TILT (TILBURG INSTITUTE FOR LAW, TECHNOLOGY, AND SOCIETY)
LAW & TECHNOLOGY
WORKING PAPER SERIES

Sewage Monitoring for Criminal Investigation and the Protection of Home Life

Bert-Jaap Koops[1], Ivan Škorvánek[1], and Bart van der Sloot[1]

TILT, Tilburg University, The Netherlands

I.Skorvanek@uvt.nl, e.j.koops@uvt.nl, B.vdrSloot@uvt.nl

TILT Law & Technology Working Paper No. 005/2019
24 April 2019, Version: 1.0

This paper can be downloaded without charge from the
Social Science Research Network Electronic Paper Collection
http://ssrn.com/abstract=3377481

An overview of the TILT Law & Technology Working Paper Series can be found at:
http://www.tilburguniversity.nl/faculties/law/research/tilt/publications/workingpapers/

Abstract

The fundamental right to inviolability of the home has traditionally been interpreted to protect people from physical intrusions into their homes. The growing use of technologies for non-physical intrusion into the home, enabling surveillance from the outside by law enforcement, makes home life more transparent without investigating officers having to physically enter. Sewage monitoring is an emerging new form of surveillance of the home from the outside, which potentially impacts the level of protection of home life in practice and in the law. The purpose of this paper is to survey forms of surveillance of the home similar to sewage monitoring, describe how German, Polish and Dutch law regulate these forms of surveillance, and suggest improvements to the legal framework so that people's fundamental right to protection of their home life remains sufficiently safeguarded. We group surveillance of the home from the outside into five groups: waste monitoring, monitoring of emanations, audio-visual surveillance, access to data in the home, and out-of-home access to data about home life. Our analysis shows that visual surveillance, acoustic surveillance, and access to data in and about the home are relatively well-regulated, usually with a sufficiently clear legal basis and considerable safeguards, thus offering generally adequate legal protection. In contrast, regulation of domestic waste (garbage and sewage) monitoring and monitoring of emanations from the home (heat, smell, electromagnetic waves) is less clear. Although these surveillance measures seem less serious interferences with inviolability of the home, law-makers should clarify the legal basis for these methods and the conditions applying to them. We conclude that legal systems will need to develop ways to more clearly distinguish between minor, more than minor, and very serious interferences with inviolability of the home. The Dutch systematicness requirement and the German protection of the core area of private life are useful starting points for developing a more comprehensive normative framework that can deal with non-physical intrusions of the home as well as current legal frameworks regulate physical intrusions of the home.

Keywords

privacy, sewage monitoring, surveillance, drugs, home life, home protection, fundamental rights

Sewage Monitoring for Criminal Investigation and the Protection of Home Life[1]

Version 1.0, April 2019

Bert-Jaap Koops,[2] Ivan Škorvánek,[3] and Bart van der Sloot[4]

Table of Contents

[1] The research for this paper was part of a project that received funding from the European Union's *Horizon 2020 research and innovation programme* under grant agreement No 653626. The research was conducted from mid-2016 to mid-2018 and reflects the legal situation as of mid-2018.
[2] Bert-Jaap Koops is Professor of Regulation and Technology at TILT – Tilburg Institute for Law, Technology, and Society, Tilburg University, the Netherlands.
[3] Ivan Škorvánek is PhD researcher at TILT – Tilburg Institute for Law, Technology, and Society, Tilburg University, the Netherlands.
[4] Bart van der Sloot is senior researcher at TILT – Tilburg Institute for Law, Technology, and Society, Tilburg University, the Netherlands.

Abbreviations

Awbi	Algemene wet op het binnentreden [General Entering Act, the Netherlands]
BKA	Bundeskriminalamt [Federal Criminal Police, Germany]
BKAG	Bundeskriminalamtgesetz [Act governing the Federal Criminal Police Office, Germany]
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
GG	Grundgesetz [Basic Law, Germany]
Gw	Grondwet [Constitution, the Netherlands]
HR	Hoge Raad [Supreme Court, the Netherlands]
IoT	Internet of Things
KPK	Kodeks postępowania karnego [Code of Criminal Procedure, Poland]
LEA	Law Enforcement Agency
NJ	Nederlandse Jurisprudentie
PA	Police Act [Poland]
Rn	Randnummer [marginal number, reference system in German doctrinal texts]
StPO	Strafprozeßordnung [Code of Criminal Procedure, Germany]
Sv	Wetboek van Strafvordering [Code of Criminal Procedure, the Netherlands]

Summary

This paper provides an overview of the relation between sewage monitoring and similar forms of covert surveillance, in relation to the right to protection of the inviolability of the home. This right has traditionally been interpreted to protect people from physical intrusions into their homes. The growing use of forms of non-physical intrusions into the home, of which sewage monitoring is a new example, makes home life more transparent to government agents who no longer have to rely on physical entering. This potentially impacts the level of protection that home life enjoys in practice and in the law. The purpose of this paper is to create an inventory of forms of surveillance of the home similar to sewage monitoring, describe how German, Polish and Dutch law regulates these forms of surveillance, and suggest improvements to the legal framework so that people's fundamental right to protection of their home life remains sufficiently safeguarded.

Sewage monitoring and similar forms of surveillance can be very useful and valuable in the fight against crime, including as tools for detecting illicit production of synthetic drugs. However, as with any new technology, together with the benefits, potential negative consequences must also be considered, including their interference with fundamental rights, such as the right to protection of home life. Whereas sewage monitoring is unlikely to be specifically regulated in the law, it is useful to look at similar measures and how they have been regulated, on order to determine its place in criminal procedure law and the proper safeguards that should be placed on its use.

In this paper, the main forms of surveillance of the home from the outside are grouped into five broader groups: waste monitoring, monitoring of emanations, audio-visual surveillance, access to data in the home, and out-of-home access to data about home life. The European Convention of Human Rights and the protection of the home in the national constitutions (with the exception of the Netherlands) protects individuals not only against physical entry of the home but also from outside monitoring of home life. Thus, strict safeguards must be applied to the use of these forms, especially the more intrusive ones. The legal basis for home monitoring appears to be sufficiently clear and largely to have sufficiently strong safeguards in the cases of visual surveillance, acoustic surveillance, and access to data in and about the home. For these measures, the legal protection is generally found to be adequate. In Poland, the protection might be strengthened where the law defines possibly overly broad surveillance powers, and the Polish provision on operational measures (Art. 19 Police Act) should be made more technology-neutral, so that it can cover more forms of surveillance with its relatively strict safeguards.

There is less legal clarity with regard to domestic waste monitoring and monitoring of emanations from the home. These forms are not explicitly regulated in the law, and case law is relatively scarce. The available case law suggests that these forms of surveillance are generally considered less intrusive than audio-visual surveillance and subject to lower safeguards. In principle, no legislative change is needed to improve protection of the home against such relatively less intrusive forms. Most of these measures, with the technology currently available or in the form currently implemented, do not appear particularly intrusive in terms of interfering with the inviolability of the home. This is the case with sewage monitoring in its most immediately likely implementation, which focuses only on identifying very specific, crime-related, chemical substances in sewage waste. In the jurisdictions we studied, this constitutes only a minor interference with the inviolability of the home.

However, we do recommend to increase legal clarity with regard to these forms of surveillance, either by legislative change or by authoritative interpretation of existing provisions. This is relevant because of the general lack of authoritative case law, which may lead to legal uncertainty about the legal basis for these methods and the conditions applying to them. Moreover, depending on the technical capabilities of the monitoring systems and the set-up of the monitoring, the level of intrusion might increase in the future, requiring a more explicit and specific legal basis and appropriate legal safeguards. In that light, the legal systems will need to develop ways to more clearly distinguish in the law between minor, more than minor, and very serious intrusions of the inviolability of the home. The systematicness requirement in the Netherlands and the protection of the core area of private life in Germany are useful starting points for developing a more comprehensive normative framework that can regulate non-physical intrusions of the home as well as the current normative frameworks can regulate physical intrusions of the home.

1. Introduction

1.1. Background, aim, and scope

This paper analyses the fundamental right to protection of home life in relation to new surveillance measures that allow monitoring the home from the outside for criminal investigation purposes, such as sewage monitoring. Currently, legal frameworks protecting against private-life intrusions are rapidly becoming disconnected, as traditionally, the constitutional protection of home life applies to physical intrusions of the home, but not to outside monitoring of in-home life that can be done without touching the home (based on the assumption that walls shield sound and curtains shield vision). Now that technologies such as thermal imagers, smart energy meters, domotics and the Internet of Things, facilitate sensing from outside what happens inside the home much more than was possible in times when constitutional protection of home life developed, it becomes urgent to reflect on how home life is protected, since outside monitoring of in-home life can have a considerable chilling effect on people's behaviour in the most private place available. Sewage monitoring has important implications in this respect, since much information about home life can potentially be inferred from sewage waste (e.g., food patterns, medicine use). Although sewage monitoring systems for criminal investigation will only be targeted at investigating the production of illicit substances, such as synthetic drugs, the potential chilling effect on home life needs to be taken into consideration.

Systems are being developed for sewage monitoring for criminal investigation purposes. For example, in the European µMole project,[5] a sensor system is developed to track down the production of illicit substances. The system would be placed in the sewer, monitor waste flow, and take samples that could indicate, for instance, drugs production. The information retrieved by such a system could serve as evidence in itself (if it complies with forensic standards of evidence collection), but could also function as a trigger for follow-up investigation activities, such as search and seizure in particular premises identified as the likely source of drugs production. Such sewage monitoring systems could be used in a targeted way, as part of an on-going investigation based on existing suspicion of illicit substance production, but also in a broader, exploratory way, to scan wider parts of the sewage system, to identify and narrow down possible areas where drugs might be being produced.

For the purpose of this paper, we will abstract away from specific use cases and focus more generally on sewage monitoring of domestic waste, including hypothetical future uses, as well as on similar forms of covert surveillance of in-home activities in the context of law enforcement. This approach reflects the recognition that sewage monitoring as being developed in projects such as µMole is part of a broader trend related to the emergence of new ways allowing the law enforcement to sense what is happening inside private premises while staying on the outside. Since the traditional constitutional and statutory protection of home life applies primarily to physical intrusions into the home, the emergence of these forms of home monitoring from the outside creates a significant challenge to the protection of home life. Sewage monitoring (depending on which substances are monitored, and to what extent) potentially enables a significant amount of information from inside private homes to be revealed. Therefore, the emergence of sewage monitoring by law enforcement calls for reflection on how this and other similar forms of surveillance of home life are to be regulated.

In this paper, we build on the research in a parallel working paper on the criminal procedure implications of sewage monitoring,[6] and provide a more comprehensive inventory of similar forms of surveillance, describing how these forms are regulated in Germany, Poland, and the Netherlands. These countries were selected as the main countries involved in the project in the context of which the research for this paper was conducted. We also discuss the case law of the European Court of Human Rights, since its interpretation of Art. 8 of the European Convention on Human Rights is binding in these jurisdictions. For purposes of comparison and enrichment of the

[5] See http://micromole.eu/.
[6] Škorvánek et al. 2019. Since both papers discuss the same case of sewage monitoring (albeit from different perspectives), but are intended to be read independently from each other, we have reused some minor text parts of the previous paper in this paper.

discussion by potentially introducing inspiring solutions to similar problems, we also briefly describe how courts in the main common-law countries (United States, United Kingdom, Canada) have dealt with these forms of surveillance. The goal of this exercise is to assess to what extent people are protected from non-physical intrusions of home life in these jurisdictions, which allows us to compare the level of protection across these countries and identify weak spots or inconsistencies of the protection regime. Based on the comparison of different types of monitoring of the home and different legal systems, we can draw conclusions on sewage monitoring and its impact on the right to protection of home life, and whether more concrete and/or stricter regulation of sewage monitoring in the context of criminal investigation should be considered in order to adequately protect the right to inviolability of the home.

1.2. Methodology

The research for this paper was based on doctrinal legal analysis methods, which combines desk research of literature with analysis of statutory law, case law, and legal doctrinal literature, with a view to assessing how existing law applies to a certain activity (in this case, various forms of surveillance of the home from the outside). Since the critical conceptual analysis conducted within the legal-doctrinal methods aims to reveal a statement of the law relevant to the matter under investigation,[7] it is primarily concerned with understanding the meaning of legal rules and principles. Legal rules are formulated in natural language, which, by its nature, is open to interpretation. The process of formulating doctrines, therefore, relies on an (inter)subjective, argument-based methodology that differs from the empirical, data-based methods of social and natural sciences. As a result, the validity of the doctrinal method relies upon developing an interpretation of the law that is convincing to the legal community, based on arguments.[8]

Doctrinal legal research relies primarily on describing the applicable law and offering interpretation of the law. In doing so, the researcher has to keep in mind various guiding principles of the law. For instance, the hierarchy of norms refers to the idea that legal norms are organised vertically in such a way that the norms appearing lower in this order must comply with all the norms on the higher level. For this reason, we first discuss the European Convention on Human Rights, which takes precedence over national laws. Second, we discuss the constitutional law that includes legal norms of the highest level in domestic law. Last, we describe the lower level, statutory legal norms, which derive their validity from the constitutional law. The civil law systems of continental Europe are based on written legal norms (Constitutions, statutes). Judicial decisions are generally applicable only to individual cases and do not constitute formal sources of law, although the interpretation of the high courts (e.g. the federal Constitutional Court or the Supreme Court) is usually binding for the lower courts in future decision-making and has a significant impact on the state of applicable law. Furthermore, even decisions that do not form precedent for future judgements provide strong indications of how particular legal rules are applied in the jurisdiction at hand. Therefore, our analysis relies on both written law and case-law, but the focus may differ per jurisdiction due to varying institutional set-up (e.g. absence of a Constitutional Court in the Netherlands) and legal culture.

1.3. Outline

In Section 2, the constitutional framework of protection of home life will be briefly outlined. The focus will be on the protection of home in art. 8 of the European Convention on Human Rights and the protection in the constitutions of Germany, Poland and the Netherlands. Special focus will be given to the identification of the core values protected in these constitutional provisions, and specifying to what extent the protection extends to surveillance activities that are not connected to physical intrusion into the protected space.

[7] Terry C. Hutchinson, 'Valé Bunny Watson? Law Librarians, Law Libraries, and Legal Research in the Post-Internet Era' (2014) 106 Law Library Journal 579, 584.
[8] Paul Chynoweth, 'Legal Research' in A Knight and L Ruddock (eds), *Advanced Research Methods in the Built Environment* (Wiley-Blackwell 2008) 30.

In Section 3, an inventory will be made of the various forms of covert surveillance of in-home activities. Where appropriate, this section includes a comparison how these forms relate to sewage monitoring.

In Section 4, the criminal law systems of Germany, Poland and the Netherlands will be discussed, focusing on how these jurisdictions regulate covert surveillance of the home from the outside by the law enforcement. Legal provisions providing legal basis for such activities will be outlines and, where available, case law and doctrine dealing with particular forms of surveillance described in Section 3 will be presented. The principal aim of this section will be to describe how the jurisdictions protect people from non-physical intrusions of home life and to identify promising concepts and doctrines that can be used to strengthen the legal protection in light of developments in technology and surveillance. For this purpose, the last part of Section 4 will look at case law and doctrine of common law countries (USA, UK, Canada) in order to compare how these countries are dealing with the issue and potentially to identify interesting solutions.

Section 5 will focus on recommendations for improvement. Focusing on the legislative frameworks in Germany, Poland and the Netherlands, as described in Section 4, this section will make suggestions for improving and strengthening these legal frameworks in order to protect home life from non-physical intrusions.

2. Fundamental right to protection of home life

2.1. Protection of home life in the European Convention on Human Rights

The European Convention on Human Rights (ECHR) is supervised by the European Court of Human Rights (ECtHR). It is an instrument by the Council of Europe, to which 47 European countries are member. Together with the European Union's (EU) Charter for Fundamental Rights, which applies only to the 28 Member States of the European Union, the ECHR is the most important legal document in Europe. Germany, the Netherlands and Poland are member to both the Council of Europe and the European Union. Article 8 of the Convention contains the right to privacy:

> ARTICLE 8
>
> Right to respect for private and family life
>
> 1. Everyone has the right to respect for his private and family life, his home and his correspondence.
>
> 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.[9]

This section will briefly describe three aspects of this article, in so far as they are relevant for the purposes of this paper. First, it will analyse the scope of the concept of 'home' contained in article 8 ECHR (section 2.1.1). Second, it will provide three categories of intrusions upon the home, namely the physical intrusion (section 2.1.2), the non-physical intrusion (section 2.1.3) and the chilling effect (section 2.1.4). Thirdly and finally, it will suggest that even if a building falls under the concept of 'home' and even if a certain tool for monitoring can be considered an 'intrusion' upon this aspect of the right to privacy, this does not mean per se that there will be a violation of Article 8 ECHR. If the intrusion is based on a law, serves a legitimate aim and can be considered necessary to achieve that aim, the intrusion will be deemed legitimate (section 2.1.5).

[9] Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) (ECHR) art 8.

2.1.1. The scope of the 'home'

In the early jurisprudence of the former European Commission of Human Rights and the European Court of Human Rights,[10] it was held that a second home, a building site, a professional working place, a temporary shelter or other unconventional houses did not fall under the scope of 'home'.[11] However, this approach has been overturned in later case law by the Court. The Convention is drafted in two official languages, English and French, and like the Declaration, the French version of the European Convention does not refer to 'maison', 'chez' or 'résidence' but rather to the concept 'domicile'. Domicile has a broader scope than the concept of 'home' and might, for example, be used to refer to professional dwellings. In its more recent case law, it is the concept of 'domicile', rather than 'home', that is increasingly referred to by the Court.

