.nu.nl/internet/3885624/wil-zeven-jaar-cel-internetdealers.html (last visited on 17 April 2015). See also J.J. Oerlemans, 'Veroordelingen voor drugshandel via online marktplaatsen', *Computerrecht* 2015, no. 3, p. 170.

81 See Wikipedia, 'Internet forum'. Available at: http://en.wikipedia.org/wiki/Internet_forum#Moderators (last visited on 16 April 2015).

82 See Rb. Midden-Nederland 9 October 2014, ECLI:NL:RBMNE:2014:4790 and ECLI:NL:RBMNE:2014:4792. Interestingly, the authorisation to infiltrate the criminal investigation also encompassed the use of a foreign undercover agent.

Dutch law enforcement authorities aimed at becoming a 'moderator' within this online drug-trading forum, in order to gather evidence about drug dealers who were active in it. In order to achieve this goal, the officials applied the following special investigative powers:

(1) Systematic information gathering (to enable online interactions with the moderators);
(2) A pseudo-purchase of drugs (to enable the purchase and tracking of drugs deals from the online market place);
(3) Systematic observation (to enable the investigative method to observe a suspect's movements in the physical world); and
(4) Infiltration (to enable the officials' (eventual) participation in the online forum as a moderator).[83]

The court's judgment in this case indicates that the special investigative power for infiltration was applied for the entire operation, which may have enabled Dutch law enforcement officials to become a moderator and commit crimes (such as purchasing drugs). In the end, the officials were unable to climb the forum's hierarchical ladder to attain a moderator position.

However, Dutch law enforcement officials were able to contact a moderator of the online drug-trading forum. In doing so, they presumably used the special investigative power for systematic information gathering to interact with the suspect in an undercover capacity. A meeting was subsequently set up in the physical world to buy drugs. It is likely that the special investigative power for pseudo-purchase was applied for this part of the operation. After the drug transaction, the suspect was followed by an observation team, for which the special investigative power for systematic observation was applied. Dutch law enforcement authorities eventually successfully prosecuted five suspects for drug trading and arms trading.[84]

In this case, the judge noted how undercover investigative methods were applied in the physical world as well as 'virtually' under the application of the same special investigative power for infiltration. Despite the defendants' objections, the judges did not identify any problems with this 'hybrid' application of undercover investigative methods.[85] In my view, this hybrid application is indeed unproblematic, insofar as it is clear which investigative methods are authorised by which special investigative power and the relevant facts of the operation are disclosed to the suspects to provide sufficient transparency. Dutch law thus allows for both online and

83 See Rb. Midden-Nederland 9 October 2014, ECLI:NL:RBMNE:2014:4790 and ECLI:NL:RBMNE:2014:4792.

84 See Rb. Midden-Nederland 9 October 2014, ECLI:NL:RBMNE:2014:4790 and ECLI:NL:RBMNE:2014:4792.

85 See Rb. Midden-Nederland 9 October 2014, ECLI:NL:RBMNE:2014:4790 and ECLI:NL:RBMNE:2014:4792. Siemerink (2000b, p. 144) considers this an aspect that will be common in online infiltration operations. Interactions with undercover agents can initially start online and then further develop in interactions in the physical world

offline application of this method. However, case law on online application is scarce. Therefore, while this single case sheds light on the online application of the special investigative power, the case law is insufficient for distinguishing a pattern as to how this digital investigative method is used in practice.

D Public guidelines

The Guideline for Special Investigative Powers offers much information about the use of infiltration as a special investigative power. Much of this information is already provided in legislative history. Therefore, only the most relevant information that helps to further clarify the scope of the investigative method and manner in which the investigative method is applied is presented below.

The guideline makes it clear that the special investigative power to infiltrate a criminal organisation allows law enforcement officials to use investigative methods that fall under the special investigative powers of systematic information gathering and pseudo-purchases. The authorisation of the special investigative power in question must mention the use of these other investigative methods as part of an infiltration operation. Infiltration operations should be executed by a special police team.[86]

Finally, the guideline further specifies the differences between the special investigative powers of infiltration and systematic information gathering. The first difference is that the special investigative power for infiltration authorises law enforcement officials to commit crimes that are in direct relation to the crimes of the criminal organisation,[87] which is not allowed when the special investigative power for systematic information gathering is applied. The second difference is that in infiltration operations, law enforcement officials participate in a criminal organisation, whereas during systematic information gathering they merely 'maintain contacts' with suspects or individuals involved in a criminal organisation. The third difference is that the special investigative power to infiltrate can only be applied with regard to a group of individuals that is preparing to commit or already committing crimes. This requirement does not apply to the special investigative power for systematic information gathering. The fourth difference is that the legal thresholds for using the special investigative power for systematic information gathering are lower than those for using the special investigative power for infiltration.

86 These police teams are specially trained. Further requirements for infiltration operations are specified in the 'Regeling infiltratieteams' (Regulation for infiltration teams) (*Stcrt.* 2001, no. 7), but they are not relevant to the research question at hand.

87 See also subsection 7.2.2 under D.

7.2.4 Section conclusion

With regard to online undercover methods, the foreseeability of the Dutch legal framework in criminal procedural law can be assessed based on the analyses conducted in subsections 7.2.1 to 7.2.3. The results of these analyses are summarised below.

The regulations for online pseudo-purchases in Dutch criminal procedural law are considered *foreseeable*. The reason is that statutory law clearly details that law enforcement officials can purchase goods or data using the special investigative power for pseudo-purchase. Dutch legislative history makes clear the investigative methods can be applied in an online context and there is a large amount of case law available that further indicates how the investigative method is applied in practice. Case law indicates that the special investigative power in art. 126i DCCP to conduct a(n) (online) pseudo-purchase is applicable as soon as law enforcement officials start the undercover operation and contact the suspect to buy the (illegal) good offered on an online trading platform. The Guideline for Special Investigative Power does not mention that the investigative method can be applied in an online context, but details the manner it is applied in the physical world. The manner the investigative method are applied in an online context and the physical world are similar and due to its one-time application limited in scope. Therefore, no specific regulations are in my view required for application of the investigative method in an online context.

The regulations for online interactions with individuals in Dutch criminal procedural law are considered *not foreseeable*. The special investigative power for systematic information gathering in the DCCP, which regulates the investigative method, only applies when the investigative method is applied systematically. However, the lack of guidance in the explanatory memoranda to the Special Investigative Powers Act and Computer Crime Act II, the lack of case law, and the lack of direction in the Guideline for Special Investigative Powers, means it remains unclear when the investigative method becomes systematic in nature and hence when the special investigative power for systematic information gathering must be applied. There are no factors provided by the legislator to determine when the investigative method is applied systematically, as opposed to the investigative method of observation. It is unclear whether the same factors are also suitable for the special investigative power of systematic information gathering. This creates ambiguity with regard to the scope of the investigative method and how the manner the investigative method is applied in Dutch law. It is important that the scope of the investigative method is detailed in statutory law or guidelines, because the text of the provision for systematic information gathering is very broad. It is currently unclear which online applications of the special investigative power are legitimate.

The regulations for online infiltration operations in Dutch criminal procedural are considered *foreseeable* in this study. The special investigative power for infiltration indicates the scope of the investigative method and the

requirements that must be met before the investigative method is applied. The prohibition of entrapment clearly restricts the scope of the investigative method and the manner the investigative method is applied. These detailed regulations for the investigative method are desirable, because the investigative method seriously interferes with the right to privacy of the individuals involved and the undercover interactions with poses risks with regard to entrapment in online infiltration operations. The privacy interference and risks of entrapment are in my view not greater in an online context. The explanatory memoranda to the Special Investigative Powers Act and Computer Crime Act II clearly state that the special investigative power can be applied in an online context. Case law concerning the online application of the investigative method is scarce, but also confirms the special investigative power can be applied in online context and indicates in which manner it may take place. Finally, the Guideline for Special Investigative Power indicates the scope of the investigative method in detail for its application on the physical world, but not in the digital world. The guideline does explain the difference of the special investigative power compared to the special investigative powers of systematic observation, pseudo-purchases, and systematic information gathering. The examined legal sources thus clarify (1) when the use of the special investigative power for infiltration is appropriate and (2) in which manner the investigative method can be applied.

7.3 Quality of the law

The normative requirement regarding the quality of the law, means that the ECtHR can specify the level of detail required for the description the investigative power and the minimum procedural safeguards that must be implemented vis-à-vis a particular method that interferes with the right to privacy. The detail that the ECtHR requires in the law and procedural safeguards depends on the gravity of the privacy interference that takes place.[88]

The desired quality of the law for online undercover investigative methods has been determined in Chapter 4, in subsection 4.3.3. As explained in the introduction of the chapter, 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 as protected by art. 6 ECHR. These requirements are such that it is possible to transpose them to requirements for the *regulation* of undercover operations. As such, these requirements are taken as a point of departure as the desirable quality of the law. The ECtHR has specified in case law that it requires *detailed regulations* to ensure transparency regarding an undercover operation and aim to prevent entrapment by law enforcement authorities. In addition, the ECtHR has repeatedly emphasised in case law that *supervision of an investigative judge* is

88 See subsection 3.2.2 under C.

'most appropriate' for undercover operations. Nevertheless, the ECtHR also accepts the supervision of a public prosecutor, insofar 'adequate procedures and safeguards' are available.[89] The desired quality of the law for undercover investigative methods is illustrated in Figure 7.2.