The Court has held as principle that the concept of 'home' is not limited to those buildings which are lawfully occupied or which have been lawfully established.[12] Accepting caravans and other mobile homes and temporary shelters under the concept of 'home' has had important consequences for Roma and other nomadic groups,[13] who generally do not possess a fixed shelter or home.[14] This doctrine has gradually been expanded to include certain minority rights and the protection of minority life styles.[15]

Not only is the home of importance to the quality of one's life, the private life and the group life one pursues, it is also of the essences for the protection of the family life. The European Court of Human Rights has referred to 'the applicant's right to respect for her "home", a right which is pertinent to [the applicant] and her children's personal security and wellbeing.'[16]

Finally, it is important to stress that even working environments can, under certain conditions, be considered 'home'.[17] The concept extends to a professional person's office or business premises,[18] a newspaper's premises,[19] a notary's practice,[20] or a university professor's office.[21] It also applies to a registered office, and to the branches or other business.[22] In a seminal judgement, the ECtHR held that

> the Convention is a living instrument which must be interpreted in the light of present-day conditions. As regards the rights secured to companies by the Convention, it should be pointed out that the Court has already recognized a company's right under Article 41 to compensation for non-pecuniary damage sustained as a result of a violation of Article 6 § 1 of the Convention. Building on its dynamic interpretation of the Convention, the Court considers that the time has come to hold that in certain circumstances the rights guaranteed by Article 8 of the Convention may be construed as including the right to respect for a company's registered office, branches or other business premises. In the instant case, the Court observes that during a large-scale administrative investigation, officials from the DGCCRF went to the applicant companies' head offices and branches in order to seize several

---

[10] The sections below are partially based on: B. van der Sloot, 'Privacy as Personality Right: Why the ECtHR's Focus on Ulterior Interests Might Prove Indispensable in the Age of "Big Data"' (2015) 31 Utrecht Journal of International and European Law 25.
[11] *X. v. Belgium* App no 5488/72 (Commission Decision, 30 May 1974).
[12] *McKay-Kopecka v. Poland* App no 45320/99 (ECtHR, 19 September 2006), *McGonnell v. UK* App no 28488/95 (ECtHR, 8 February 2000).
[13] *Lay v. UK* App no 13341/87 (Commission Decision, 14 July 1988).
[14] *Smith v. UK* App no 14455/88 (Commission Decision, 4 September 1991), *Smith v. UK* App no 18401/91 (Commission Decision, 6 May 1993).
[15] See e.g. *G. and E. v. Norway* App no 9278/81 (Commission Decision, 3 October 1983).
[16] *Buckley v. the United Kingdom* App no 20348/92 (ECtHR, 25 September 1996).
[17] For this section, use has been made of the documents produced by the Council of Europe, in particular: <https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf>, <https://www.echr.coe.int/LibraryDocs/Roagna2012_EN.pdf> and <https://www.echr.coe.int/Documents/FS_Own_image_ENG.pdf>.
[18] *Buck v. Germany* App no 41604/98, (ECtHR 28 april 2005), *Niemitz v. Germany* App no. 13710/88, (ECtHR, 16 December 1992).
[19] *Saint-Paul Luxembourg S.A. v. Luxembourg* App no 26419/10 (ECtHR, 18 April 2013).
[20] *Popovi v. Bulgary* App no 39651/11 (ECtHR, 09 June 2016).
[21] *Steeg v. Germany* App nos 9676/05 10744/05 41349/06 (ECtHR, 03 June 2008).
[22] *Kent Pharmaceuticals limited and others v. the United Kingdom* App no 9355/03 (ECtHR, 11 October 2005).

> thousand documents. It notes that the Government did not dispute that there had been interference with the applicant companies' right to respect for their home, although they argued that the companies could not claim a right to the protection of their business premises "with as much force as an individual could in relation to his professional or business address" and that, consequently, the entitlement to interfere "might well be more far-reaching".[23]

In conclusion, although not every remote barn containing a synthetic drug lab will fall under the concept of 'home', there are many instances where the building containing a drug lab might do so. When labs are exploited from locations where people sleep, this will be the case as a matter of principle. Whether the site is occupied illegally has no bearing on the question of whether the location can be qualified as a 'home' in legal terms. Even if the location is only used for (illegal) business activities, and not for personal reasons, it may be qualified as a 'home' under the right to privacy as contained in the European Convention on Human Rights.

The following three sub-paragraphs will describe three types of potential intrusions: physical intrusions, non-physical intrusions and the chilling effect.

2.1.2. Physical intrusion

Traditional intrusions upon the right to respect for the home are deliberate destruction of the home by the authorities[24] or confiscation,[25] refusal to allow displaced persons to return to their homes,[26] the transfer of the inhabitants of a village by decision of the authorities,[27] police entry into a person's home[28] and searches[29] and seizures,[30] occupation or damaging of property[31] or expulsion from home,[32] including an eviction order which has not yet been enforced,[33] changes to the terms of a tenancy,[34] loss of one's home on account of a deportation order,[35] impossibility for a couple, under the immigration rules, to set up home together and live together in a family unit,[36] decisions regarding planning permission,[37] compulsory purchase orders,[38] a person's inability to have their name removed from the register of permanent residences[39] and an obligation to obtain a license to live in one's own house and imposition of a fine for unlawful occupation of own property.[40]

Importantly, cooperation with the police by citizens does not mean that there is no interference on the right to the sanctity of one's home:

> The Court reiterates, first of all, that the notion of "home" in Article 8 § 1 does not only encompass a private individual's home. The word "domicile" in the French version of Article 8 has a broader connotation than "home" and may, for example, also refer to a professional person's office. Consequently, "home" is to be construed as including also the registered office of a company run by a private individual and a legal entity's registered office, branches or other business premises, as in the case of the applicant company. The fact that the journalist and other employees of the applicant

---

[23] *Stes Colas Est and others v. France* App no 37971/97 (ECtHR, 16 April 2002).
[24] *Selcuk and Asker v. Turkey* App nos 23184/94 23185/94 (ECtHR, 24 April 1998), *Akdivar and others v. Turkey* App no 21893/93 (ECtHR, 16 September 1996), *Mentes and others v. Turkey* App no 23186/94 (ECtHR, 28 November 1997).
[25] *Aboufadda v. France* App no 28457/10 (ECtHR, 04 November 2014).
[26] *Cyprus v. Turkey* App no 25781/94 (ECtHR, 10 may 2001).
[27] *Noack and others v. Germany* App no 46346/99 (ECtHR, 25 May 2000).
[28] *Gutsanovi v. Bulgaria*, App no 34529/10 (ECtHR, 15 October 2013).
[29] *Murray v. The United Kingdom* App no 14310/88 (ECtHR, 28 October 1994).
[30] *Chappell v. the United Kingdom* App no 10461/83 (ECtHR, 30 March 1989), *Funke v. France* App no 10828/84 (ECtHR 25 February 1993).
[31] *Khamidov v. Russia* App no 72118/01 (ECtHR, 15 November 2007).
[32] *Orlic v. Croatia* App no 48833/07 (ECtHR, 21 June 2011).
[33] *Gladysheva v. Russia* App no 7097/10 (ECtHR, 06 December 2011), *Cosic v. Croatia* App no. 28261/06 (ECtHR, 13 January 2009).
[34] *Bertger-Krall and others v. Slovenia* App no 14717/04 (ECtHR, 12 June 2014).
[35] *Slivenko v. Latvia* App no 48321/99 (ECtHR, 09 October 2003).
[36] *Hode and Abdi v. The United Kingdom* App no 22341/09 (ECtHR 06 November 2012).
[37] *Buckley v. the United Kingdom* App no 20348/92 (ECtHR, 25 September 1996).
[38] *Howard v. The United Kingdom* App no 10825/84 (Commission Decision 16 July 1987).
[39] *Babylonova v. Slovakia* App no 69146/01 (ECtHR, 20 June 2006).
[40] *Gillow v. The United Kingdom* App no 9063/80 (ECtHR, 24 November 1986).

> company cooperated with the police cannot be construed as making the search and the associated seizure less intrusive. The Court has already had occasion to find that cooperation under threat of a search cannot cancel out the interfering nature of such an act. Nor has it been alleged in the present case that failure to cooperate would have prevented the police officers from executing the legal warrant entrusted to them. On the contrary, the police officers had made clear that they could carry out the measure by force in the event of a refusal to cooperate. The Court therefore considers that the search and the seizure carried out in the applicant company's registered office must be construed as "interference" in the exercise of the applicant company's rights under Article 8 § 1 of the Convention.[41]

Furthermore, the fact that the offence giving rise to the search had been committed by a third party is irrelevant. In the case of *Buck v. Germany*, the applicant complained that the search of his business and residential premises and the seizure of documents, which had been ordered by the District Court, had been in breach of his right to respect for his home. He argued in particular that, in the context of investigations into a contravention of a regulation committed by a third person, the search was disproportionate. The European Court of Human Rights stressed that governments, when taking measures to prevent disorder or crime and to protect the rights of others, may consider it necessary to resort to measures such as searches and seizures in order to obtain evidence of certain offences in a sphere in which it is otherwise impossible to identify the person guilty of the offence.

In that case, the Court continued to hold that: 'However, having regard to the severity of the interference with the right to respect for his home of a person affected by such measures, it must be clearly established that the proportionality principle has been adhered to. Having regard to the special circumstances of this case, in particular the fact that the search and seizure in question had been ordered in connection with a minor contravention of a regulation purportedly committed by a third person and comprised the private residential premises of the applicant, the Court concludes that the interference cannot be regarded as proportionate to the legitimate aims pursued.'[42] Consequently, the fact that a third party operates a drug lab from the property of another person does not meant that entering the home of that person will not be regarded as an intrusion upon his private life.

1.1.3 Non-physical intrusions

Besides entering the property of a person and other physical intrusions upon the right to the sanctity of one's home, the European Court of Human Rights has also accepted that there may be other, non-physical intrusions. In an early case from 1986, regarding the level of noise caused by airports in the vicinity of an individual's house, the Commission held that Article 8 ECHR 'cannot be interpreted so as to apply only with regard to direct measures taken by the authorities against the privacy and/or home of an individual. It may also cover indirect intrusions which are unavoidable consequences of measures not at all directed against private individuals. In this context it has to be noted that a State has not only to respect but also to protect the rights guaranteed by Article 8 para. 1. Considerable noise nuisance can undoubtedly affect the physical well-being of a person and thus interfere with his private life. It may also deprive a person of the possibility of enjoying the amenities of his home.'[43] In subsequent case law, it was accepted that similarly, noise nuisance produced by nuclear power plants working day and night in a rural area[44] and by nightclubs near someone's home interferes with the protection of the home.[45]

Sewage monitoring might itself be considered a non-physical intrusion upon the home of a suspect or his neighbours, as it may be used to monitor the home life without entering the premise itself. It may undermine the quality of someone's life, on subjective grounds, when it is known that sewage waste (including inhabitants' bodily excretions) is or can be monitored by the police. On the other hand, the state might be under a positive obligation to stop illegal drug

---

[41] *Saint-Paul Luxembourg S.A. v. Luxembourg* App no 26419/10 (ECtHR, 18 April 2013).
[42] *Buck v. Germany* App no 41604/98 (ECtHR, 28 April 2005).
[43] *Rayner v. UK* App no 9310/81 (Commission Decision, 16 July 1986).
[44] *Spire v. France* App no 13728/88 (Commission Decision, 17 May 1990).
[45] *Moreno Gomez v. Spain* App no 4143/02 (ECtHR, 16 November 2004), *Villa v. Italy* App no 36735/97 (ECtHR, 14 November 2000).

production, even under the scope of Article 8 ECHR, because of the environmental pollution it causes and the impact it might have on the quality of life of the neighbours – this may either be due to the smells drug production causes, because of the feeling of unsafety in one's home due to explosion danger, etc.

There are many forms of non-physical intrusion upon the right to private and family life, home and communication, as contained in article 8 of the European Convention of Human Rights. These may be fumes and smells, radiation and air position, noises and the subjective feeling that one's quality of life has diminished due to a certain living environment. For illegal drug production, this may mean two things. First, many investigative and monitoring tools deployed by the police may be considered an intrusion upon a person's home, even if the home of a suspect is not physically entered. Second, countries, under the European Convention on Human Rights, do not only have so-called 'negative obligations', that is to abstain from certain intrusions upon the rights of citizens; they also have 'positive obligations'. Because under the Convention, citizens can only complain about the conduct or lack thereof of states, and cannot submit a complaint against fellow citizens or private organizations, the European Court of Human Rights has stressed that citizens may also complain about the lack of protection by states against the intrusion upon their rights by private parties. Consequently, the state may have a positive obligation to combat illegal drug production, both in terms of safety and security and because environmental pollution, unhealthy and unsafe living environments and fumes, smells and noises may fall under the protective sphere of the right to privacy, as contained in the ECHR.

1.1.4 Chilling effect

Finally, a chilling effect may also constitute an interference with the right to privacy.[46] For a chilling effect to exist, there need not be a real intrusion (either physical or non-physical). The threat or possibility thereof may be enough. The doctrine of the chilling effect is primarily connected to the freedom of speech, as contained in Article 10 of the European Convention on Human Rights, and the Court uses it to explain that certain actions by the government, although not directly limiting the freedom of speech of its citizens, may lead to self-restraint: a chilling effect in the lawful use of a right. The chilling effect is the effect that exists when people know that they are watched or know that they might be watched and adapt their behaviour because of this knowledge. Afraid of the potential consequences, people may restrain their behaviour and abstain from certain acts which they perceive as possibly inciting negative consequences.[47]

The European Court of Human Rights is also willing to accept this doctrine in certain cases relating to Article 8 ECHR, primarily when they regard surveillance measures, but also in relation to laws that discriminate or stigmatize certain groups in society. Here, the Court is willing to accept that although no harm has been done yet to an applicant, he may still be received in his (a priori) claim if it is likely that he will suffer from harm in the future, either because he is curtailed in his right to privacy by the government or because he will resort to self-restraint in the use of his right.

This approach is becoming increasingly important in cases revolving around surveillance activities by the state, in which the Court is also willing to accept potential future harm and chilling effects. A good example may be the case of *Colon v. the Netherlands*, in which the applicant complained that the designation of a security risk area by the Burgomaster of Amsterdam violated his right to respect for privacy as it enabled a public prosecutor to conduct random searches of people over an extensive period in a large area without this mandate being subject to any judicial review. The government, to the contrary, argued that the designation of a security risk area or the issuing of a stop-and-search order had not in itself constituted an interference with the applicant's private life or liberty of movement. Since the event complained of, several preventive search operations had been conducted; in none of them had the applicant been subjected to further

---

[46] This sub-section is based on: B. van der Sloot, 'Is the Human Rights Framework Still Fit for the Big Data Era? A Discussion of the ECtHR's Case Law on Privacy Violations Arising from Surveillance Activities' in S. Gutwirth, R. Leenes and P. De Hert (eds), *Data protection on the move: current developments in ICT and privacy/data protection* (Springer 2016) 411.

[47] J. Bentham, *Panopticon; or, The Inspection House* (Dublin 1791), Michel Foucault, *Surveiller et punir: naissance de la prison* (Gallimard 1975).

attempts to search him. This was, according to the government, enough to show that the likelihood of an interference with the applicant's rights was so minimal that this deprived him of the status of victim.

The Court stressed, that in principle, it did not accept in abstracto claims or an actio popularis. 'In principle, it is not sufficient for individual applicants to claim that the mere existence of the legislation violates their rights under the Convention; it is necessary that the law should have been applied to their detriment. Nevertheless, Article 34 entitles individuals to contend that legislation violates their rights by itself, in the absence of an individual measure of implementation, if they run the risk of being directly affected by it; that is, if they are required either to modify their conduct or risk being prosecuted, or if they are members of a class of people who risk being directly affected by the legislation.'[48] It went on to stress that it was 'not disposed to doubt that the applicant was engaged in lawful pursuits for which he might reasonably wish to visit the part of Amsterdam city centre designated as a security risk area. This made him liable to be subjected to search orders should these happen to coincide with his visits there. The events of 19 February 2004, followed by the criminal prosecution occasioned by the applicant's refusal to submit to a search, leave no room for doubt on this point. It follows that the applicant can claim to be a "victim" within the meaning of Article 34 of the Convention and the Government's alternative preliminary objection must be rejected also.'[49]

The applicant was left only the choice between two evils: either he avoided traveling to the capital city of the Netherlands or he risked being subjected to surveillance activities. This is enough for the Court to accept a victim status, which it has reaffirmed in later jurisprudence.[50] The analogy to sewage monitoring is obvious. If people are aware that in their neighbourhood or city, sewage monitoring will be applied, they may be mindful about what they flush down the drain. When their sewage is or might be monitored, they are faced with a choice: either they subject themselves to monitoring or they avoid using the sewage. Most likely, the European Court on Human Rights will find that this qualifies as an interference, even if the person in question could avoid being monitored by using other sewage systems of using tools for obfuscation.

1.1.5 Legitimation

The right to privacy under the European Convention on Human Rights is a so-called qualified right.[51] This means that Article 8 ECHR specifies under which conditions the right can be legitimately curtailed by the government; these conditions are listed in paragraph 2 of Article 8 ECHR, which specifies: 'There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.' Consequently, if the government infringes on a person's privacy, for example by entering his home, this need not be illegitimate or a violation of his privacy. The infringement can be deemed in harmony with the European Convention on Human rights when it abides by three cumulative requirements: (1) the infringement must have a legal basis; (2) must serve one of the legitimate goals as listed in the second paragraph of Article 8 ECHR; and (3) must be necessary in a democratic society.

There may be a number of reasons why no violation of Article 8 ECHR is found. For example, because the Court finds that a case has been wrongfully declared admissible, because a settlement has been reached by the parties in the meantime and the case needs to be struck from the list, or because a violation of another provision under the Convention has been established, and the Court finds it unnecessary to determine whether there has also been a separate violation of the right to privacy (the ECtHR may, for example, hold that in a case, a person's right to freedom from torture (Article 3 ECHR) had been violated and find it unnecessary to analyse to what extent the torture also violated a person's right to privacy). These are

---

[48] *Colon v. the Netherlands* App no 49458/06 (ECtHR, 15 May 2012).
[49] Ibid, § 60.
[50] *Ucar and others v. Turkey* App no 4692/09, (ECtHR, 24 June 2014).
[51] This sub-section is based on: B. Van der Sloot, 'Where Is the Harm in a Privacy Violation? Calculating the Damages Afforded in Privacy Cases by the European Court of Human Rights' (2017) 8 JIPITEC 322.

preliminary and procedural reasons. Alternatively, the ECtHR may find that although there has been an infringement of the right to privacy (as provided in paragraph 1 of Article 8 ECHR), this was a legitimate one and thus not in violation of Article 8 ECHR. The ECtHR only reaches this conclusion if all three requirements (legal basis, legitimate aim, necessary) have been fulfilled; if the government fails to fulfil either one of these requirements, a violation of the right to privacy will be found.