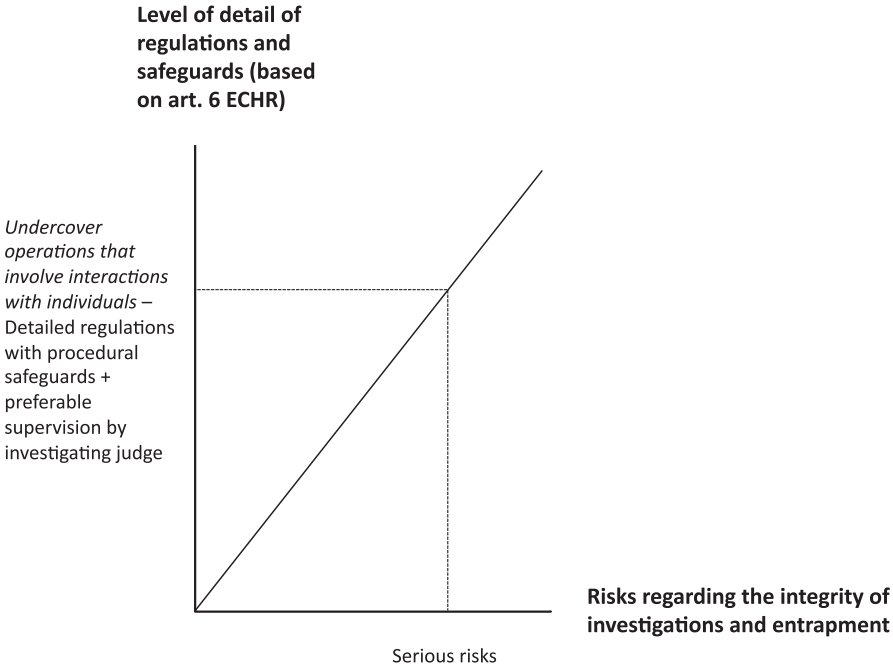

Figure 7.2: The desired quality of the law for undercover investigative methods.

Figure 7.2 illustrates how the scale of gravity looks different for undercover investigative methods than it does for the investigative methods examined in chapters 5 and 6. This difference is attributable to the fact that the ECtHR essentially requires a quality of the law for undercover methods, but does not differentiate between undercover variants. All investigative methods that involve undercover interactions with individuals in which serious risks of entrapment arise must have both detailed regulations that ensure transparency concerning the investigation and adequate supervision to prevent entrapment from taking place.

From a general point of view, the analysis in sections 7.1 and 7.2 has shown that Dutch law has detailed regulations for undercover investigative methods. These regulations are deemed desirable due to the privacy interference that accompanies these methods and the risks regarding the

89 See subsection 4.3.1.

integrity of the investigation.[90] The analysis in subsection 4.3.2 has shown that law enforcement officials can apply online investigative methods on a global scale and relatively anonymously, thanks to the characteristics of the Internet. However, in my view these characteristics generally do not significantly influence the gravity of the privacy interference or risks regarding the integrity of an investigation. The manner the investigative method is applied are the same; they only take place in a different context or with different communication services.

In the remainder of this section, the quality of the Dutch legal framework is tested with regard to each of the identified online undercover investigative methods. In subsections 7.3.1 to 7.3.3, the quality of the law of the special investigative powers that regulate the identified online undercover investigative methods is compared to the desired quality of the law. Subsection 7.3.4 presents conclusions regarding the adequacy of the quality of the Dutch legal framework for the digital investigative method.