The Court may find that an infringement was not prescribed for by law for a number of reasons – the 'law', in this sense, is always the national law of a country. The ECtHR uses a quite wide definition of law, it includes not only legislation, but also judge-made law typical of common law jurisdictions and secondary sources, such as royal decrees and internal regulations. First, a violation of the Convention will be found on this point if the actions of governmental officials are not based on a legal provision granting them the authority to act in the way they did. Second, a violation will be established if the conditions as specified in the law for using certain authority have not been complied with, for example, if police officials have no warrant for entering the home of a citizen. Third, the actions of the governmental officials may be prescribed for by law, but the law itself may not be sufficiently accessible to the public. Fourth, the law may be so vague that the consequences of it may not be sufficiently foreseeable for ordinary citizens. Fifth and finally, the ECtHR has in recent years developed an additional ground, namely that the law on which actions are based does not contain sufficient safeguards against the abuse of power by the government. This typically applies to laws authorizing mass surveillance activities by intelligence agencies that set virtually no limits on their capacities, specify no possibilities for oversight by (quasi-) judicial bodies, and grant no or very limited rights to individuals, with respect to redress.[52]

The Court may also find a violation of Article 8 ECHR if the infringement serves no legitimate aim.[53] The second paragraph specifies a number of legitimate aims, primarily having to do with security related aspects, such as national security, public safety, and the prevention of crime and disorder. These terms are sometimes used interchangeably by the Court, but in general 'national security' is applied in more weighty cases than 'public safety', and 'public safety' in more weighty cases than the 'prevention of crime and disorder'. The right of privacy may also be legitimately curtailed to protect the rights and freedoms of third parties; for example, a child may be placed out of home (an infringement on the right to family life of the parents), because the parents sexually molested the child. The protection of health and morals may be invoked to curtail the right to privacy, though this category is applied hesitantly by the ECtHR, because the protection of the morals of a country may lead to quite restrictive rules. Still with respect to controversial medical issues, such as euthanasia, or sexual practices such as sadism or masochism, the ECtHR sometimes allows a country to rely on this ground to curtail the right to privacy. Finally, a country can rely on the 'economic wellbeing of the country'; this ground can only be found in Article 8 ECHR and in no other provision under the Convention. It is invoked by countries in a number of cases; for example, if an applicant complains about the fact that a factory or airport in the vicinity of his home violates his right to private life, the country can suggest that running a national airport is in fact necessary for the economic wellbeing of a country.

Much more can be said about the use, extent and interpretation of these aims, but this is unnecessary, because this requirement plays no role of significance. This is due to two factors. First, the ECtHR is often very unspecific about which term exactly applies, stressing that an infringement 'clearly had a legitimate aim', or that 'it is undisputed that the infringement served one of the aims as contained in Article 8 ECHR'. It often combines categories, underlining that the infringement served a legitimate aim, such as "'the prevention of crime', 'the economic well-being of the country' or 'the rights of others'" or it merely lists all different aims and holds that one of these grounds applies in the case at hand. Furthermore, it introduces new aims, not contained in Article 8 ECHR, especially in cases revolving around positive obligations for states (explained below). Second, the Court almost never finds a violation of Article 8 ECHR on this point. It usually allows the government a very wide margin of appreciation with respect to the question of whether

[52] See for instance *Zakharov v. Russia* App no 47143/06 (ECtHR 04 December 2015).
[53] B. van der Sloot, 'How to Assess Privacy Violations in the Age of Big Data? Analysing the Three Different Tests Developed by the ECtHR and Adding for a Fourth One' (2015) 24 Information & Communications Technology Law 74.

and which of the aims apply in a specific case and whether the infringement did actually serve that aim. In many cases, it simply ignores this requirement when analysing a potential violation of the right to privacy or incorporates it in the question of whether the infringement was necessary in a democratic society. Thus, only in twenty cases was Article 8 ECHR violated on this point.

Finally, the third requirement that must be fulfilled by a government wanting to curtail the right to privacy is that the infringement must be necessary in a democratic society. This question is approached by the Court primarily as a question of balancing the different interests at stake. 'This test requires the Court to balance the severity of the restriction placed on the individual against the importance of the public interest.'[54] Consequently, to determine the outcome of a case, the Court balances the damage a specific privacy infringement has done to the individual interest of a complainant against its instrumentality towards safeguarding a societal interest, such as national security.

As the European Court of Human Rights determines whether these three requirements have been met on a case-by-case basis, only very general things can be said about the admissibility of sewage monitoring to combat illegal drug production. Firstly, such monitoring should be based on a law, with a clear legal provision allowing for such investigative tool. The law must also contain sufficient mechanisms for control and oversight on the use of the competence of the police, the law may not provide for a blanket power and it must be foreseeable for citizens as to its effect and application. Secondly, there will in general be a legitimate aim for the purposes of Article 8 ECHR. Reference can either be made to aspects of safety, public order or the prevention of crime. With respect to the last aspect, the matter of necessity and balancing, in general, blanket sewage surveillance will not be allowed by the ECtHR. The more specific the form of monitoring, the more likely it is to be accepted. In addition, the Court requires that only those people are placed under surveillance against which the police has a reasonable suspicion.

2.2. Protection of home life in national constitutions

2.2.1. Germany

The inviolability of the home is protected in Art. 13 of the German Constitution (GG), which states that the home is inviolable. The subsections of Art. 13 specify various exceptions to this general principle. Subsection 2 allows searches authorized by a judge or other authorities when time is of the essence. Subsection 3 allows deployment of technical means of acoustical surveillance of homes, but only when a suspicion exists that a person has committed an especially serious crime. Acoustical surveillance must be ordered by a panel of three judges and the authorization shall be limited in time. Subsection 4 allows technical means of surveillance of the home, which include means other than acoustical, but only to avert acute dangers to public safety, especially dangers to life or to the public. This also needs to be ordered by a judge, unless time is of the essence, in which case other authorities designated by law can order it and obtain the judicial order at a later time. The use of technical means of surveillance of the home under subsections 3 and 4 shall be reported annually to the Bundestag, which shall exercise oversight over these surveillance measures.

The inviolability of the home, as evidenced above, protects primarily from physical entries, but its purpose as a spatial area of privacy can also be infringed if it is possible to monitor events in the dwelling by technical means.[55] This applies even when the home is monitored from the outside.[56] However, state intervention against the substance of the dwelling is not an infringement of Art. 13 GG, because it protects the undisturbed use of the home and not the existence of the dwelling.[57] The surveillance of private homes is a particularly serious intrusion of privacy. By its nature, it has a more serious impact than surveillance measures outside of private homes or than telecommunications surveillance. The weight of its interference is paralleled only by interferences

[54] F.G. Jacobs, R. White and C. Ovey, *Jacobs and White, the European Convention on Human Rights.* (3rd edn, OUP 2002) 209.
[55] BVerfGE 65, 1 (40) = NJW 1984, 419, BVerfGE 109 , 279 (309) = NJW 2004, 999 ff.
[56] Kluckert and Fink, 'GG Art. 13 [Unverletzlichkeit Der Wohnung]' in Epping and Hillgruber (eds), *BeckOK Grundgesetz* (37th edn, 2018) 8.
[57] ibid 9.

with information technology systems. For this reason, the appropriateness of such a measure can only be ensured if it is restricted from the outset to exclusively capturing conversations of the target person responsible for the threat.

In Germany, surveillance that allows observing the outside of private homes is clearly distinguished from that which targets the inside. The former interferes with constitutional protection of informational self-determination and the surveillance measures undertaken pursuant to it will, as must be ensured by technical means if need be, end at the doorstep.[58] The latter is considered a particularly serious interference with fundamental rights. It permits the state to penetrate into spaces that are a person's private refuge and that are closely linked to human dignity and interferes with the inviolability of the home protected by Art. 13 of the GG.[59] It is, however explicitly permitted in certain situations by Art. 13 secs. 3 and 4 GG. It is interesting to note that acoustic surveillance of the home is distinguished from other forms of monitoring (e.g. visual) and permitted in a wider array of situations.

Furthermore, the core area of private life is (almost) absolutely inviolable. The constitutional protection of the core area of private life guarantees a highly private area for the individual that is free from surveillance. It has its roots in each of the fundamental rights affected by surveillance measures in conjunction with Art. 1(1) GG and ensures a core of human dignity that is beyond the state's reach and provides constitutional protection against such measures. Even paramount interests of the general public cannot justify an interference with this absolutely protected area of private life.[60] The possibility of expressing inner processes such as impressions and feelings, as well as reflections, views, and experiences of a highly personal nature belongs to the free development of personality in the core area of private life. These conversations do no lose their overall highly personal character merely because they combine highly personal with everyday matters.[61] Particular protection is afforded to non-public communication with persons enjoying the highest level of personal trust, conducted under the reasonable assumption that no surveillance is taking place, as is the case, in particular, in a private home.[62] Although the protection of the core area is primarily based on human dignity protected in Art. 1 GG and not Art. 13 protecting the home, the home is important as a consideration in determining whether something falls under the core area or not. Generally, people can reasonably assume that they are not being monitored in their own private home.

In contrast, communication directly about criminal offences is not protected, not even when it also covers highly personal elements. The discussion and planning of criminal offences is not content that belongs to the core area of private life, but rather is of societal relevance.

2.2.2. Poland

In Poland, the right to inviolability of the home is protected in Art. 50 of the Constitution. In the literature, it is often connected to the general right to privacy, as guaranteed by Article 47 of the Polish Constitution.[63] The usual understanding of this term is a relative prohibition of search, unauthorized entry and stay in someone's closed house or any other space protected by the inviolability if the house without the consent of the owner or inhabitant.[64] This is, however, not a license to do anything inside the protected premises.[65] It is a right granted to not only natural, but also legal persons.[66]

The concept of home is understood broadly, which is in line with the jurisprudence of the European Court of Human Rights. It is not only the building, but rather a place of family seat

[58] BVerfG, Judgment of the First Senate of 20 April 2016 - 1 BvR 966/09, para. 148.
[59] BVerfG, Judgment of the First Senate of 20 April 2016 - 1 BvR 966/09, para. 180.
[60] BVerfGE 109, 279 (351) = NJW 2004, 999 (1012), para. 13.
[61] BVerfG, Judgment of the First Senate of 20 April 2016 - 1 BvR 966/09, para. 121.
[62] BVerfGE 109, 279 <321 et seq.>.
[63] Łukasz Kaczkowski, 'Nienaruszalność Mieszkania' in Mariusz Jabłoński (ed), *Realizacja i ochrona konstytucyjnych wolności i praw jednostki w polskim porządku prawnym* (E-Wydawnictwo 2014) 210.
[64] Marek Chmaj, *Wolności i Prawa Człowieka w Konstytucji Rzeczypospolitej Polskiej* (Seria Akademicka Prawo).
[65] Sabina Grabowska, Radosław Grabowski and Wiesław Skrzydło, *Konstytucja Rzeczypospolitej Polskiej. Komentarz Encyklopedyczny* (Wolters Kluwer 2009) 252.
[66] Marek Safjan and Leszek Bosek, *Konstytucja RP. Tom I. Komentarz do art. 1–86* (CH Beck 2016) 1216.

(*siedlisko rodzinne)* and the place where the family leads their life.[67] This is influenced especially by the judgement of the European Court of Human Rights in the *Buckley* case.[68] Moreover, as explained by Sierpowska, this has to do with the connection between the home and the possibility to develop family and social life.[69]

Furthermore, the inviolability also protects other spaces, which are not necessarily a house, but are not public either, as well as vehicles.[70] The inviolability of the home assumes also the possibility to freely use the premises and curtilages,[71] again motivated by the *Buckley* decision.[72] In literature, curtilage is defined as the entirety of homestead, non-residential buildings such as garage, as well as the garden.[73] What is more, the protection encompasses not only spaces meant for permanent stay, but also any other space which allows them to isolate themselves from the outside world. This can be a space used for commercial or professional activities.[74]

According to some authors, the protection of the home, although mainly mentioned in relation to searches, extends beyond the prohibition of physical intrusion. It also contains protections against more distant techniques and measures, such as installation of video cameras, wiretapping systems, or peeping.[75] This has to do with the immaterial aspect of the inviolability of the home, which encompasses the mental and emotional state induced by safety and undisturbed use of the home.[76]

2.2.3. The Netherlands[77]

The Dutch Constitution (*Grondwet, Gw*) contains a general right to privacy in article 10 para. 1 Gw: 'Everyone shall have the right to respect for his privacy [*persoonlijke levenssfeer*, literally: personal life sphere], without prejudice to restrictions laid down by or pursuant to Act of Parliament.'[78] Constitutional protection of the home is covered by article 12 Gw: 'Entry into a home against the will of the occupant shall be permitted only in the cases laid down by or pursuant to Act of Parliament, by those designated for the purpose by or pursuant to Act of Parliament.' Paragraphs 2-3 of article 12 require prior identification and ex post notification to the occupant, subject to statutory exceptions.[79]

---

[67] Paweł Sławicki, *Prawo Człowieka Do Mieszkania i Jego Miejsce w Systemie Praw Człowieka* (Currenda 2015) 123.
[68] *Buckley v. the United Kingdom* App no 20348/92 (ECtHR, 25 September 1996).
[69] Iwona Sierpowska, *Socjalne Aspekty Ochrony Prawa Do Mieszkania* (Koło Naukowe Doktryn Politycznych i Prawnych 2010) 279–280.
[70] Lech Garlicki and Krzysztof Gołyński, *Polskie Prawo Konstytucyjne: Wykłady* (Liber) 108.
[71] Sławicki (n 67) 124.
[72] *Buckley v. the United Kingdom* App no 20348/92 (ECtHR, 25 September 1996).
[73] Maksymilian Pazdan, 'Komentarz Do Art. 23' in Krzysztof Pietrzykowski (ed), *Maksymilian Pazdan, 'Komentarz Do Art. 23' in Krzysztof Pietrzykowski (ed), Kodeks cywilny. Tom I. Komentarz do artykułów 1–449* (CH Beck 2011) 139.
[74] Safjan and Bosek (n 66) 1220.
[75] Kaczkowski (n 63) 210.
[76] Pazdan (n 73) 139.
[77] For an overview of the Dutch constitutional protection of the home, see A.Q.C. Tak, *Het huisrecht*, diss. Utrecht, (Hoenderloo's Uitgeverij en Drukkerij 1973) and S.S. Buisman and S.B.G. Kierkels, 'Artikel 12 – Binnentreden Woning' in E. Hirsch Ballin and G.J. Leenknegt (eds), *De Grondwet. Artikelsgewijs commentaar*, online: http://www.nederlandrechtsstaat.nl/grondwet.html (last accessed 28 February 2019). For a general analysis of constitutional protection of privacy in the context of criminal law, see B.J. Koops, 'Criminal Investigation and Privacy in Dutch Law' (Social Science Research Network 2016) https://papers.ssrn.com/abstract=2837483 (last accessed 28 February 2019), on which the overview in this section builds.
[78] Constitution of the Kingdom of the Netherlands, official translation 2008, https://www.government.nl/documents/regulations/2012/10/18/the-constitution-of-the-kingdom-of-the-netherlands-2008.
[79] '2. Prior identification and notice of purpose shall be required in order to enter a home under the preceding paragraph, subject to the exceptions prescribed by Act of Parliament.
3. A written report of the entry shall be issued to the occupant as soon as possible. If the entry was made in the interests of state security or criminal proceedings, the issue of the report may be postponed under rules to be laid down by Act of Parliament. A report need not be issued in cases, to be determined by Act of Parliament, where such issue would never be in the interests of state security.'

Although the official translation uses the term 'home', the text of article 12 Gw uses the term 'dwelling' (*woning*). Use of the term 'home' is warranted, however, by the fact that what article 12 Gw seeks to protect is people's *huisrecht*, which – although literally translated as 'right pertaining to a house' – means protection of the home. The concept of 'home' or 'dwelling' is not defined in the law. It can be conceptualised as 'any place in which actual private home life takes place'.[80] It is irrelevant whether the residence is lawful, nor whether it is for a shorter or longer period. The *use* of the place is decisive; the use may be derived from the external looks of the place, but the overall circumstances need to be taken into account. The place needs to be somehow closed off (*afgesloten*) from the outside world,[81] and be a space furnished and intended for exclusive stay of a person or a limited number of people living together in a joint household.[82] The presence of a sleeping place or a bed is an important, but not decisive, factor.[83]

Examples of places considered a dwelling in case law are houseboats, caravans, tents, holiday cottages (if in actual use), the living compartments in vehicles, and hotel rooms (if in actual use).[84] Cellars are part of a dwelling, but appurtenances such as separate sheds or dog houses are not; neither are the common stairs in a residential building.[85] Gardens and courtyards are not part of the dwelling.[86] A pit in a forest may be qualified as a dwelling, although it is not always recognised as such in case law.[87] Company premises are not a dwelling, even when they can be qualified as 'home' in terms of article 8 ECHR.[88] Altogether, the Dutch interpretation of 'dwelling' is narrower than the concept of 'home' in the ECHR.[89]

Article 12 Constitution provides special protection to the dwelling only against entering (*binnentreden*, literally: treading inside) without the inhabitant's consent[90]. The inhabitant who can give consent for entering a dwelling is the person who leads her private home life in the dwelling. In case of more than one inhabitant, the consent of one inhabitant is assumed to be on behalf of all inhabitants, unless one of those explicitly object; one inhabitant refusing entry outweighs the consent of another inhabitant. Minors can also give consent if they can be supposed to be capable of adequate self-determination, which is more likely to be the case with a 14-year-old than with a 9-year-old.[91] The owner of a place cannot give consent on behalf of the tenant or actual inhabitant, nor can the main inhabitant (*hoofdbewoner*) consent to entering separate dwellings on the premises.[92]

The limitation to entering implies that generally, observing the inside from the outside is not considered to fall under the constitutional protection.[93] Entry is the case if 'the officer is wholly or partially in the dwelling or procures access to the dwelling using violence'.[94] The physical boundary of the dwelling thus needs to be passed, wholly or partially, for example by an arm.[95] In the literature, the limitation of the constitutional protection of the home to government officials entering the home is criticised, since observation (visual or otherwise) from the outside of what

---

[80] P.A.M. Mevis, 'Algemene Wet op het binnentreden. Inleidende opmerkingen' in CPM Cleiren, JH Crijns and MJM Verpalen (eds), *Tekst & Commentaar Strafvordering*, (11th Edn, Wolters KLuwer 2015), comment 5(a).
[81] Tak (n 77) 11; Buisman and Kierkels (n 77) comment 3(b).
[82] Buisman and Kierkels (n 77) comment 3(b).
[83] Tak (n 77) 13, observing that a 'proper bed' is not required, given that in cases where doubt arises, the people involved tend to have scarce furniture and utensils anyway.
[84] Mevis (n 78) comment 5(a).
[85] Ibid.
[86] Tak (n 77) 13.
[87] Mevis (n 80) comment 5(a).
[88] Ibid.
[89] Ibid.
[90] Before 2002, art. 12 Gw used the phrase 'against the inhabitant's will', which raised questions whether entering was possible in case an inhabitant was not at home and thus could not express consent or refusal. The term 'consent' now makes clear that the inhabitant should be able to express his will, and thus entering while the inhabitant is not in a position to give consent is not allowed. See Buisman and Kierkels (n 77) comment 3(a).
[91] Mevis (n 80) comment 5(b).
[92] Ibid.
[93] Mevis (n 80) comment 5(c).
[94] *Kamerstukken II* 1984/85, 19 073, no. 3, p. 13, quoted in Mevis (n 80) comment 5(c).
[95] HR [Dutch Supreme Court] 7 February 1956, NJ 1956/147 ('Arm').

happens inside the dwelling can also impact on the peace of the home (*huisvrede*) that is the primary rationale of constitutional home protection.[96]

It should be observed that, compared to most countries, the Dutch Constitution plays a relatively limited role in the legislation and legal practice of criminal procedure. This is largely due to the fact that there is no judicial constitutional review (see art. 120 Dutch Constitution) and hence no constitutional court.[97] Instead, the legislator and courts focus more on the European Convention on Human Rights as the primary guiding instrument for fundamental-rights protection. Thus, article 8 ECHR in particular plays the most important role in terms of the constitutional protection of privacy in general. Since article 12 paras 2 and 3 Gw do contain specific requirements for intrusions into the home, these requirements nevertheless do play some role in the legislation (primarily the Awbi) and case law interpreting these norms.