7.3.1 Online pseudo-purchases

In the Netherlands, using pseudo-purchases as an investigative method is considered an undercover investigative method that requires detailed regulations in the DCCP.[91] The special investigative power that regulates pseudo-purchases can be applied only once in a criminal investigation with regard to crimes that are stipulated in art. 67(1) DCCP (including cybercrimes).[92] An order from a public prosecutor is required to apply the special investigative power. The involvement of a public prosecutor thus functions as a procedural safeguard to protect both the integrity of the investigation and the right to privacy of the individuals who are involved in it.[93] Public prosecutors must also apply the proportionality and subsidiary test to determine whether the application of the investigative method is legitimate. [94]

The undercover operation is restricted in time and scope since only authorises a single pseudo-purchase. As explained in subsection 4.3.2, I regard the privacy interference the application of the investigative method causes as serious, but not as serious compared to online undercover interactions (that can cover a broader set of operations and which operations can take longer in time) and online infiltrating operations (that involve the participation in crime and the possibility to commit crimes) as online undercover investigative methods.

---

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

91 See *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 2, 23, and 33-34.

92 See also *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 33.

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

94 See also subsection 3.2.3.

The Dutch special investigative power for pseudo-purchase also specifically notes that law enforcement officials are not allowed to incite a suspect to commit a crime that this suspect did not intend to commit.[95] It thus explicitly prohibits entrapment by law enforcement officials. The risk of entrapment is also present in online pseudo-purchases, because law enforcement officials interact in an undercover capacity with suspect in order to purchase the good. These undercover law enforcement officials are thus not authorised to pressure a suspect to sell a good or data, which he did not intend to sell. The examined case law in subsection 7.2.1 indicates that the special investigative power that authorises an online pseudo-purchase was applied when illegal goods were already offered on online trading platforms. In that situation, the risk of entrapment appears small, since the suspect has a predisposition to commit the crime and it likely does not require effort to come to an agreement to purchase the good.

Subsection 4.3.3 identified the desirable quality of the law concerning pseudo-purchases to be detailed regulations and the involvement of a public prosecutor to supervise the application of the investigative method. Considering the above analysis, it can be concluded the Dutch regulations for pseudo-purchases *meet the desired quality of the law*, insofar the special investigative power to conduct a pseudo-purchase is applied.

7.3.2 Online undercover interactions with individuals

The analyses in subsections 7.1.2 and 7.2.2 have shown that the legal basis for online undercover interactions with individuals as an investigative method is derived from either (1) the description in art. 3 of the Dutch Police Act of the statutory duty of law enforcement officials to investigate crime or (2) the special investigative power for systematic information gathering. Based on the examined sources in law in subsection 7.2.2, it not clear exactly when the application of the investigative method becomes systematic in nature and hence when it is appropriate to apply the special investigative power.

The Dutch legislature considers the privacy interference that occurs when this investigative method is applied to be minor in nature, insofar as the method is not applied systematically. However, this argument fails to take the risk of entrapment and important role of supervision in these undercover investigations into account. For example, in the past Dutch law enforcement officials have attempted to pose as a minor in online chat rooms to gather evidence about individuals who want to engage in sexual activi-

95 See art. 126i(3) DCCP.

ties with minors in these online spaces and possibly in the physical world.[96] Smeets (2013, p. 335) implies that the legal basis that was used for the undercover operation was art. 3 of the Dutch Police Act and not the special investigative power of systematic information gathering. The judgement itself does not provide clarity on this issue.[97] Nevertheless, it is clear that law enforcement officials posed as a minor in a chat room to combat grooming. The risk of entrapment is considerable in this context, as the undercover investigative method requires law enforcement officials to actively engage with the individuals involved. To prevent entrapment from taking place, law enforcement officials will need to have a reasonable suspicion that a crime is taking (or will take) place and be able to prove a suspect's predisposition.[98] This investigative method is different from using *passive* decoys, such as unlocked bicycles that may lure bicycle thieves, which Dutch courts have previously found legitimate.[99] If the goal is to successfully prosecute a suspect for grooming by gathering evidence obtained while posing as a minor, the undercover agent must gain the individual's trust by interacting and having conversations of a sexual nature with him or her; the result may then be that the suspect proposes a meeting to engage in sexual activities. It may thus be challenging for law enforcement officials to remain 'essentially passive' in this kind of online undercover operation (cf. Smeets 2013, p. 336 and Ölçer 2014, p. 18). As explained in the introduction of section 7.3, the ECtHR desires detailed regulations and preferably the supervision of an investigative judge for the application of undercover investigative methods in which the risk of entrapment arises. In this case, the risk of entrapment is clearly present and a higher authority than law enforcement officials should test whether the undercover operation is legitimate considering the risk of entrapment. The ECtHR prefers that an investigative judge supervises the operation. In this case, the undercover operation was likely based on art. 3 of the Dutch Police Act, which does not require the authorisation of a public prosecutor. Even when the special investigative power of systematic gathering was applied in this case, it may have been more appropriate that an