2.3.Physical v. non-physical intrusions

The protection of the home in the ECHR applies to both physical and non-physical intrusions and could even include potential intrusions that may cause a so-called chilling effect on the exercise of the right to privacy to occur. That the constitutional protection of the home at the national level also protects individuals from government surveillance of the home is only evident in Germany, which explicitly regulates acoustic surveillance and other forms of technical surveillance of the home in Art. 13 GG, which protects the inviolability of the home. Therefore, German constitutional law, although it primarily protects against physical intrusions, also considers monitoring of the home without physical intrusion as an interference with the inviolability of the home. In Poland, although this is not evident from the text of Art. 50 of the Polish Constitution, doctrinal accounts extend its application beyond physical intrusions, and includes protection of the mental and emotional state induced by safety and undisturbed use of the house.

The constitutional protection of the home in the Netherlands, an exception among the jurisdictions we study, only protects against physical entry by government agents. While this is a narrower understanding of the inviolability of the dwelling, it does not necessarily mean that individuals in the Netherlands are unprotected from government surveillance of their homes. Although this may not fall under the Art. 12 Gw, other provisions, such as the general right to privacy (art. 10 Gw), limit the ability of the government to monitor home life. Moreover, the statutory law-maker (in contrast to the constitutional law-maker) has introduced certain protections of the home from the outside in view of the inviolability of the home (see section 4.3.2 under ‘Visual and aural monitoring’).

3. Inventory of forms of monitoring of home life

3.1. Introduction

This section provides an inventory of forms of monitoring of home life. We focus on forms of surveillance that can either directly monitor the inside of the home, or allow to make inferences about home life from various emanations leaving the home or by accessing data generated in the home. Thus, we exclude traditional powers of the police such as home searches, unless these remain relevant for this paper when searches of certain premises allow the law enforcement to gain informational access to physically separate premises protected under home right (think of extended computer searches). The main focus is thus on measures which are conducted

[96] Bert-Jaap Koops, Hanneke van Schooten and Merel Prinsen, *Recht naar binnen kijken. Een toekomstverkenning van huisrecht, lichamelijke integriteit en nieuwe opsporingstechnieken* (Sdu 2004); Buisman and Kierkels (n 77); P.A.M. Mevis , ‘De bescherming van de woning 25 jaar later’, in E.J. Hofstee, O.J.D.M.L. Jansen and A.M.G. Smit (eds), *Kringgedachten Opstellen van de Kring Corstens* (Kluwer 2014), 157.

[97] A bill was proposed to change art. 120 of the Constitution and allow constitutional review; see *Kamerstukken I*, 2004/05, 28 331, No. A. This bill was accepted by both Chambers of Parliament in first reading, but required acceptance in second reading with a two-thirds majority. Before a second reading, however, it was withdrawn; see *Kamerstukken II* 2018/19, 32 334, no 12.

covertly, i.e. without knowledge of the person whose home or home life is being monitored in this way.

We first focus on monitoring of domestic waste since the primary object of this project is sewage monitoring. We compare sewage monitoring to searches of solid garbage. Subsequently we describe various forms of audio-visual monitoring, including monitoring of speech and sound in the home and visual monitoring of the home; monitoring of other emanations from the house; remote police access to data in the home; and police access to data relating to the home but located elsewhere. We do not claim that our inventory is comprehensive in the sense that is would include all possible and foreseeable forms of monitoring. Our aim is to cover the principal types of monitoring and the most common specific forms of monitoring as identified in our research.

3.2. Monitoring of domestic waste

3.2.1. Sewage monitoring

Sewage monitoring consists of technologically mediated surveillance of the contents of sewage water. Such technology has a number of potential uses for the law enforcement. In general, it consists of placing sensors into sewage pipes for the purpose of measuring and detecting chemical substances that reveal something relevant for criminal investigation. Sewage water can potentially reveal much about home life: from daily cooking patterns, drug use, drug production, to very sensitive information associated with bodily waste. Naturally, the usefulness of such monitoring depends on the particular capabilities and specificity of the sensors, the set-up of their placement into the sewage system and the period of time during which they can operate.

Generally, it is important to distinguish between targeted monitoring, capable of revealing facts pertaining to an individual household, and non-targeted monitoring aiming to uncover general trends within a larger area (for example to map production of narcotics per area). The targeted monitoring would require either placement of the sensors in the (semi)private sewage pipes of an individual household, which may be practically difficult, or a set-up of sensors which enables singling out the relevant chemical substance(s) in the public sewage.

Sewage monitoring that is targeted and limited to detecting certain chemical substances, e.g. directly related to the production of certain drugs, may be considered a relatively non-intrusive investigation measure. Nevertheless, it is important to keep in mind that this qualification might change depending on the exact capabilities and aims of a sewage monitoring technology.

3.2.2. Garbage searches

Garbage search, while perhaps not a pleasant activity, is a low-cost and potentially high-reward form of monitoring of home life. The contents of domestic garbage may reveal an abundance of information about the inhabitants and their home life. Discarded food and packaging reveals consumption habits, envelopes, letters and bills reveal information about correspondence, financial and other matters, hygiene products, medicine boxes, pregnancy tests can reveal highly sensitive information of bodily nature, and discarded injections or packaging with remaining traces of narcotics can reveal information on drug use and production. These are just a few examples from a much longer list to illustrate the usefulness of waste monitoring.

The police may gain access to domestic garbage in a number of ways, depending on the particular set-up in the area. House units often have their own cans for collecting garbage, located on private premises, which may be hard to access by the police (requiring warrants). However, these are regularly placed outside private premises, either permanently or temporarily for disposal by the waste management service. Here, the waste is accessible to anyone, including the police officers. Another set-up, typical for larger apartment buildings consists of garbage disposal units shared by a number of people. These may be located on public streets, either in the form of large underground spaces or containers, with various degrees of accessibility, or in semi-private shared areas inside the apartment buildings. The possibility of police access to this waste depends on the particular set-up, which would often require assistance from the waste disposal service. Furthermore, the shared waste disposal can be seen as a form of anonymisation, unless the waste contains traces which can be clearly traced to a

particular household. However, even individual garbage bins placed on a public street may contain waste not originating from the household.

Garbage search is generally not considered a particularly intrusive investigation method in legal systems. In many countries it is assumed that garbage search can be based on the general task or power description of the police (or that is even considered not to infringe privacy at all, so that there is no need for a legal basis[98]), such as a search of the garbage that is put on the sidewalk to be picked up by garbage collectors. At first glance, this seems to make it an equivalent of sewage monitoring. After all, what is flushed down the toilet is also a form of garbage that people discard and send into public space to be processed by public utility companies. At second glance, however, there are some potentially significant differences between the two methods. First, people can decide to put out the garbage just before the garbage collectors come, to minimise the risk that others will go through it; this is not possible with sewage waste. Second, garbage collection is relatively more visible than sewage monitoring for citizens; they can, in principle, see who collects the garbage (and possibly note differences if these are not the ordinary garbage vans or regular garbage collectors they see every week, whereas they cannot see who is collecting (or going through) their sewage waste. Third, garbage search is likely to be done by the investigator in person, while targeted sewage monitoring (presumably) is possible only through deployment of technical means. Fourth, and most importantly, people can decide what to put in the garbage bag and in which state; they may, for instance, dispose of certain goods elsewhere if they fear it might be searched by the police if put in their garbage bags, and, more relevantly, they can try to obfuscate sensitive information by destroying something before throwing it away (such as burning a letter and throwing away the ashes). Such obfuscation and alternative disposal methods are significantly more limited with toilet use, at least when it comes to people's natural needs of excretion. Overall, there seem to be sufficient differences, particularly in terms of covertness and in citizens' practical capacities to control the information derivable from their waste, to conclude that sewage monitoring cannot simply be equated with garbage searches.

3.3. Audio-visual monitoring

3.3.1. Monitoring of speech and sound

Monitoring of sound and speech inside private homes has extraordinary potential of revealing facts relevant for criminal investigation. People are arguably more willing to utter sensitive information that they would wish to remain hidden from strangers when they are located in their own home and communicating with their family members or other persons close to them, and they have a high expectation of privacy with regard to such conversations. For this reason, monitoring of speech and sound is considered highly intrusive and generally subject to very strict procedural requirements. There are a number of ways in which the police can monitor sound from private homes; the main distinction we will make here is between direct monitoring (eavesdropping, space interception) and monitoring of mediated communications by intercepting it during transmission.

Eavesdropping, aural space interceptions

Private conversations in the home and other sounds generated by people (self-talk, singing), animals (dog barking) or other objects (machine rattling) can be of high relevance for criminal investigations. The law enforcement authorities have a number of ways to gain access to these sounds. Rather than listing the various means, we will briefly make some important differences between them.

Often, the sounds from a private place are heard from the outside without technological help. In some cases, these sounds may even be addressed to the police intentionally (cries for help). In other cases, the police may be able to eavesdrop on relevant conversations by just standing outside the private space. Such cases could be comparable to sewage monitoring in a sense that the sound leaves the home and enters public space, just as the sewage water leaves the home

[98] This is the case in the Netherlands, see Bert-Jaap Koops, 'Criminal Investigation and Privacy in Dutch Law' (Social Science Research Network 2016) https://papers.ssrn.com/abstract=2837483 (last accessed 28 February 2019), 43.

and enters public space. From that moment, both are in principle accessible to others, although sewage water reveals relevant information only through use of technology. If the sound can be heard by anyone (including the police) this also means that the occupants of the home made little effort to hide the content, or at least the tone, of their conversations.

This is, however, often not the case. People tend to adjust the volume of their conversations in a way that enables them to determine the range of people who can hear them. This is especially true for sensitive conversations of the kind that the police might be interested in. Nevertheless, it is in some cases possible to use technologies enhancing the normal sensory capacity of the police officer and capture sounds that would otherwise be unavailable or at least incomprehensible. Such tools can range from a cup pressed against the wall, to sensitive directional microphones which enhance the sound needed to be heard and diminish background noise. In these cases, while the sound still leaves the home and is available in public space, it cannot be said that it is available to anyone, since certain effort must be made to obtain it. This situation might be more comparable to sewage monitoring than the previous, since technological means are used to obtain information from emanations coming from the home. However, in most cases, the contents of conversations are more privacy sensitive than the content of sewage water.

A third, and the arguably most intrusive form of eavesdropping occurs when the police places a listening or recording device physically inside the home. This can be either done by physically penetrating the space and installing such devices, placing the device on a person who will inadvertently carry it inside, or using other means. It is even conceivable that the police gain remote access to a device located in the home that is capable of serving as an eavesdropping device (phone, computer) and use it to overhear and record conversations of its inhabitants.

Wiretapping

Another way of overhearing people's conversations is to tap into their mediated communications, either via phone, or the internet. However, here we can assume that in most cases it is not so much the fundamental right to protection of home life that is at stake, but the fundamental right to the secrecy of communications. For these reasons, we will not discuss it further, other than pointing out that even this form of interception can lead to the overhearing of private conversations and sounds occurring within the home (e.g. background noise on one end of the phone call).

3.3.2. Visual monitoring

Visual observation

As with aural observations, visual observation of people in private premises has a potential to reveal information significant for the investigation, but at a very high cost to the privacy of individuals. From daily activities, gesticulation, body language, to very intimate acts that should perhaps be out of bounds to the law enforcement, visual observation of people in their homes can reveal much about their home life. In some jurisdictions, such as Germany, visual observation may be considered even more intrusive than aural observation, as suggested by the fact the German criminal procedure allows to record sound inside people's homes, but not the image. Nevertheless, the two measures are rather similar, if not in their intrusiveness then at least in the existence of various means of achieving them.

Visual observation can also be conducted by naked-eye observation from the outside (peeking through the windows) or outside observation with technological enhancement (binoculars, night vision). And similarly to aural observation, cameras can be installed inside the home, or devices already there, such as computers can be covertly accessed to obtain the image.

Aerial monitoring

Aerial monitoring is based on deployment of flying objects, usually drones, equipped with various sensing capabilities, typically a camera for recording images, but also sounds, and possibly other means such as thermal imaging. As such, it is not necessarily a form of monitoring in itself, but an

enhancement of existing forms, by for example offering better views than would normally be available, or by being able to bring the recording device closer to the target.

3.4. Emanations from the house

3.4.1. Heat monitoring

Thermal imaging is a technology that gives access to some general information on the consumption of heat and its distribution. From that, further information can be inferred, such as presence of people in rooms, a heat-producing activity taking place, etc. It finds use in many fields and areas, such as coal mining, or by the firefighters during operations and rescue actions. It has potentially useful applications for criminal investigation.

Thermal imaging (flying over an area with a thermal imager to detect which buildings radiant excessive heat patterns, which suggests the presence of a marihuana plantation or heated reaction vessels used in synthetic drug production) is another investigation method that is somewhat similar to sewage monitoring. This can be considered a form of (an extension of) visual observation by police. Thermal imaging is often considered not to be a very intrusive type of investigation power, since it seems a functional equivalent of observing the outside of houses (and, in snowy climates in winter, it is easily observable for police that in certain snow-less buildings, excessive heat is generated).[99] This may be a more fitting analogy to sewage monitoring than garbage searches: the goal is similar (finding signals of drug production) and the method is similar to the effect that a sensor is used to measure a particular type of information (temperature and the presence of a particular chemical substance, respectively). One difference is that the type of information sensed is much more specific in the case of sewage monitoring; this makes it less intrusive (since it only provides a positive signal if the particular chemical is present in the sewage waste, whereas the thermal imager always measures a temperature) but at the same time also more intrusive (since the presence of a particular chemical yields more information about what is going on in a building than the temperature indicates). Another difference is that citizens can, up to a point, protect themselves from thermal imaging by increasing the isolation of the building, so that less heat is radiated to the outside; such obfuscation is not possible with toilet use (people can hardly install filters in their toilets that capture substances from their excretions that they do not want to be detectable in the sewer). Perhaps more importantly, thermal imagers are normally used for short periods, flying over a certain area, and it requires humans to carry and operate the imager. In contrast, sewage monitoring relies on a robot and on sensing over a longer period of time. This implies that the practical obstacles for police may be higher for thermal imagers (require more human resources) than they are for sewage monitoring (although this may also depend on the cost of sewage-monitoring robots, which can be high at the initial stages of their development).

3.4.2. Olfactory surveillance

Olfactory surveillance of the home is based on the sensing of smells emanating from the home. In essence, it is a detection of certain particles in the air that reveal information about a particular object or a certain activity taking place in the home. Since a well-functioning human body has a natural ability to detect smells and based on experience associate them to certain substances, the most basic form of olfactory surveillance is when the investigators simply rely on their own senses. However, although many smells relevant for criminal investigations may be easily detectable by human senses (decomposing bodies, production of marihuana), many smells are not. Similarly to visual and aural sensing, there are means available to the investigators that are better suited to detect the particles in the air than their own sense of smell. These can either be specially trained sniffer dogs, whose sensing presumably function on similar principles as human sensing but with much greater sensitivity, or technological solutions that can do the same. The use of such technologies arguably comes very close to the type of sensing done in the waste

[99] Cf., however, the US case of Kyllo v. United States, 533 U.S. 27 (2001), where the Supreme Court considered thermal imaging to be an unreasonable search that requires a judicial warrant, partly because the technology used for it was not in general public use.

water. In both cases, the chemical signature of the air or waste water emanating from the home is identified to determine what is happening inside.

3.4.3. Monitoring of electromagnetic emanations

Another form of emanations from the home that can be monitored by the police and reveal relevant information are the electromagnetic emanations related to the use of electric appliances in the home. These emanations potentially allow those who can detect and read them privacy sensitive knowledge, or knowledge useful for further investigation measures. For example, Vuagnoux and Pasini have experimentally shown that keystrokes of computer keyboards can be identified with striking accuracy from the electromagnetic emanations up to a distance of 20 meters.[100] However, it is unclear to what extent such technologies are available and deployed by criminal investigators.

3.5. Police access to data in the home

3.5.1. Network search

Computers, or more precisely the data stored in and processed by computers, have grown in importance as a source of intelligence, investigative clues as well as evidence for the law enforcement. The traditional forms of police access to such data has been through search and seizure powers, which allow the police to physically access the computers, search the data, seize the device or make copies of the data. Nevertheless it may sometimes be practically difficult to gain physical access to these devices, while at the same time the interconnectedness of computers provides opportunities to do gain such access remotely. One of the common forms of such access is the so-called network search, or extended computer search. This form of search is an extension of an existing physical search: by accessing a computer in a particular place, the police can extend their search of this computer the physically separate storage media that are accessible from the computer being searched. In such a way, the police may gain access to computers located within someone's home, without having to physically access this home, and often without the knowledge of the person concerned by such extension of the search.

Of course, a potentially very large amount of data and computers are available from any computer; extended searches are generally restricted to such computers and data that are lawfully accessible to the user of the searched computer.

3.5.2. Police hacking

Unlike the network search, which is generally considered an extension of the traditional search, recognising the networked character of computing and the nature of storing data, police hacking is considered to be a significantly more intrusive measure. By using this power, the police remotely and covertly gains access to computers, usually by means of programming designed to overcome the security measures protecting the computer from unauthorised access. Although the law often limits the ways in which such access can be utilized, it potentially gives the police a very wide range of possibilities to monitor the life of the user or users of the device from browsing or copying of the stored data, monitor the activity on the computer, turn on the microphone and camera on the device to conduct visual or acoustic surveillance, delete or alter data stored on the computer or work around encryption of communications by intercepting it at the source. Considering the large role computers play in people's lives, police hacking is often described as the most privacy-intrusive tool available to the law enforcement.

[100] Martin Vuagnoux and Sylvain Pasini, 'Compromising Electromagnetic Emanations of Wired and Wireless Keyboards', *Proceedings of the 18th Conference on USENIX Security Symposium* (USENIX Association 2009) https://www.usenix.org/legacy/event/sec09/tech/full_papers/vuagnoux.pdf (last accessed 28 February 2019).

3.6. Access to data relating to home life

3.6.1. Access to communication data generated in the home

Today, with the rise of the Internet of Things, homes are being filled by more and more electronic devices, often connected to each other and communicating with the outside world. These processes are often automated and hidden to the inhabitants of the home, yet have the potential to reveal much about home life. Both the content of these various transmissions, as well as the meta-data generated can be useful to the investigators. Unlike data stored exclusively inside the home and not transmitted outside (which therefore can be accessed almost exclusively by overt measures of search and seizure), data generated in the home by devices which communicate with each other and the outside world can potentially be accessed by the police covertly by means of interception. Therefore, e.g. a smart-home device that backs-up its data in a cloud repository offers the police a number of ways of accessing this data, usually on different legal terms (interception of communications and physical searches are subject to different procedural requirements and safeguards, even if the data being accessed is the same).

3.6.2. Search and seizure of data stored with third parties

Search and seizure are overt measures and thus generally excluded from this paper. However, one particular case deserves mentioning: search and seizure of data generated in the home, but stored with third parties. Although the measure is overt regarding the person whose premises are being searched, the search may recover data relating to someone's home (but stored elsewhere) without the knowledge of the inhabitants of this home. In this way, although it is a traditionally overt measure, it may in some cases and aspects resemble a covert surveillance measure.

3.6.3. Data production orders to third parties

The same as above applies to a specific case of access to data stored with third parties, the production orders. A number of rules in criminal procedure as well as sectoral laws require various service providers to cooperate with law enforcement and, for the purposes of criminal investigation, produce data they have collected. In this way, data generated in the home, but stored by these other parties may be surrendered to law enforcement without the knowledge of the inhabitants of the home. This could include a wide range of data, including data about energy consumption from energy meters or meta-data generated by smart-home devices.

4. Legal framework of monitoring of home from the outside

4.1. Germany

4.1.1. Legal bases for monitoring of home from the outside

The German criminal procedural law serves two functions. It constitutes the legal basis for measures carried out during the investigation of a possible offense and also provides the framework for execution of sentences decided upon during the criminal trial. Procedural law thus serves as a means to solve any criminal law related conflicts.[101] Criminal procedural law concentrates almost completely on criminal prosecution (*Strafverfolgung*) by conducting repressive measures, as distinct from German police law which focuses on averting danger (*Gefahrenabwehr*) by conducting preventive measures. Because of this, and due to the fact that the police laws are primarily state-based in Germany, we will focus primarily on the law of criminal procedure as regulated in the Code of Criminal Procedure (Strafprozeßordnung, StPO). Additionally, we briefly deal with the Act on the Federal Criminal Police Office (Bundeskriminal-amtgesetz, BKAG), which includes power going further in some aspects related to monitoring of the home than the StPO.

In German law, a legal basis does not need to consist of a single provision, but can, depending on the actual conduct, consist of several provisions. Sections 160, 161 and 163 of the StPO provide for the general rules regarding criminal investigation of all criminal offences by the prosecution office and/or the police carried out without special technical equipment (anything going beyond human senses) and without entering areas or rooms protected by fundamental human rights (*e.g.* home, body) for a length of no more than 24 hours; in other words, this only covers short-term and non-intrusive forms of observation. The legislator created Section 161 (basis for conduct of the Prosecution Office) and Section 163 (basis for Police or other investigative personnel's conduct) with the intention of providing a general legal basis for measures, which interfere with fundamental rights in a less substantial way.[102] In this context, section 163(1) allows police to conduct investigations of any kind, but only to the extent that such investigations are not covered by other, specific provisions.

For surveillance taking longer than 24 hours or occurring during two or more days, Section 163f of the StPO (*lex specialis*) is most relevant and applies when a "criminal offence of substantial significance" could have been committed. This type of investigation interferes with one's fundamental right in a more serious and intrusive manner. Although BGH case law exists suggesting that Section 163f is broad enough to encompass surveillance using technical means,[103] some scholars raise doubts whether the provision provides a legal basis for such deployment of technical means, and whether a legal basis must be found elsewhere.[104] If Section 163f of the StPO does not cover the use of any *special* technical instruments that do more than reinforce human sensory perception (thus, the use of GPS tracking,[105] for instance, would require an additional legal basis), or conduct using force, the legal basis under Section 163f must be combined with provisions regulating the usage of such instruments (e.g. 100f, 100g, 100h and 100i of the StPO) for the legal basis.[106] Section 100h paragraph 1 under 2 of the StPO often acts as the additional legal basis. This Section gives the police the power to make pictures of suspects and other persons, or to use other technical means for their observations, for example 'low-jacking' a car, tracking a person via GPS, use of motion sensors, etc.[107]

---

[101] Urs Kindhäuser, *Strafprozessrecht* (4th edn, Nomos 2015) §1 Rn 7.
[102] Wohlers, '(Vor)§ 94', *Systematischer Kommentar zur Strafprozessordung* (online) Rn 1.
[103] BGH, Urteil v. 24. Januar 2001 – Az. 3 StR 324/00.
[104] It should be noted that the practical significance of the distinction is limited to the question of sufficient legal basis, but has little impact on the procedural requirements that must be followed. Since Section 163f is a measure interfering with fundamental rights more intensively, if the procedural requirements for ordering the measure under Section 163f are met, they would also be sufficient for applying a measure under Section 100h (see below).
[105] Eschelbach, 'StPO § 100h Weitere Maßnahmen Außerhalb von Wohnraum' in Satzger, Schluckebier and Widmaier (eds), *StPO* (3rd edn, 2018) Rn 7.
[106] Zöllner, '§ 163f', *Heidelberger Kommentar zur StPO* (online). Rn 2.
[107] For long-term police observations, § 163f. 107 MG § 100h Mn 2– 3.

Doctrinal texts discuss what counts as a "Special Technical Device Intended Specifically for Surveillance Purposes" (hereinafter "Technical Device"), according to Section 100h para. 1 under 2 StPO, largely in a negative sense, i.e., discussing measures that are not covered. Measures that are not covered include the taking of images (photographs and video) or even audio-recordings that still allow for observation, although not exclusively designed for this purpose.[108] Measures that *do* fall under this provision include: determining the location of a person by e.g. RFID[109] or stealthy ping,[110] investigating facts and circumstances by e.g. night-vision devices[111] or drones.[112] The scope of this provision is, thus, quite broad.

It is important to note that none of the provisions discussed above permit the law enforcement to conduct surveillance of the inside of private homes. These measures must end at the doorstep. Arguably the only provision that allows to directly monitor (in a covert manner) what is happening inside private homes is Section 100c StPO which regulates acoustic monitoring of private dwellings. This is only permitted for investigations of particularly serious criminal offences (see section 4.1.2 under 'Visual and aural monitoring' for a more detailed discussion). Interestingly, the provision is limited to acoustic surveillance (similarly to the Art. 13 par. 3 GG) and thus the StPO does not include a legal basis for other forms of monitoring of the home, i.e. visual surveillance.

Nevertheless, other covert investigation measures further permit to gain information from private homes, even if only in an indirect manner. This includes Section 100a, which allows to intercept the content of telecommunications (including so-called source interception, i.e. covert remote access to the communication device to bypass encryption), a newly introduced Section 100b which permits covert access by technical means to information-technology systems (to collect data or monitor activity of the suspect), Section 100g which permits the collection of traffic data and Section 100j which grants access to the subscriber data stored with the service provider. Search and seizure measures under Section 94 and following and 102 and following are not covert measures and therefore remain outside the scope of this paper, although in certain circumstances when the measure target service providers (e.g. ISPs), they may reveal information generated in the home, but stored elsewhere, without the knowledge of the occupant of that home.

Lastly, the BKA (the Federal Criminal Police) is permitted to conduct both acoustic and visual surveillance of private homes under Section 20h BKAG, but only to avert urgent danger to the existence or the security of the state or the life, limb or freedom of a person, or property of significant value. This is one of the powers given to the BKA in relation to their task of preventing the dangers of international terrorism and not available in general criminal investigations. The information obtained in the course of preventive police activity may not be used for evidentiary purposes in the criminal proceedings due to lack of corresponding powers in criminal procedure, it may nevertheless be used as an investigatory clue.[113]

4.1.2. Specific forms of monitoring

Although a number of investigative measures discussed in this section is not explicitly regulated in the StPO, this does not mean that they are necessarily unavailable to the investigative authorities. In Germany a technologically open definition of the means of surveillance does not meet with any objections of the Constitutional Court. The legislature is not obligated to limit the authorised means of surveillance to the technological state of the art at the point in time of the legislative process. As long as the type of surveillance that is permitted can be sufficiently made out, the legislature can provide that the authorisation shall also cover future technological developments. Furthermore, it falls upon the legislature to carefully observe technological developments and to take appropriate corrective action if the specific defining of openly phrased

---

[108] Hegmann, 'StPO § 100h Weitere Maßnahmen Außerhalb von Wohnraum' in Graf (ed), *BeckOK StPO mit RiStBV und MiStra* (29th edn, 2018). Rn 6; similar BGHSt 46, 266, 271.
[109] Gercke, '§ 100h', *Heidelberger Kommentar zur StPO* (online). Rn 4.
[110] Hegmann (n 108). Rn 6.
[111] Schmitt, '§ 100h' in Meyer-Großner, *Beck'sche Kurz-Kommentare Strafprozessordnung*. Rn. 2.
[112] Tobias Singelnstein, 'Bildaufnahmen, Orten, Abhören – Entwicklungen Und Streitfragen Beim Einsatz Technischer Mittel Zur Strafverfolgung' [2014] Neue Zeitschrift für Strafrecht 305. 305-306.
[113] Meyer-Gosser/Schmidt Section 161, 18d

legal terms takes an undesirable turn.[114] Therefore, a number of relatively open norms (such as Section 100h StPO) may accommodate new, previously unforeseen means of surveillance, without the need for legislative change. However, it should also be noted that measures permitting access to the inside of dwellings are more restricted and generally limited to acoustic monitoring.

Sewage monitoring

Short-term sewage monitoring could partially be based on Section 161 (basis for conduct of the Prosecution Office) and Section 163 (basis for Police or other investigative personnel's conduct) which are intended to provide a general legal basis for measures, which interfere with fundamental rights in a less substantial way.[115] In this context, section 163(1) allows police to conduct investigations of any kind, but only to the extent that such investigations are not covered by other, specific provisions; since sewage monitoring might fall under the use of technical measures for surveillance purposes in Section 100h (see below), it is questionable whether short-term sewage monitoring can be based solely on 163(1).[116]

For sewage monitoring taking longer than 24 hours or occurring during two or more days, Section 163f of the StPO (*lex specialis*) is most relevant and applies when a "criminal offence of substantial significance" could have been committed. This type of investigation interferes with one's fundamental right in a more serious and intrusive manner. Although BGH case law exists suggesting that Section 163f is broad enough to encompass surveillance using technical means,[117] some scholars raise doubts whether the provision provides a legal basis for such deployment of technical means, and whether a legal basis must be found elsewhere.[118] Sewage monitoring relies on the usage of several different technical tools involving different sorts of sensors and other technology for the purpose of detecting (and gathering evidence for prosecuting) narcotics laboratories. If Section 163f of the StPO, however, does not cover the use of any *special* technical instruments that do more than reinforce human sensory perception (thus, the use of GPS tracking,[119] for instance, would require an additional legal basis), or conduct using force, the legal basis under Section 163f must be combined with provisions regulating the usage of such instruments (e.g. 100f, 100g, 100h and 100i of the StPO) for the legal basis.[120]

Since sewage monitoring will usually be deployed in the public sewage system, thus outside of constitutionally protected homes and without interfering with the protection of communications, Section 100h paragraph 1 under 2 of the StPO can act as the additional legal basis.[121] Since in the first use-case (targeted sewage monitoring), no images, video or audio-recordings are made, section 100h para. 1 under 2 of the StPO would likely cover the use of the technical observation. However, the requirement of legal specificity could render this technologically neutral provision inapplicable to sewage monitoring. Although the provision seems to cover a wide range of technological means, in some cases of new investigative technologies, the legislator, acting upon concerns of constitutional incompatibility, has created a separate, more technology-specific legal basis for the use of these investigative tools. This was for instance the case with the so-called "IMSI catcher", the use of which has now been explicitly regulated in Section 100i of the StPO, since the use of Section 100h of the StPO would not satisfy the principles of legal clarity and certainty.[122] Since it is yet untested whether the German judiciary would find the existing legal basis sufficient for technological sewage monitoring, no clear conclusions on the matter can be made. One argument why applying these general provisions to sewage monitoring may not pass

[114] BVerfGE 112, 304 (319) – NJW 2005,1338 (1340), para. 316 and 317.
[115] Wohlers (n 102). Rn. 1.
[116] German law also includes special provisions for situations of imminent danger ('Gefahr im Verzug'), but we think that is not relevant to sewage monitoring for criminal investigation. See Škorvánek et al. 2019, p. 21n.
[117] BGH, Urteil v. 24. Januar 2001 – Az. 3 StR 324/00.
[118] It should be noted that the practical significance of the distinction is limited to the question of sufficient legal basis, but has little impact on the procedural requirements that must be followed. Since Section 163f is a measure interfering with fundamental rights more intensively, if the procedural requirements for ordering the measure under Section 163f are met, they would also be sufficient for applying a measure under Section 100h (see below).
[119] Eschelbach (n 105). Rn 7.
[120] Zöllner (n 106). Rn 2.
[121] See text surrounding note 107.
[122] See Deutscher Bundestag Drucksache 14/9088, 7.

the scrutiny of the Constitutional Court is the lack of specific statutory safeguards, such as a notification requirement. The possible need of a new regulation therefore cannot be precluded.

In Germany, the observation measures in accordance with Section 163f of the StPO are subject to the warrant requirement (*Richtervorbehalt*) set out in paragraph 3 of the provision. In exigent circumstances, when delaying the measurement would harm the investigation to uncover a criminal offence, measures can be ordered by the prosecution office or the police (*investigative personnel)* but only if a warrant issued by the court is obtained within three days after ordering the measures.[123] If such an order is not confirmed by the court within three days, it will become ineffective.

According to Section 101 I, IV No. 7 and 12, "the person targeted" and "other persons significantly affected" by the conducted measures must be notified of the measures taken against them. The notification should also mention the option of subsequent court relief and the applicable time limit. According to Section 101 I, V, the "notification shall take place as soon as it can be effected without endangering the purpose of the investigation". In case notification is delayed, the reasons must be documented in the file.

Garbage search

A garbage search is a measure that strongly resembles sewage monitoring in some aspects. In both cases the investigators try to learn something about what happens inside a particular dwelling, based on the waste that has been disposed from that dwelling. We could not find any relevant case law dealing with garbage searches or setting boundaries for such investigative measure. Nevertheless, we argue that people should have some reasonable expectations of privacy with regard to the waste they dispose of. This can also be read into the various state laws dealing with waste disposal, which prohibit the searching and taking of garbage that has been placed on the street for the purposes of waste disposal.[124] Nevertheless, it is doubtful that a warrant requirement would be placed on one time garbage search, which would likely be covered by the general task of the police (Section 161 StPO). However, repeated long-term monitoring of domestic garbage over a period longer than 24 hours would likely require authorisation under Section 163f StPO (see section on sewage monitoring). Unlike sewage monitoring, garbage searching does not require the use of technical means and therefore would not require combining the legal basis of Section 163f StPO with Section 100h StPO.

The above applies to searching garbage that has been placed on a public street. Garbage still located on the premises that are protected under Art. 13 GG as part of the dwelling could probably be searched only on the basis of a warrant under Sections 102 and following of the StPO. This would make it an open measure toward the person concerned, and thus fall outside the scope of this paper.

Thermal imaging

Thermal imaging is another surveillance measure that resembles sewage monitoring. We are not aware of any higher court case law in Germany dealing with thermal imaging of private homes in criminal investigations. Although it is generally not considered to be a very intrusive type of a measure, since it can be likened to the observation of the outside walls, unlike sewage monitoring and garbage searches, its application under German law of criminal procedure appears more controversial. While waste water in public sewers and garbage put on the street can undoubtedly reveal relevant information about home life, what is being monitored is undoubtedly located outside the dwelling. Thermal imaging, although it does not penetrate inside the walls of the home, does measure the temperature of the outside walls and monitors what happens inside in (almost) real-time. Arguments could be made that this constitutes means of technical monitoring of the home, which is only permitted in exceptional circumstances under Art. 13(4) GG and for which the legal basis does not exist in the StPO (StPO only covers acoustic surveillance),

[123] BGHSt 44, 246; see especially Zöllner (n 106). Rn 7.
[124] See for example Section 11 of the State Waste Act (*Landesabfallgesetz*) of Bad.-Württ.

especially since the dwelling also includes the surrounding premises (front garden, backyard) encircling the walls of the home.[125]

If, however, thermal imaging of the outside walls of the home could qualify as a measure that does not interfere with the inviolability of the home, it could be based on the same legal basis as sewage monitoring (see subsection 'Sewage monitoring' above), i.e. Section 161 for monitoring up to 24 hours or Section 163f for monitoring taking place over a period longer than 24 hours, both in combination with Section 100h permitting the use of technical means. Due to lack of available case law, it is not clear whether German courts would accept these legal basis for thermal imaging targeting private homes. Some German authors raise doubts whether the legal basis of Section 163f in combination with Section 100h are sufficient to cover thermal imaging.[126] This determination may also depend on the actual capabilities of the system and how much can they reveal of the home life.