96 See Jarl Van der Ploeg, 'Inzet 'lokpuber' komt weer in beeld', *Volkskrant*, 11 January 2014. Available at: http://www.volkskrant.nl/archief/inzet-lokpuber-komt-weer-in-beeld~a3575528/. When an actual meeting is arranged, the act may amount to the crime of grooming. Questions with regard to the use of a 'virtual child' to combat grooming are not addressed in this study. See Michelle Starr, 'First man convicted in child predator sting with virtual girl Sweetie', *CNET* 21 October 2014. Available at: http://www.cnet.com/news/first-man-convicted-in-child-predator-sting-with-virtual-girl-sweetie/ (last visited on 22 April 2015). See also the letter of 28 November 2013 to the Dutch Parliament from the Minister of Security and Justice concerning the news reports that 'a virtual Filipina girl traced 1000 child molesters'.

97 See Hof Den Haag, 25 June 2013, ECLI:NL:GHDHA:2013:2302.

98 Reasonable suspicion and a suspect's predisposition to the crime may be obtained after reports that indicate specific chat rooms in which relevant activities take place have been filed.

99 See HR 28 October 2008, ECLI:NL:HR:2008:BE9817, *VA* 2009, no. 1, m.nt. J. Silvis.

investigative judge supervises the investigation due to the intrusiveness of the investigative method and the high risk of entrapment.[100]

In my view, the Dutch legal framework for this investigative method does *not meet the desirable quality of the law*. At present, (online) undercover investigative methods can be based on either (1) the general legal basis in art. 3 of the Dutch Police Act or (2) the special investigative power for systematic information gathering, which is not even restricted to serious crimes. These regulations are not sufficiently detailed and do not provide the procedural safeguards needed to meet the desired quality of the law. A special investigative power that regulates (online) undercover interactions with individuals and requires authorisation from (or at least the involvement of) a public prosecutor is instead desirable (cf. Janssen 2015, p. 681-682).[101]

From a legal system viewpoint, it is also logical to have an investigative judge supervise undercover operations where entrapment is a risk. In the Netherlands, investigative judges have the responsibility to supervise the legitimacy of the application of investigative methods and ensure that the interests of (1) the investigation and (2) the suspect are balanced (cf. Corstens & Borgers 2014, p. 264). Since 2012, Dutch investigative judges have taken on a more coordinating function for evidence-gathering activities in criminal investigations.[102] As Corstens and Borgers (2014, p. 362) point out, law enforcement officials and public prosecutors are the 'natural adversaries' of suspects, while investigative judges are perceived as more independent in the Netherlands. Investigative judges can therefore serve an important function by safeguarding the integrity of a criminal investigation and preventing entrapment, both of which are particularly important in undercover investigations.

7.3.3 Online infiltration operations

The desirable quality of the law for online infiltration operations was formulated in subsection 4.3.3 as (1) a detailed legal basis in law for applying the investigative method and (2) the procedural safeguard of an investigative judge to supervise the online undercover investigative method. The involvement of an investigative judge is a desirable procedural safeguard, as infiltration operations involve considerable risks that endanger the integrity of criminal investigations.

---

100 See also *Rechtspraak.nl*, 'Advies Rechtspraak: Regel inzet van 'lokpuber' beter', 31 October 2014. Available at: http://www.rechtspraak.nl/Actualiteiten/Nieuws/Pages/Advies-Raad-regel-inzet-van-lokpuber-beter.aspx (last visited on 16 April 2015).

101 See also Ölçer 2015, p. 307, who argues that a warrant an of investigative judge should be considered by the Dutch legislature for the special investigative powers relating to undercover investigative methods. See also ECtHR 23 October 2014, *Furcht v. Germany*, appl. no. 54648/09 (*EHRC* 2015/1, m. nt. Ölçer at 9.

102 As a result of the Act on Strengthening the Position of the Investigative Judge (*Stb*. 2012, 408). See Parliamentary Series II 2009/10, 32 177, no. 2 (explanatory memorandum Act on Strengthening the Position of the Investigative Judge), p. 1.

In the Netherlands, stringent requirements must be fulfilled before the special investigative power for infiltration can be applied.[103] According to the Dutch legislature, these stringent conditions are necessary due to the risk that an operation will endanger a criminal investigation's integrity and the privacy interference that occurs when this investigative method is applied.[104] Apart from the DCCP, more detailed procedures are specified in public guidelines. In its legislation the Dutch legislature explicitly mentions how 'moral dilemmas' are present in undercover investigative methods, due to the fact that law enforcement officials (1) are authorised to commit crimes, (2) the risk they participate in unauthorised crimes, and (3) are subjected to safety risks.[105] Based on this legislative history, the Dutch legislature appears to be well aware of the risks involving infiltration operations and the danger of entrapment.[106] This is also reflected by the application of an extra procedural safeguard. Legislative history describes how – apart from the stringent requirements in the special investigative power itself – an operation must be consulted with a special commission of the Public Prosecution Service.[107] This commission will test (again) whether the operation is proportional in light of the relevant circumstances and determine if any other investigative methods that could be used to achieve the same result are available.

However, authorisation from an *investigative judge* is not required to apply the special investigative power for infiltration, and thus also for online infiltration operations. As a result, the current regulations for online infiltration in Dutch law do *not meet the desired quality of the law*. The Dutch legislature should consider adding a supervisory role for an investigative judge as an extra safeguard (cf. Janssen 2015). This extra safeguard is appropriate when the intrusiveness of the investigative method and the accompanying risks with regard to the integrity of the investigation are taken into account. An investigative judge can carefully balance the interests of both the investigation and the suspect.

7.3.4 Section conclusion

This section has compared the quality of the law of the current Dutch legal framework in criminal procedural law with the desirable quality of the law as determined in subsection 4.3.3. The results of the analyses conducted in subsections 7.3.1 to 7.3.3 are summarised below.

---

103 See subsections 7.1.3 and 7.2.3.

104 *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 29-30 and p. 34.

105 *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 29.

106 See, e.g., *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 31, p. 34, p. 74-75, and p. 120.

107 See *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 15.

The investigative method of online pseudo-purchases is regulated in detail in Dutch statutory law. The risk of entrapment is low when this investigative method is applied and the method does not interfere with the involved individuals' right to privacy in a particularly serious manner. For that reason, the detailed regulations for the investigative method and the required authorisation from a public prosecutor to use the special investigative power were found to *meet the desirable quality of the law*.

The Dutch legal framework for the investigative method of online undercover interactions with individuals *does not meet the desired quality of the law*. The first reason for this assessment is that the investigative method is not regulated in a foreseeable manner in the Dutch legal framework, due to ambiguity with regard to the question when the investigative method is applied in a systematic manner. The analysis again shows that the normative requirements of foreseeability and the quality of the law are intertwined. The second reason is that the analysis in section 4.3 showed that supervision from an investigative judge is desirable when there is a risk of entrapment in the application of this method. The special investigative power that is currently applicable when the investigative method is applied systematically only requires authorisation from a public prosecutor, not mandatory supervision from an investigative judge.

The investigative method of online infiltration operations with individuals does *not meet the desired quality of the law*. The reason is that the analysis in section 4.3 indicated that authorisation from an investigative judge is appropriate for the investigative method. This procedural safeguard is not required in the special investigative power for infiltration. In the Netherlands, only the authorisation of a public prosecutor is required.

7.4 Improving the legal framework

This section discusses how the DCCP can be improved to provide an adequate legal framework for regulating online undercover investigative methods. A legal framework is considered adequate when (1) it is accessible, (2) it is foreseeable, and (3) the desired quality of the law in the sense of procedural safeguards is met. The results of the analyses of the three normative requirements (as presented in sections 7.1 to 7.3) are summarised in Table 7.1.

Normative requirement	**Online pseudo-purchases**	**Online undercover interactions**	**Online infiltration operations**
Accessible	✓	✓	✓
Foreseeable	✓	✗	✓
Meets the desirable quality of the law	✓	✗	✗

Table 7.1: Representation of the research results in sections 7.1 to 7.3 (✓ = adequate, ✗ = not adequate).

This overview of the research results from sections 7.1 to 7.3 shows that the detailed regulations for undercover investigative methods have created an accessible legal framework. The Dutch legislature was quick to point out that the special investigative powers for undercover investigative methods can also be applied on the Internet. However, this statement alone does not create a foreseeable legal framework; further guidance and elaboration is necessary for certain online undercover investigative methods.

According to the Dutch legislature, the Dutch legal framework for special investigative powers only requires amendments when *"the specific nature of investigations in a computerised environment"* merits specific legislation.[108] This chapter has shown that it is not the change of environment that necessitates amendments to the legal framework for online undercover investigative methods, but the heightened procedural safeguards (preferably an investigative judge) for the regulation of the investigative methods that are derived from ECtHR case law. The online application of undercover investigative methods is not more privacy intrusive, since the investigative technique that is used are the same and bring with similar privacy interferences. The online application also does not create more risks regarding the integrity of an investigation than offline variants, although the risk of entrapment remains present.