Visual and aural monitoring

In Germany, the Code of Criminal Procedure only provides legal basis for audio surveillance of private homes. Visual surveillance is permitted under Art. 13(4) of the GG, but is generally allowed under more restricted circumstances (for example the BKA have legal basis to conduct it under a special anti-terrorist provision)

Furthermore, according to the German Constitutional Court, interference combining audio and visual surveillance carries substantially more weight than, for example, audio surveillance only, and requires special justification. Accordingly, when ordering these measures, the suitability, necessity and appropriateness requirements for each form of surveillance must be examined individually, as well as with a view to their combination with one another. It will normally not be sufficient for the additional ordering of visual surveillance to cite merely the increased ease at matching voices, more significant grounds relevant to the success of the surveillance are needed. In the context of applying the law, these requirements can and must be taken into consideration.[127]

Section 100c and following of the StPO deal with acoustical surveillance of residential spaces, sometimes called "der große Lauschangriff". Section 100c StPO concerns the requirements for eavesdropping and recording of non-public conversations taking place within the home using technical measures. Section 100d StPO regulates the protection of the core area of private life when measures under Section 100c are deployed and Section 100e StPO regulates the procedures of deploying these measures. Section 100c does not include tapping the phone or any visual surveillance measures[128].

The use of this provision is limited to the particularly serious crimes stated in Section 100b(2). These include murder and manslaughter, formation of criminal groups, crimes against personal liberty, aggravated robbery, particularly serious cases of money laundering, smuggling of aliens, crimes against humanity and serious cases related to the narcotics act and others.

The provision is based upon article 13 (3)-(4) German Constitution.[129] It is important to note that 100d StPO explicitly forbids measures which would infringe the core are of private life (see section 2.2.1). The measure may be ordered only if on the basis of factual indications, in particular concerning the type of premises to be kept under surveillance and the relationship between the persons to be kept under surveillance, it may be assumed that statements concerning the core area of the private conduct of life will not be covered by the surveillance. Conversations on operational or commercial premises are not generally to be considered part of the core area of the private conduct of life. The same shall apply to conversations concerning criminal offences which have been committed and statements by means of which a criminal offence is committed. The interception and recording is to be interrupted without delay if during

[125] Mark A Zöller and Saleh R Ihwas, 'Rechtliche Rahmenbedingungen des polizeilichen Flugdrohneneinsatzes' [2014] Neue Zeitschrift für Verwaltungsrecht 408, 414.
[126] ibid, 414.
[127] BVerfG, Judgment of the First Senate of 20 April 2016 - 1 BvR 966/09, para. 185.
[128] Eisenberg NStZ 2003, 638.
[129] Kindhäuser (n 101). § 8, Rn 96.

the surveillance indications arise that statements concerning the core area of the private conduct of life are being recorded. Recordings of such statements are to be deleted without delay. Information acquired by means of such statements may not be used. The fact that the data was obtained and deleted is to be documented. The requirement of deleting recordings pertaining to the core area of private life, while aimed to protect it, may in some cases, ironically, place the core area under heightened scrutiny. The duty to delete also means a duty to go through all of the footage to determine, if any parts belong to the core area. Thus, even parts which may have otherwise been overlooked will enter the sphere of cognizance of the law enforcement officer responsible for such redaction.

Such a measure can only be ordered by a special panel of judges called “Staatsschutzkammer” The panel will decide upon the measure after the prosecutor put in a request. In exigent circumstances the order may also be issued by the presiding judge, but needs to be confirmed by the panel within three working days. An order is valid for the maximal duration of 1 month (Section 100d (1) 4 StPO). An extension can be issued for 1 month, until a total period of 6 months is reached provided that the conditions continue to exist and the higher regional court needs to decide upon further extensions taking into account the results of the investigation.

The need to enter the home for the purposes of installing the eavesdropping equipment is also covered by section 100c StPO.[130]

While Section 100c StPO permit only acoustic monitoring of the home, Section 20h BKAG permits audio and visual surveillance in private homes. It thus constitutes an interference with Art. 13 (1) GG. The provision is not disproportionate for permitting audio as well as visual surveillance of private homes. The fact that the Constitution does not already fundamentally rule out visual surveillance of private homes for interferences serving to protect against threats pursuant to Art. 13 (4) GG can be deduced *a contrario* from Art. 13 (3) GG. However, interference combining audio and visual surveillance carries substantially more weight than, for example, audio surveillance only, and requires special justification. It should be noted here that Section 20h BKAG has been ruled unconstitutional in 2016 by the BVerfG due to insufficient protection of the core area of private life, and although it was permitted to stay in force until necessary amendments are made, this permission expired on 1 July 2018. Therefore, the provision currently cannot be applied until the considerations of the BVerfG are taken into account by the legislator.

Aerial surveillance

Although we were able to find reports of aerial technology, such as drones, being in use by the police in Germany[131], we could not find any references as to its use by the law enforcement in the investigation of criminal offences and in relation to surveillance of homes. Some authors are sceptical about the legality of the use of drones under the legal basis of Section 163f in combination with Section 100h of the StPO, stating some legal, but mostly practical limitations.[132] Nevertheless, barring practical considerations, Section 100h appears sufficiently technologically neutral to cover the use of aerial surveillance[133], of course only outside of private premises. Whether aerial surveillance could be used to monitor private homes, arguably depends on the type of monitoring attached to the usage of the drone. Since StPO only permits acoustical monitoring of the home and not visual, a drone equipped with a camera in order to monitor the inside of a private home could for instance not be used within the confines of criminal procedural rules (but could possibly be used under Section 20h BKAG).

Olfactory surveillance

Olfactory surveillance relies on detection of small particles in the air, which reveal certain substances and activities that occur in a certain area or place. In the most rudimentary form, it may rely on the police officer’s own senses, or more likely the senses of a specially trained sniffer dog. Alternatively, technological sensing of smell may greatly improve the precision and reliability

---

[130] Hegmann, ‘StPO § 100c Akustische Wohnraumüberwachung’ in Graf (ed), *BeckOK StPO mit RiStBV und MiStra* (29th edn, 2018) Rn 3.
[131] Zöller and Ihwas (n 125). 408; BVerwG, 22032018 - 2 C 4217 [2018] BVerwG 2 C 42.17.
[132] Zöller and Ihwas (n 125). 414.
[133] Singelnstein (n 112). 305-306.

of the sensing. We are not aware of any case law dealing with olfactory surveillance of private homes in Germany. Arguably, olfactory surveillance resembles sewage monitoring, which also relies on detection of certain particles, but in sewage water, instead of air. If we accept that such olfactory sensing does not interfere with the inviolability of the home, since it happens outside, it could be based on the general observation provisions of Section 161 StPO (short-term) and Section 163f StPO (longer than hours). In cases where technological means of olfactory surveillance are used, Section 100h StPO would also be applied. However, if olfactory surveillance was to be applied in such a way that would be considered to interfere with the inviolability of the home, than the StPO does not contain a legal basis for the type of monitoring.

Network search and police hacking

Modern homes are filled with various devices which generate and store data which may be of relevance to the criminal investigation and which at the same time reveals much about the home life of its inhabitants. The police may seek access to this data in various ways, both open and covert. Open measures, such as home searches and seizures are outside the scope of this paper, but we will focus on measures which are not open towards the person that is investigated.

The network search is regulated in Section 110(3) StPO which states that the examination of an electronic storage medium at the premises of the person affected by the search may be extended to cover also physically separate storage media insofar as they are accessible from the storage medium, if there is a concern that the data sought would otherwise be lost. Data which may be of significance for the investigation may be secured. In this way data in the home may be remotely accessed as long as it can be lawfully accessed from another computer to which the police have gained access during a traditional search.

In 2017, the StPO was amended to include the previously unregulated covert access to information-technology systems. Since such covert access is a breach of the right to confidentiality and integrity of information systems constructed by the BVerfG, it must be restricted by especially stringent procedural safeguards. Under Section 100b StPO the investigative authorities may covertly and by technical means gain access to informational-technology systems of the suspect, but only if there are particular grounds to suspect that this person has committed an especially serious criminal offence listed in Section 100b(2) StPO. Such a measure can only be ordered by a special panel of judges called “Staatsschutzkammer” The panel will decide upon the measure after the prosecutor put in a request. In exigent circumstances the order may also be issued by the presiding judge, but needs to be confirmed by the panel within three working days. An order is valid for the maximal duration of 1 month (Section 100d (1) 4 StPO). An extension can be issued for 1 month, until a total period of 6 months is reached provided that the conditions continue to exist and the higher regional court needs to decide upon further extensions taking into account the results of the investigation.

The same rules about the protection of the core area of private life that apply to acoustic surveillance (see 4.1.2 under ‘Visual and aural monitoring’) apply (with small exceptions) to police hacking under Section 100b. In the case of measures under § 100b it must be, as far as possible, technically ensured that data concerning the core area of private life are not collected. Findings that have been obtained by means of measures pursuant to Section 100b and concern the core area of private life must be deleted immediately or submitted by the public prosecutor's office to the court which issues a decision on the usability and deletion of the data. The decision of the court on the usability is binding for the further proceedings.

An important limitation of the measure under Section 100b is that the gaining of access to the information technology system by the investigators cannot be used to actively generate new data. They may access and copy existing data, but may not for example turn on the microphone or the camera on the device in order to conduct visual or acoustic surveillance.[134]

[134] Tobias Singelnstein and Benjamin Derin, ‘Singelnstein/Derin: Das Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens’ [2017] Neue Juristische Wochenschrift 2646.

Other forms of accessing data generated in the home

The data generated by the variety of devices within the home is rarely confined solely to the devices itself. Devices connected to the internet communicate with other devices within the home and outside and the various communications streams may be intercepted by the investigators. Furthermore, the data generated in the home may often be physically located in remote storage. The police may seek access to this data and avoid the requirements of a house search. Furthermore, the service providers, be it energy companies or internet service providers have large amounts of data generated within the home at their disposal and the police may seek access to this data by means of production orders.

In Germany, the content of communications can be intercepted under Section 100a of the StPO. Since 2017, this provision also covers the so-called source interception, in order to gain access to encrypted communications before they are encrypted. Section 100a is restricted to serious crimes (the list of crimes is broader than it is with police hacking and acoustic surveillance) and must be ordered by a court. In exceptional circumstances it can be authorised by the prosecutor, but this must be confirmed by the court within three days.

Section 100g(1) StPO allows for long-term collection of traffic data without the knowledge of the person concerned. This has to be ordered by a judge for a period of up to three months, which can be further extended. Telecommunication service providers are required to cooperate in the exercise of this measure, as well as the measure pursuant to Section 100a StPO. Section 100g(2) allows the investigative authorities to access traffic data that is retained under a special law.

The law enforcement authorities may also gain access to data generated in the home in the context of search and seizure. Although this is an open measure, in some cases, the person might be in the same position as in case of telecommunications surveillance (think of the seizure of emails at the provider).

4.2. Poland

4.2.1. Legal bases for monitoring of home from the outside

In Polish criminal procedure, the powers of covert surveillance are not regulated in the Code of Criminal Procedure, with the exception of wiretapping, but in the Police Act. This section will briefly outline the relevant provisions, explain some key terms and clarify their relation to the criminal proceedings. The relevant provisions of the Police Act (Art. 14–15, 19-22) regulate the so-called operational reconnaissance activities. This term is understood as an array of activities aiming at gathering information about a crime and obtaining evidence that will allow or facilitate to establish the course of events.[135] Moreover, it also aims at identification and prevention of crimes and offences.[136] The key provision here is Art. 19, which regulates operational surveillance (an array of covert surveillance powers). It can only take place if there is a justified suspicion of the crime being committed, or at least in the form of a presumption.[137] It can be used when other measures are either not effective or not useful.[138]

Although operational surveillance is a separate concept to the preparatory proceedings governed by Article 297 KPK, there is an observable trend towards the concurrence between the two, leading to the original strict division becoming obsolete and blurred.[139] Literature describes the evidential value of such activities and findings as problematic. There is an obvious discrepancy between operational and procedural findings, flowing from differences in the rules governing

[135] Wojciech Kotowski, *Ustawa o Policji. Komentarz* (Wolters Kluwer 2012) 441.
[136] Małgorzata Czuryk and others, *Prawo Policyjne* (Difin 2014).
[137] Kotowski (n 135) 441.
[138] Bartłomiej Opaliński, Maciej Rogalski and Przemysław Szustakiewicz, *Ustawa o Policji. Komentarz* (CH Beck 2015) 109.
[139] Adrian Szumski, 'Rola Czynności Operacyjno-Rozpoznawczych w Uzyskiwaniu Dowodów w Procesie Karnym' in Leszek Bogunia (ed), *Nowa Kodyfikacja Prawa Karnego. Tom XXVI* (Wydawnictwo Uniwersytetu Wrocławskiego 2010).

operational and procedural activities.[140] Although the obtaining of evidence is explicitly mentioned in Art. 19 of the Police Act, the information gathered in the operational reconnaissance can only be used as evidence during the procedural stage, if they have been authorized by the court within 5 days.[141] As operational surveillance is conducted covertly, information gathered in this manner are considered classified. What follows is that before it can be used as evidence in the trial, the information has to be declassified and should be overtly presented in the court as any other evidence.[142] The information gathered in the operational stage can be subsequently used to conduct specific procedural activities in order to obtain information that can be used as evidence.[143] Another evidentiary issue occurs in situations when information was gathered during operational control using deception or provocation.[144]

The power to use methods of operational surveillance is limited to specific crimes and offences listed in Article 19(1), which includes inter alia crimes against life, financial offences, sexual offences (when the victim is under age) and illegal production, possession of guns, ammunition, explosives, drugs and psychotropic substances and others. The power is not limited by the severity of the crime, but by its type.

The ordering of operational surveillance conducted by the police is regulated under the Police Act. More specifically, the requirements are laid down in Article 19(2) and (3). Accordingly, the primary control is exercised by the courts who can order the activities to be undertaken on the application from the chief of the Police office that will be conducting them, with the approval of a Public Prosecutor.[145] In cases of urgency, it is possible to act on the basis of approval of General Prosecutor or the local prosecutors. The urgency is usually caused by risk of loss of information, obliteration or destruction of evidence.[146] Subsequently, the authority in question should also file for approval of the operational surveillance measures to the appropriate court. Usually, the operational surveillance is ordered for a period not longer than 3 months. However, on the basis of special circumstances, it can be extended for another 3 months, even repeatedly, in justified circumstances, up to a total period of 12 months. The extension can be granted by a District Court on the basis of written application from the Chief of Police.[147] The authority asking for permission to conduct operational control is obliged to inform appropriate prosecutor about the results after the completion.

The means and measures that can be used by the Police in the exercise of operational surveillance have been reformed following the decision of Constitutional Tribunal that contested the specificity and precision of provisions that empower authorities to use them. In the judgement, the recommendations were made to specify not only the methods and means which can be used, but also the crimes which justify such a severe interference, time limits, regulation of the procedure and the subsequent use of the findings. Moreover, what was highlighted by the Tribunal is that such measures should be employed in line with subsidiarity only when there is no other alternative available and with an independent controlling authority.[148] The Center for Studies and Legislation of the National Council of Legal Advisors in their opinion criticized the lack of inclusion of subsidiarity in the reform.[149]

---

[140] Zbigniew Niemczyk, 'Czynności Operacyjno-Rozpoznawcze i Możliwość Wykorzystania Ich Rezultatów w Postępowaniu Karnym' (2013) 3 Kwartalnik Krajowej Szkoły Sądownictwa i Prokuratury 8.
[141] Izabela Dembowska, 'Wykorzystanie Materiałów Zgromadzonych Podczas Stosowania Operacyjnej i Procesowej Kontroli Rozmów (Postulaty de Lege Lata)' in Maciej Szostak and Izabela Dembowska (eds), *Innowacyjne metody wykrywania sprawców przestępstw. Materiały z konferencji* (Wroclaw University 2014) 34.
[142] Aneta Posytek, 'Wartość Dowodowa Czynności Operacyjno- Rozpoznawczych' (2011) 23 Prokuratura i Prawo 27.
[143] Adrian Szumski, 'Rola Czynności Operacyjno-Rozpoznawczych w Uzyskiwaniu Dowodów w Procesie Karnym' in Leszek Bogunia (ed), *Nowa Kodyfikacja Prawa Karnego. Tom XXVI* (Wydawnictwo Uniwersytetu Wrocławskiego 2010) 30.
[144] ibid 205.
[145] 80/7/A/2014 Wyrok z dnia 30 lipca 2014 r (Sygn akt K 23/11) [6.1.7].
[146] Ibid.
[147] Ustawa z dnia 6 kwietnia 1990 r. o Policji, art 19(8).
[148] 80/7/A/2014 Wyrok z dnia 30 lipca 2014 r. (Sygn. akt K 23/11).
[149] Ośrodek Badań Studiów i Legislacji, 'Stanowisko Ośrodka Badań, Studiów i Legislacji Krajowej Rady Radców Prawnych Dotyczące Poselskiego Projektu Ustawy o Zmianie Ustawy o Policji Oraz Niektórych Innych Ustaw'.

The reform transformed Article 19(6) of the Police Act, which previously read:

> Operational control is done secretly and entails:
>
> controlling contents of correspondence;
>
> controlling contents of packages;
>
> using technical means allowing for obtaining in a secret manner information and evidence and their recording, especially contents of telephone communications and other information transmitted using telecommunication network.

was changed into:

> Operational control is done secretly and entails:
>
> obtaining and recording of the contents of telephone communications carried out using technical means including telecommunication network;
>
> obtaining and recording picture and sound of persons from rooms, means of transportation or places that are not public places;
>
> obtaining and recording of the contents of correspondence, including correspondence carried out using means of electronic communication;
>
> obtaining and recording data contained in IT data carriers, telecommunications terminal devices, IT and tele-information systems;
>
> obtaining access to and controlling the contents of packages.[150]

Although various stakeholders expressed satisfaction with the new, more specific delimitation of the means of operational surveillance, a close reading reveals that certain activities previously covered by the provision due to their general nature could hardly find legal basis in the reformed text. For instance, while sewage monitoring could be undertaken as "using technical means of obtaining information in a covert manner", none of the existing means can be applied to it. A broad, technologically neutral provision, that would allow the investigating authorities to use new, previously unforeseen means, is therefore missing, and inclusion of such new means would require legislative change.