Improvements to the Dutch legal framework are proposed for each of the identified online undercover investigative methods in subsections 7.4.1 to 7.4.3.

7.4.1 Online pseudo-purchases

The Dutch legal framework for online pseudo-purchases is deemed to be accessible and foreseeable and to offer a sufficient quality of the law. The Dutch Ministry of Security and Justice has recommended that the requirement that data is 'stored, processed or transferred by an automated device through the intermediary of public telecommunication network' in the special investigative power to conduct a pseudo-purchase in art. 126i(1)(b) DCCP be removed. The reason for this proposal is that data can also be transferred by other means of communication; the special investigative power should simply indicate that law enforcement officials can buy data from a suspect as part of a pseudo-purchase.[109] I agree with the suggestion to remove this redundant text from the special investigative power for pseudo-purchases (*Recommendation I*).

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

109 See the discussion document regarding special investigative powers (6 June 2014), p. 30.

7.4.2 Online undercover interactions with individuals

The legal basis in Dutch criminal procedural law for using online undercover interactions with individuals as an investigative method is currently too ambiguous. It is not clear when undercover interactions with individuals are deemed 'systematic in nature' and hence when the special investigative power for systematic information gathering must be applied. The regulations for this investigative method can be improved as follows.

First, the foreseeability of the method can be strengthened by requiring the application of the special investigative power for systematic information gathering whenever law enforcement officials launch undercover operations that involve undercover interactions with individuals as opposed to only requiring the special investigative power when the investigative method is conducted in a systematic manner (*Recommendation 2*). At the start of such an operation, officials must indicate in which manner they intend to interact with an individual and how much time they think they will require to gather sufficient evidence for their criminal investigation. The text of the special investigative power itself can be improved by stating more clearly that law enforcement officials can gather the information by interacting with the suspect and his direct environment (both offline and online).[110]

Second, to improve the quality of the law, it is desirable to involve an investigative judge to supervise the undercover operation. The prohibition of entrapment should also apply in the context of the special investigative power for (systematic) information gathering (*Recommendation 3*). In that respect, it is noteworthy that the Dutch Minister of Security and Justice proposed to mention the prohibition of entrapment explicitly in the general provisions for pre-trial investigations of the DCCP.[111] The provision will make it explicit that the prohibition of entrapment applies to all investigative methods.

Third, more stringent legal thresholds are desirable for the application of the method, considering the high intrusiveness of the special investigative power. Undercover law enforcement officials can gain intimate knowledge about the private lives of the individuals involved – also individuals in the direct environment of the suspect – when the investigative method is applied (both in an online and offline context). On that basis, the application of the special investigative power should be restricted to criminal investigations involving more serious crimes, as defined in art. 67 DCCP (*Recommendation 4*).[112]

---

110 See also the discussion document regarding special investigative powers (6 June 2014), p. 28.

111 See the discussion document regarding the general provisions for pre-trial investigations (6 June 2014), p. 20.

112 See also p. 26 of the discussion document regarding the special investigative powers of 2014 as part of the modernisation programme for Dutch criminal procedural law, which contains a suggestion to increase the special investigative power for criminal investigations with a minimum prison sentence of one year or more.

7.4.3 Online infiltration operations

The use of an infiltration operation as an investigative method is regulated in detail in Dutch criminal procedural law. The special investigative power for infiltration must also be used for online infiltration operations. The Dutch legal framework for online infiltration operations can be considered as accessible and foreseeable, due to the detailed regulations that specify the scope of the investigative method and the manner in which the method can be applied. The additional safeguard of a mandatory review by the special commission of the Dutch Public Prosecution Service is applicable to infiltration operations.

However, the supervision of an investigative judge in undercover operations, which is preferred by the ECtHR, is notably absent in Dutch criminal procedural law for infiltration operations. The mandatory involvement of an investigative judge is thus recommended for the application of the special investigative power for infiltration (*Recommendation 5*).

7.5 Chapter conclusion

The aim of this chapter was to determine how Dutch criminal procedural law should be improved to adequately regulate online undercover investigative methods (RQ 4c). To answer the research question, the Dutch legal framework regulating online undercover investigative methods (i.e., online pseudo-purchases, online undercover interactions with individuals, and online infiltration operations) was investigated with regard to (1) its accessibility, (2) its foreseeability, and (3) the desired quality of the law.

From a broad perspective, Dutch criminal procedural law provides a solid legal basis for investigative methods by outlining detailed corresponding regulations. The Dutch legislature has also been visionary by stating as early as in 1997 that undercover investigative methods can also be applied in an online context. However, statements alone do not create a foreseeable legal basis for those investigative methods that are regulated by special investigative powers with a broad description, most notably with regard to the special investigative power for systematic information gathering.

The results of the adequacy of the Dutch regulation for the investigative method in terms of the three normative requirements are summarised in subsection 7.5.1. The specific recommendations that arise from these results are presented in subsection 7.5.2.

7.5.1 Summary of conclusions

Section 7.1 analysed the accessibility of the Dutch legal framework for online undercover investigative methods. In the Netherlands, detailed regulations for undercover investigative methods are created in the DCCP. The Dutch legislature already stated in 1997 that the special investigative powers that

regulate undercover investigative methods are also applicable in the context of the Internet. An indication of the applicable regulations for the investigative methods is thus provided in the Dutch law. As a result, the Dutch legal framework for online undercover investigative methods should be regarded as accessible.

In section 7.2, the analysis of the foreseeability of online undercover investigative methods showed that (1) the scope of the investigative method of online pseudo-purchases and (2) the manner in which Dutch law enforcement authorities exercise the investigative power for pseudo-purchases are clear. The legal basis in Dutch criminal procedural law for applying the investigative method of online undercover interactions with individuals is not sufficiently clear. Online undercover interactions require the application of a special investigative power once the investigative method is applied 'systematically'. However, due to a lack of guidance in (1) statutory law, (2) the explanatory memoranda of the Special Investigative Powers Act and the Computer Crime Act II, (3) case law, and (4) the Guideline for Special Investigative Powers, it is unclear at what point the application of this method becomes systematic. Finally, online infiltration operations are regulated in detail by the special investigation order for infiltration in Dutch criminal procedural law. The examined legal sources indicate with sufficient clarity the (1) scope of the investigative method and (2) the manner in which the method is applied.

The analysis of the desired quality of the law conducted in section 7.3 showed that the Dutch legal framework does not meet the desired quality of the law for all three online undercover investigative methods. The detailed regulations for online pseudo-purchases, which include mandatory authorisation from a public prosecutor and restriction to serious crimes, are deemed to be of sufficient quality. When this digital investigative method is applied, risks related to both entrapment and the integrity of the investigation appear lower than for the other two digital investigative methods. With regard to the regulations for (1) online undercover interactions with individuals involved in criminal investigations and (2) online infiltration operations, the preferable involvement of an investigative judge is notably absent. Both investigative methods seriously interfere with the involved individuals' right to privacy and generate risks related to the integrity of criminal investigations. Furthermore, based on the desired quality of the law that has been derived from art. 6 ECHR, the involvement of an investigative judge is appropriate for all undercover investigative methods that entail a higher risk of entrapment. The involvement of an investigative judge in these investigative methods is therefore merited.

7.5.2 Recommendations

Section 7.4 presented five recommendations to improve the Dutch legal framework for online undercover investigative methods. These recommendations followed the analysis of the adequacy of the Dutch legal framework

based on the three normative requirements in sections 7.1 to 7.3. These recommendations are as follows.

1. The special investigative power to conduct a pseudo-purchase should be amended by removing the redundant text stating that data can be purchased that is 'stored or transferred by an automated device through the intermediary of public telecommunication network'.
2. The Dutch legislature should create a more foreseeable legal basis for the application of the investigative method of undercover online interactions with individuals. A special investigative power should regulate the use of this investigative method that indicates more clearly that it involves undercover interactions with suspects or individuals in their direct environment.
3. The Dutch legislature should improve the quality of the law for the special investigative power for systematic information gathering by requiring the supervision of an investigative judge. This improvement is suggested considering the risks related to undercover operations, which include the serious risk of entrapment and risks regarding the integrity of criminal investigations. The prohibition of entrapment should also apply to the special investigative power for systematic information gathering.
4. The Dutch legislature should also improve the special investigative power for systematic information gathering by restricting the application of this special investigative power to criminal investigations involving the more serious crimes defined in art. 67 DCCP. This improvement is suggested considering the seriousness of the privacy interference that accompanies the application of this undercover investigative method.
5. The Dutch legislature should require the involvement of an investigative judge to supervise online infiltration operations that necessitate the application of the special investigative power for infiltration. This improvement is suggested considering the risks related to undercover operations, which include the serious risk of entrapment and risks regarding the integrity of criminal investigations.