Much of the literature on operational surveillance in Poland is outdated and comments on the previous wording of the provision. Furthermore, the secretive nature of these powers and their scarce use as evidence in the criminal proceedings (and resulting lack of case law) has created a situation where it is difficult to describe clear limits of these powers. What is important to point out that the list of means of operational surveillance remains to a large extent technologically neutral. It does not actually specify the means, tools and techniques, but only the type of evidence that can be obtained, i.e. contents of communications, picture and sound from private places, contents of correspondence, data from data carriers and IT systems and content of packages. Such regulation could be seen as too specific in some ways (excluding relevant types of evidence, e.g. chemical surveillance), but too broad at the same time, not providing any limits on how the evidence can be collected. For instance, allowing the police to covertly access data in computer systems without specifying the power any further opens up a number of questions. Does this include the power to break through security measures protecting such data? Does it include remote access to the data using another computer system? Similar questions can be raised for other means of operational surveillance.

Further surveillance powers are included in Article 19a and 19b of the Police Act. Art. 19a provides legal basis for controlled purchase and controlled delivery. These activities can only be undertaken if there is justified suspicion and reliable information to support the claim that there has been in fact a crime committed and that there is a need for evidence with the outlook on future prosecution.[151]

---

[150] Ustawa z dnia 15 stycznia 2016 r. o zmianie ustawy o Policji oraz niektórych innych ustaw.
[151] Opaliński, Rogalski and Szustakiewicz (n 138) 121.

Article 19b in paragraph 1 allows for *covert supervision of manufacturing, displacement, storage and circulation of the objects of the crime.* In the literature, the covert supervision is understood to cover packages which are suspected of containing objects of the crime, real estate and movable objects – including vehicles, which are suspected of being used for the manufacturing, transportation, storage of circulation of the objects of the crime and lastly, of persons who are suspected of those crimes.[152]

4.2.2. Specific forms of monitoring

In this section various methods and available technologies of monitoring the house from the outside will be discussed. In most cases, it is unclear how the Polish legal system regulates them. Most forms of monitoring are not explicitly mentioned in the legislation, and rarely – if at all – mentioned in the literature. The various forms of surveillance deployed by the police are more specifically regulated in a sub-statutory legal document (Pf-634, Order of the Police Chief). However, this document is not accessible to the public and is unavailable for the purposes of this research. Hence, an overarching question when discussing all of them will be: is there a legal provision that can be interpreted as governing such activity? If so, it will be argued which one and for what reasons. When possible, arguments to the contrary will also be provided. In cases where a legal provision potentially applicable to the form of monitoring is identified, we will focus the discussion primarily on the institutional (judicial and other) oversight of the monitoring.

Sewage monitoring

There is no specific provision in either the Code of Criminal Procedure or the Police Act regulating sewage monitoring. The operational surveillance under Art. 19, which previously included a technology-neutral legal basis for the use of technical means[153] in the covert obtaining of information and evidence, has recently been amended, and due to it being strictly limited now to visual and aural surveillance, cannot be applied to the types of sensing envisioned in sewage monitoring.

The legal basis for sewage monitoring in Poland could arguably be based on Art. 19b of the Police Act. This provision allows the police to conduct covert supervision of the preparation, handling, storage and trade in objects of criminal offences, for the purposes of documenting a selected list of criminal offences (the same list as operational surveillance, see section 4.2.1), or to determine the identity of persons taking part in these offences, or to acquire the objects used in these offences. This provision seems to provide a sufficient legal basis for the use of sewage monitoring. Although the provision itself is relatively vague, the manner in which it should be applied is further specified in a sub-statutory regulation of the Ministry of the Interior, as prescribed by Art. 19b(6) of the Police Act. In this regulation, it is specified that the supervision consists of observing parcels, immovable or movable property including vehicles, if a justifiable assumption exists that they are used for preparation, handling, storage and trade in objects of criminal offences.[154] The power is not limited to observation: the police can interfere with such objects of criminal offences, especially for the purposes of labelling, removing or exchanging them, or to discover and record forensic traces.[155] The police can use organoleptic methods (acting on or involving the use of sensing organs) to evaluate the traces, but can also collect samples for the analysis of physical or chemical attributes of the objects.[156] As such, the provision seems to be applicable to monitoring sewage water, if there is a reasonable suspicion that traces of substances relevant for the investigation can be detected.

However, the provision itself lacks the mentioning of specific technical means that could be used for sewage monitoring, and any mention of technical means whatsoever. The Ministry Regulation and the literature mention that the observation can be conducted with the use of technical devices

[152] ibid 127.
[153] P Pochodyla and S Franc, 'Kontrola Operacyjna Oraz Zakres Jej Stosowania' (2011) 1 Zeszyty Naukowe WSEI 197, 199.
[154] Regulation of the (Polish) Ministry of Interior, nr. 23 nt. 239, 2002, §2(1, 1-2).
[155] Regulation of the (Polish) Ministry of Interior, nr. 23 nt. 239, 2002, §2(2, 1-2).
[156] Regulation of the (Polish) Ministry of Interior, nr. 23 nt. 239, 2002, §2(3).

registering image and sound, or other technical devices[157], suggesting this is the established practice. Nevertheless, doubts can be raised whether the text of the provision can be interpreted in this way. Sewage monitoring technology does more than merely enhance human perception. This means that the technology cannot be readily qualified as 'ordinary' human surveillance that is conducted by the police in the regular course of their work. Furthermore, a number of provisions in the Police Act explicitly allow the use of technical devices[158], which can be seen (using *a contrario* reasoning) as an indication that provisions that do not mention the use of technical devices cannot be understood to implicitly assume that technical devices can be used (otherwise, the explicit mention of technical devices in the mentioned provisions would be superfluous). A more restrictive reading of the law relying on the requirements of legal specificity and certainty might therefore exclude the use of technical devices, making the provision inapplicable to technical sewage monitoring.

The Polish provision of Art. 19b of the Police Act, which we identified as the potential legal basis for sewage monitoring, is not subject to a warrant requirement. It can be ordered by high-ranking police commanders, and the prosecution office has to be notified without delay. Thus, the prosecutor is not involved *ex ante*. Nevertheless, the prosecutor can order the police to stop the activity at any time. The police commanders are also obliged to regularly inform the prosecutor about the results of the activity. Importantly, while in criminal procedure the prosecutor is a party responsible for investigation – and can delegate it to police officers –, the standing of the prosecutor under the Police Act is different. The prosecutor does not have powers equivalent to those of the police under the Police Act and cannot undertake operational reconnaissance activities. The police are not bound by prosecutors' orders in conducting these activities, unless explicitly provided otherwise by the law. Therefore, although the authorisation by the prosecutor cannot be considered equivalent to the authorisation by the court, in the exercise of operational activities by the police under the Police Act, the prosecutor's role is more similar to an independent oversight authority than in investigations regulated under the KPK.

Garbage search

Garbage search poses similar issues as the sewage monitoring system. Primarily because, the position of trash in the polish criminal law system is unclear. On one hand, it could be interpreted as being a private property. On the other hand, it has been thrown away and supposedly there is no longer a proprietary connection. Searching garbage that is still located in private premises would probably require conducting a search of private premises as regulated by the Code of Criminal Procedure. In case the garbage is located outside private premises, which can be either a private garbage bin placed on the street for disposal or a communal garbage bin placed in a public place, arguably it could be searched on basis of Art. 19b of the Police Act, similar to sewage monitoring (see above). This would be the case, if there is a justifiable assumption that objects used in preparation, handling, storage and trade in objects of criminal offences listed in Art. 19 of the Police Act can be found in among the garbage searched. Since garbage search does not require technical means, the reservation we expressed in case of sewage monitoring does not apply here.

However, a specific evidentiary concern related to garbage search, is ascertaining with sufficient certainty the owner or producer of the trash. There is no legal obligation imposed on Polish citizens to mark their waste in any way. Because of that, linking garbage obtained for instance from communal containers to a certain person can pose issues. Unless there is other information in the garbage itself that allows identification, its connection to specific persons may be questionable.

Thermal imaging

The use of thermal imaging by the police in Poland is not clear. The technology is not mentioned in the legislation. Moreover, no mention of its usefulness to such authorities or their possibility to use it have been found in the literature. Nevertheless, it appears that thermal cameras are used by the police, including for detection of indoor cannabis cultivation, although the legal basis for

[157] Opaliński, Rogalski and Szustakiewicz (n 138) 261.
[158] Art. 15(4a) PA; Art. 15(5a) PA; Art. 19 PA.

this is not immediately clear. It does not clearly fit within the operational control measures allowed under Article 19(6) Police Act. The word "imaging" suggests that it could possibly fall under Art. 19(6)(2) of the Police Act worded "obtaining and recording the image (…) of persons from rooms, means of transportation or places that are not public places". However, strictly speaking the technology does not capture the image from inside the home, only graphically represents measurements of the temperature of its outside walls. Therefore, interpreting Art. 19(6)(2) in a way that would provide legal basis for the use of thermal imaging seems overly broad.

An argument could be made that Art. 19b of the Police Act, which allows for observation of movable and immovable property, if a justifiable assumption exists that they are used for preparation, handling, storage and trade in objects of criminal offences, could also be used as legal basis for thermal imaging.[159] However, as with sewage monitoring (see subsection above in 4.2.2), the counterargument is that the provision does not mention technical means, and thermal imaging certainly involves technical means beyond mere enhancement of human perception. As a form of covert surveillance, using technical means allowing to penetrate into a private home, it could be argued that thermal imaging would fit better among the means of operational surveillance in Art. 19 which are subject to judicial oversight. Nevertheless, as explained above, it does not seem that the forms of surveillance specified there allow for obtaining of the kind of evidence gathered by thermal imaging. In a comparative perspective, thermal imaging does not seem to be considered a highly intrusive measure in other jurisdictions, which could be used as an argument that Art. 19b can serve as an adequate legal basis for the measure.

The above concern would not apply to forms of thermal observation that do not require use of technology. Naked-eye observation (e.g. of snow melted on the roof) can sometimes reveal relevant information about heat distribution within a house. Such forms of observation could be non-controversially conducted with lesser safeguards.

Visual and aural monitoring

Visual and aural monitoring of the home has a clear legal basis in the Police Act. Art. 19(6)(2) reads that the police can covertly obtain and record the image and sound of persons from rooms, means of transportation and places that are not public places. This clearly applies to various means of obtaining both the image and sound from people's homes. The provision is technologically neutral, as long as the evidence thus obtained is in visual or aural form, making no difference between the two. Use of technical means is clearly implied by the possibility of recording. A further qualifier is that the image and sound obtained relates to persons, which seems almost redundant considering that the image and sound of persons is arguably much more sensitive than the image and sound from unoccupied premises.

As one of the means of operational surveillance, this form of surveillance is subject to rather strict procedural requirements (see section 4.2.1).

Aerial surveillance

Polish Police forces have been equipped with drones (unmanned aircrafts) for the last few years. In December 2017, 8 new ones were purchased.[160] Their main use is to help in the operational reconnaissance activities, as well as in search and rescue actions.[161] There are also mentions of use for the purposes of catching traffic offenders, or tracking violently behaving football fans.[162] They are presumably equipped with cameras to record picture and/or sound. Moreover, there is also a possibility of equipping them with thermal imaging technologies.

For the recording of image and sound from private homes by a camera equipped drone, Art. 19(6)(2) on obtaining and recording image and sound of people from private places seems to

---

[159] Regulation of the (Polish) Ministry of Interior, nr. 23 nt. 239, 2002, §2(1, 1-2).
[160] Komenda Glowna Policji, 'Ogloszenie o Udzieleniu Zamowienia 2017/S 246-514418'.
[161] Marcin Maludy, 'Specjalistyczny Dron Trafia Do Lubuskiej Policji' (*Informacyjny Serwis Policyjny*, 2017) <http://isp.policja.pl/isp/aktualnosci/12221,SPECJALISTYCZNY-DRON-TRAFIA-DO-LUBUSKIEJ-POLICJI.html>.
[162] Marcin Pietraszewski, 'Śląska Policja Kupuje Drony. Będą Latały Nad Całą Aglomeracją' *Gazeta Wyborcza* (2017) http://katowice.wyborcza.pl/katowice/7,35063,21887904,slaska-policja-kupuje-drony-beda-lataly-nad-cala-aglomeracja.html (last accessed 28 February 2019).

provide sufficient legal basis due to its technological neutrality. As long as the drone is located outside the private premises, this is not controversial. A question would arise whether this legal basis is still sufficient, if the drone physically penetrates inside the protected space (e.g. through an open window), especially if we envision future miniaturization of the technology. The wording of Art. 19(6)(2) does not seem to preclude such a form of surveillance, but it might also be seen as bypassing the requirements set for a house search in the Code of Criminal Procedure.

A drone can also be equipped by a thermal imaging device. Whether there is legal basis in Poland for thermal imaging of homes is discussed in the subsection above.

Olfactory surveillance

Olfactory surveillance aims at detection of crimes, for instance drug production or possession, by using olfactory stimuli that are produced by the substances. The most commonly used method is the use of specially trained dogs. With the development of technology, it becomes possible to use technical devices for the same purposes, which would also most likely be more precise and reliable in the detection. However, olfactory measures that could be used by police are not governed by the legislation, since operational surveillance is limited to visual and aural cues. Arguably, Art. 19b could apply, allowing observation of premises, if a justifiable assumption exists that they are used for preparation, handling, storage and trade in objects of criminal offences. In case the police officer relies on their own olfactory sensation, this would certainly be non-controversial. Would this change, if a dog was used? A specially trained dog could be considered somewhat equivalent to a use of technology detecting particles of substances in the air, which is not clearly provided for by Art. 19b of the Police Act.

Energy meters

Smart energy meters are slowly being introduced to the Polish market. Responsible bodies, such as the Regulatory Office of Energy, highlight the benefits and advantages for the customers flowing from installation of such devices. However, the General Inspector for Personal Data Protection voices the potential issues with the amount of data held in such devices, as well as the information that can be inferred from it.[163] This begs the question of police being allowed to request, access and use such information during their activities, as it could shed some light on the behaviour and activities of the person in question.

It remains to be seen if such situations do take place, as well as what legal basis is used to justify them. If the police wants to access this data covertly (not only with regard to the person under surveillance, but also other parties involved) Article 19(6)(4) Police Act could provide the legal basis,[164] This provision allows for covert access to IT data. Whether or not data from smart energy meters fall within its scope is not discussed yet in the scholarship.

Another provision that could be used in relation to smart meters is Article 15(1)(6) of the Police Act, which allows for demanding necessary assistance from state institutions, government administration bodies and local self-government as well as entrepreneurs operating in the field of public utilities.[165] As energy falls within public utilities, it should be possible for the Police to ask the responsible body for necessary assistance in the operational control activities. Alternatively, Article 15(1)(7) of the Police Act could be used as it allows to ask for necessary assistance from other entrepreneurs and social organizations, as well as for assistance from any person in urgent cases.[166] While the advantage of these legal bases mainly lies in very low threshold of legal safeguards (no judicial or prosecutorial approval), the involvement of other parties potentially undermines the covertness of the investigation.

---

[163] Tomasz Jurczak, 'Inteligentne Liczniki Prądu: Korzyści i Zagrożenia Związane Ze Smart Meteringiem' *Gazeta Prawna* (2014) http://serwisy.gazetaprawna.pl/energetyka/artykuly/771379,inteligentne-liczniki-pradu-korzysci-i-zagrozenia-zwiazane-ze-smart-meteringiem.html (last accessed 28 February 2019).
[164] Ustawa z dnia 6 kwietnia 1990 r. o Policji, art 19(6)(4).
[165] ibid art 15(1)(6).
[166] ibid art 15(1)(6).

Data production orders

Under Art. 20c of the Police Act, the police can request data that does not include the content of transmissions, but is *inter alia* transmitted within the services provided electronically.[167] Such data can be processed without knowledge or authorization of the person to which the information pertains. The data which are subject to this provision are outlined in Article 18(1) of the Act on services provided electronically (Dz. U. 2017 r. poz. 1219). They include: names of the users, their registration number (or if lacking, number of the ID card or passport), place of permanent residence, correspondence address if different than permanent residence address, data used to verify electronic signature and electronic address of the user.[168] Although the police can obtain such data on their own, they have to refer it to the public prosecutor to decide the manner and scope of its use.

Another basis for the production orders for telecommunication data can be found in Article 218a Code of Criminal Procedure. This can be ordered by either a judge or a prosecutor, depending on the stage of the proceedings. The obliged subjects are bureaus, institutions and subjects that conduct telecommunication activities. There are certain requirements applicable, such as the order being specific in limiting what kind of data should be secured, and the manner of securing in order to make the data fit for possible evidentiary use.[169]

Police hacking

Hacking in general is regulated under the Polish Criminal Code in Article 267, which prohibits unauthorized access to a part or the entirety of an information system. There is no explicit mention in the legislation about possibility for the police officers to hack into computers as part of operational control activities. However, the wording of Article 19(6)(4) Police Act, allowing covert obtaining of data from information systems, is broad and technology-neutral, and as such does not exclude the possibility of police gaining access to (a part of) IT system. The explanatory report of the Police Act reform mentions that the police needs to be able to gain access to data (both communications and stored data) by installing special programs on the computer of the person of interest, which will monitor all activity on that computer and the results of the monitoring will be transferred by internet network to the police. This clearly indicates that the intention of the legislator was to give the police full access to computer systems in a covert manner that would be otherwise qualified as hacking. However, considering the intrusiveness of such a measure, it is still questionable whether the present legal framework is sufficiently clear and precise to provide a legal basis. The vague wording and application of the same procedural safeguards as all the other forms of operational surveillance (judicial order, subsidiarity, three-month period with extensions) might not be sufficient for a measure of such severity.

4.3. The Netherlands[170]

4.3.1. Legal bases for monitoring of home from the outside

Since monitoring the home from the outside (without physical entering) does not infringe article 12 of the Dutch Constitution (see section 2.2.3), there are no specific constitutional requirements for monitoring the home from the outside from the perspective of the sanctity of the home. Nevertheless, there may be limitations based on the general right to privacy, and the law-maker has also sometimes opted for specific limitations in the Dutch Code of Criminal Procedure (*Wetboek van Strafvordering*, hereinafter: Sv) because of the sensitivity of monitoring the home from the outside (see in particular section 4.3.2 under 'Visual and aural surveillance' below), even if not specifically required by the Constitution.

Because of the legality principle (art. 1 Sv, also art. 8 ECHR), investigation powers require a statutory basis, which needs to be sufficiently explicit that citizens are able to know what the police can do in which circumstances. According to Dutch case law and doctrine, minor privacy infringements can be based on the general task description of the police (art. 3 Police Act 2012 in

[167] ibid art 20c(1)(2).
[168] Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną.
[169] Jerzy Skorupka, *Kodeks Postępowania Karnego. Komentarz* (3rd edn, CH Beck 2017) 532.
[170] This section builds on previous research, as documented in Koops (n 77).

conjunction with the designation of investigation officers in art. 141-142 Sv). What is considered minor, depends on the circumstances; the law-maker has not clarified when the threshold between minor and significant privacy intrusions is met. This is left to case law to decide.[171] An example of an investigation method that the Supreme Court has deemed to involve a minor privacy intrusion, is sending stealth sms (text) messages (sending a text message to a cell-phone without the phone acknowledging receipt, in order to generate traffic data with the phone's location that can be ordered from a telecommunication provider), except when this is done for such a period or with such frequency and intensity that a complete image is revealed of certain aspects of someone's private life (then it becomes systematic observation).[172]

The latter criterion refers to the general indication of the threshold of privacy intrusions that require an explicit legal basis in the Code of Criminal Procedure, namely the element of 'systematicness' in special investigation powers. Systematicness (*stelselmatigheid*) indicates that 'a more or less complete image is obtained of certain aspects of someone's [private] life'.[173] This image does not have to be of the entirety of private life, but only of a certain part of it, e.g., someone's contacts with a criminal.[174] As long as the image of some part of private life is not 'more or less complete', the privacy intrusion is considered minor and is supposed to be foreseeable for citizens on the basis of the general task description of the police.

The concept of systematicness has been particularly developed in the context of systematic observation (art. 126g Sv), where a set of factors have been identified that, usually in combination, determine whether a police activity constitutes a more than minor privacy intrusion, and thus requires an explicit legal basis. These factors are: use of a technical device; place; intrusiveness, continuity, or frequency; duration; and possibly the degree of suspicion. There are interesting similarities between this concept of systematicness and the mosaic theory that is being developed in US legal doctrine,[175] which holds that privacy is at stake when different investigation results (each of which may not as such trigger a privacy interest) are put together in such a way that the combination triggers Fourth Amendment protection.

For monitoring the home from the outside, this implies that the legal basis can be found in article 3 Police Act 2012 as long as the monitoring constitutes a minor infringement of the right to privacy. As soon as the infringement is more than minor, an explicit legal basis in the Code of Criminal Procedure is required. Depending on the technology used, this may be the power of systematic observation (art. 126g Sv), oral interception (art. 126l Sv), hacking (art. 126nba Sv), production orders (art. 126n et seq. Sv), or another specific basis. We will elaborate this below for the specific methods involved in monitoring the home from the outside.

4.3.2. Specific forms of monitoring

Sewage monitoring

Sewage monitoring for law enforcement purposes is not regulated specifically in the Netherlands, and no case law has been published on such monitoring. The legal status therefore is not clear, and has to be argued on the basis of doctrinal legal reasoning.

At first glance, garbage nosing (see subsection below) seems the most relevant precedent for sewage monitoring. After all, what is flushed down the toilet is also a form of garbage that people discard and send into public space to be processed by public utility companies. The same reasoning could therefore apply as for the garbage search, implying that article 3 Police Act 2012 provides a sufficient legal basis. At second glance, however, there are some significant differences between the two methods,[176] implying that sewage monitoring cannot be totally

[171] T. Blom, 'Titels IVA-VE. Inleidende opmerkingen', in C.P.M. Cleiren, J.H. Crijns and M.J.M. Verpalen (eds), *Tekst & Commentaar Strafvordering*, (11th ed., Wolters Kluwer 2015) Comment 15(d).
[172] HR 1 July 2014, ECLI:NL:HR:2014:1569.
[173] *Kamerstukken II* 1996/97, 25 403, no. 3, p. 26-27.
[174] *Kamerstukken II* 1996/97, 25 403, no. 3, p. 27.
[175] See, e.g., C.E. Walsh, 'Surveillance Technology and the Loss of Something a Lot Like Privacy: An Examination of the Mosaic Theory and the Limits of the Fourth Amendment' (2011) 24 St. Thomas Law Review 169.
[176] See Škorvánek et al. 2019, section 3.4.

equated with garbage searches, so that the case law on garbage searches cannot be unequivocally transposed for the purposes of regulating sewage monitoring.

Two factors may imply that sewage monitoring might constitute a possibly more serious infringement than garbage searches. First, with things flushed down the sewage, one cannot similarly say that a person 'also literally, brings his private business to the street' (as the Advocate-General argued for garbage), since the sewer is not a street: it is a closed system in which average persons cannot easily enter and search through. Second, if the right to privacy protects 'only those who have themselves taken sufficient measures against possible interferences with their private life' (again in the Advocate-General's words), one can argue that people can more easily take measures to prevent their home life being visible from garbage than they can with sewage waste. For the materials that are put in the garbage can or flushed down the toilet where there is a choice how to dispose of them (e.g., a used condom or left-over medicine pills can be put in the garbage, flushed down the toilet, but also be thrown away elsewhere to prevent it being connected to the inhabitant or home), there is perhaps no significant difference in privacy expectations. However, when using the toilet in their home for its primary purpose, people can hardly decide which materials in their excretion or urine they want to just relinquish and which materials they would like to keep private even when they flush the waste down the sewer. Consequently, people arguably have a reasonable expectation in the information that can be derived from the excretion that is flushed down their toilet, and hence in the entire flow of sewage that leaves their home.

This is not to say that sewage monitoring as such will constitute a more than minor intrusion. It will depend on what exactly is monitored (e.g., which materials are being detected), how closely to the home, during which period, and how sophisticated the technology is. For specific forms of sewage monitoring in the first use case – which focuses only on specific, illicit substance-related chemicals, and involves monitoring for a relatively limited period – one could likely argue that such monitoring will imply a not more than minor privacy infringement.

Perhaps the closest analogy to sewage monitoring for the purposes of detecting drug laboratories, are two cases in which goods have been monitored in order to locate the likely place of methamphetamine production. In one case, a location tracking device was placed on goods, leading to the presumption that certain premises contained a production facility for synthetic drugs. The court found that this did not constitute a systematic form of observation, since no person was followed, but a good. The case did not involve the systematic following or observation of a person (implying, although not explicitly stating, that in the present case there was no intrinsic connection between the tracked good and a specific individual).[177] In another case, a location tracking device and detection devices were used to track the delivery of bottles of methylamine for the purposes of MDMA and/or methamphetamine production. Again, the court held that this did not constitute systematic observation, since the following and detecting of the bottles did not give rise to a more or less complete image of certain aspects of the suspect's life. In fact, the goods at issue did not lend themselves as such for giving such insight into someone's life. Moreover, the investigation was not targeted at the suspect in particular.[178]

From these cases, one might tentatively conclude that sewage monitoring to detect the flow of certain chemicals related to the production of synthetic drugs does not reach the threshold of systematicness, partly because it is not targeted at following a specific individual, but only a flow of goods, and partly because the insight that this monitoring gives into someone's life is so minimal that it does not constitute a more or less complete image of certain aspects of that life. This is a tentative conclusion, since the assessment depends on the specifics of a monitoring case, and case law will need to determine the exact conditions when sewage monitoring (when focused on a broader range of (possibly more privacy-sensitive) materials) might reach the threshold of systematicness.

[177] Rb. [District Court] Breda 20 June 2006, ECLI:NL:RBBRE:2006:AY3612.
[178] Rb. Breda 15 December 2011, ECLI:NL:RBBRE:2011:BU8457.

Garbage search

Searching garbage that is put on the sidewalk to be picked up by garbage collectors (in Dutch referred to as 'garbage nosing', *vuilnissnuffel*) is not considered an investigation measure that infringes privacy. As the Supreme Court has argued, 'someone who puts garbage bags on the street to be collected cannot be said, objectively seen, to have a reasonable expectation of privacy protection with respect to their contents'.[179] The explicit mention of the 'reasonable expectation of privacy' standard (which does not normally explicitly appear in Dutch law, although it is implicitly used in various ways) resonates the Advocate-General's argument that 'art. 8 ECHR and art. 10 Constitution (…) protect only those who have themselves taken sufficient measures against possible interferences with their private life, and in any case only those who on the basis of objective facts and circumstances can be assumed to appreciate that protection (…). Who, however, also literally, brings his private business to the street, apparently does not cherish that wish (…).'[180] The legislator has stated that a garbage search conducted for a criminal procedural purpose can be based on the task description of the police.[181]

Thermal imaging

The use of a thermal imager (*warmtebeeldkijker*) to detect heat emanation in a dwelling can be based on the general task description of the police, article 3 Police Act 2012, since it is only a minor privacy intrusion, or at least not a form of systematic observation.[182] This follows from a verdict by the Supreme Court in 2009. The police had, when being alerted that a suspect was likely to have a hemp plantation in his dwelling, used a thermal imager, which confirmed the suspicion; after entering the dwelling (with consent of the suspect's then partner), they found a hemp plantation in the attic. The defence argued that a thermal imager makes a more than minor privacy intrusion. The Court of Appeal and subsequently the Supreme Court rejected the defendant's argument, since the thermal imager was 'used only once and cannot yield more than a general indication of an unusual heat source (in or near to the dwelling) on a certain premises.'[183] The Advocate-General's advice provided additional arguments for this conclusion. The thermal imager is targeted at an object, not a person (and thus not used as a technical device to systematically observe someone's behaviour). Although one might argue that persons can be observed within the dwelling, this is not what a thermal imager does (in contrast to, for example, radar detection). In fact, the imager records heat, but it does not record heat waves that move from the inside of the home to the outside; rather, the heat source makes the wall or roof warmer, and it is the higher temperature of the wall or roof that is recorded by the thermal imager, not the internal heat source itself.[184] One could therefore argue (although the Advocate-General does not explicitly draw this conclusion) that thermal imaging only monitors the *outside* of dwellings or other places, not what happens *inside* the dwelling. In that sense, it is similar to detecting a plume of smoke emanating from a chimney in summer—also a sign, external to the home, of an unusual heat source.[185] In that sense, the technology here did not significantly augment human perception.

Visual and aural monitoring

The law-maker considers **visual observation** of the home from the outside an acceptable privacy intrusion when conducted by the naked eye. 'Observation into a dwelling from outside a dwelling is not excluded, as long as it concerns observations that can take place without technical manoeuvres: that which is, normally speaking, visible from the outside, can be observed.'[186] In

---

[179] HR 19 December 1995, NJ 1996, 249 (*Zwolsman*), §8.3.
[180] Advisory opinion A-G Van Dorst for HR 19 December 1995, NJ 1996, 249 (*Zwolsman*), §66.
[181] *Kamerstukken II* 1997/98, 25 403, no. 7, p. 19.
[182] This applies to cases when the imager is used in a targeted way, focusing on an individual suspect's place. Thermal imaging as a form of mass surveillance (e.g., flying a helicopter with a thermal imager over a certain neighbourhood) has not been addressed in case law. One could argue, however, that larger-scale use of a thermal imager would still not be systematic observation, since no individual persons are being monitored with this technology.
[183] HR 20 January 2009, ECLI:NL:HR:2009:BF5603, §§3.2 and 3.3.
[184] A-G Knigge, conclusion to HR 20 January 2009, ECLI:NL:PHR:2009:BF5603, §19-21.
[185] *Ibid.*, §20.
[186] *Kamerstukken II* 1996/97, 25 403, no. 3, p. 70-71.

other words, if people do not close the curtains, the police can simply look through the windows. If they do this systematically, however, in the sense of looking for longer periods and with considerable intensity (e.g., during night hours), they will require an order of the Public Prosecutor, since then a more or less complete image of certain aspects of someone's life will arise.[187] Also, if the police uses technical devices to enhance their sensory powers, the threshold of systematic observation is likely to be triggered, so that likewise the conditions for systematic observation have to be observed.[188] Systematic observation means systematically following a person or systematically observing a person's presence or behaviour. It requires an order from the Public Prosecutor, but can be conducted for any felony, so it is a rather low-threshold investigation power (art. 126g para. 1 Sv). The order may include use of technical devices, as long as no communications are recorded, and devices may not be placed on a person (art. 126g para. 3 Sv). These devices (e.g., binoculars, photo and video cameras, infrared cameras, thermal imagers, movement detection equipment, and tracking devices[189]) have to comply with the conditions of the Technical Devices Decree[190] (art. 126ee Sv), to ensure reliability of the evidence. The order can be given for a maximum period of three months, which can be prolonged each time with at most three months (art. 126g para. 4).

It is noteworthy that the power for systematic observation allows, for pre-trial detention crimes[191] that seriously breach the rule of law, entering *closed places* without consent in order to facilitate the observation (to observe the place, or to install a camera), but it does not allow entering a *dwelling* for this purpose (art. 126g para. 2). This choice was defended in the Explanatory Memorandum to the Special Investigative Powers Act:

> 'It is proposed to exclude the entering of dwellings for the purpose of one of the mentioned powers. People's dwellings are seen as the places where they can pre-eminently be themselves uninhibitedly. They are places of privacy. The inviolability of the home enjoys special protection, both through the Constitution and through international human-rights treaties. I consider the inviolability of the home to be an important good. In my opinion, as far as there are interests to enable entering dwellings, these do not weigh up against the protection of this constitutional right.'[192]

Interestingly, while the original Special Investigative Powers Bill consistently used this argument to disallow surveillance within the home, during the parliamentary discussions, the Bill was amended to enable interception of communications within the home (see below), but not visual observation (through systematic observation or sneak and peek). The argumentation on the strong protection of the home has thus been kept for visual intrusions into the home, but not for auditory intrusions on home life.

Moreover, the prohibition of entering dwellings for observation purposes also translated into limitations of observation from the outside: 'In case a camera is placed, so that it can be permanently monitored what happens inside a dwelling, then this must be considered to be equally intrusive as entering a dwelling; that is not allowed.'[193] Thus, while the police can use naked-eye observation, they cannot place cameras to monitor a dwelling from the outside – at least not 'permanently'. This does not exclude, however, that a police officer hides in a bush and uses a camera to take pictures of all behaviour that is relevant for the investigation; this is allowed. What is not allowed is an unmanned camera that is used to 'record all behaviour taking

---

[187] Cf. for instance Hof [Appeal Court] Amsterdam 3 June 1999, *NJCM-Bulletin* 1999, p. 905-910, which held that using special binoculars on 33 days (three hours per day) over a period of four months, to observe a living room and kitchen was systematic observation, taking into account that the dwelling was located in such a way that people could not look through the windows with normal naked-eye observation.
[188] *Kamerstukken II* 1997/98, 25 403, no. 7, p. 66.
[189] *Kamerstukken II* 1996/97, 25 403, no. 3, p. 71.
[190] Decree on Technical Devices in Criminal Procedure (*Besluit technische hulpmiddelen strafvordering*).
[191] These are the crimes defined in art. 67 para. 1 Sv for which pre-trial detention is allowed, generally crimes with a maximum imprisonment sentence of four years or more, but also certain specifically designated crimes with a lower sanction.
[192] *Kamerstukken II* 1996/97, 25 403, no. 3, p. 43.
[193] *Kamerstukken II* 1996/97, 25 403, no. 3, p. 71. See also Investigation Powers Instructions (*Aanwijzing opsporingsbevoegdheden*), section 2.2.

place in the dwelling from a to z'.[194] Thus, the Dutch law-maker makes a distinction between human-based observation with selective recording of investigation-relevant behaviour (which is allowed) and installed camera-based observation with unselective recording of in-home behaviour (which is not allowed). This may leave open some scope for installing smart cameras that do not record everything that happens inside the home but only certain behaviour that, based on a smart algorithm, is likely to be relevant for the investigation; such smart cameras might (if sufficiently smart) be considered equivalent to police officers hiding in a bush and recording relevant activities.

When it comes to **aural observation**, this is regulated by the power of oral interception (*opnemen van vertrouwelijke communicatie*, literally recording confidential communications). Article 126l Sv allows the Public Prosecutor, with authorization from the investigative judge, to order an investigation officer to record confidential communications with a technical device, in cases for which pre-trial detention is allowed and that seriously breach the rule of law. Since the power sees to *recording* communications, only (naked-ear) *listening* to a conversation by an investigation officer does not constitute oral interception (but this may fall under systematic collection of information, see *infra*, section 4.3.2 under 'Stealthy collection of data').[195] This might imply that an investigation officer can eavesdrop on conversations in a home from the outside, as long as he does not record them. It will depend, however, on the circumstances whether such eavesdropping would be considered to constitute a minor privacy infringement. If the dwelling is close to a street and conversations are plainly audible outside of the dwelling (for instance, if a window is open and people speak loudly), there will be no reasonable privacy expectation in the conversations. If, however, the dwelling is rather shielded so that there are usually no passers-by, and the officer is making a considerable effort to hide and overhear conversations, for instance using listening-enhancing devices, the eavesdropping – even with no recording – is likely to constitute a more than minor privacy infringement, seeing that the conversations are held in a home and not normally audible outside. Between these two extremes, it is likely that eavesdropping of in-home conversations from the outside is not allowed, given that the Investigation Powers Instructions stipulate that eavesdropping is allowed if (confidential) conversations *in public* (*in de openbaarheid*) can be overheard without a technical device.[196] This implies that as a default, conversations in the home cannot be eavesdropped, unless they can so easily be overheard in public space (with open windows and loud voices) that they can be supposed to be taking place in public.

Where recording devices are used, the law-maker has created a legal exception to the principle of home protection by allowing the police to enter a dwelling in order to place a bug for oral interception.[197] Article 126l para. 2 Sv stipulates that the Public Prosecutor can determine that a closed space be entered without the right-holder's consent. If the closed space is a dwelling, this is only possible if the investigation urgently requires it and concerns a crime carrying a maximum penalty of at least eight years' imprisonment (a significantly higher threshold than the pre-trial detention crimes that ordinarily legitimate special investigation powers). The investigatory judge, who has to authorize the oral interception, explicitly needs to authorize that a dwelling may be entered for this purpose (art. 126l para. 4). Moreover, before the prosecutor can request authorization from the investigatory judge, she has to obtain permission from the Council of Procurators-General, after advice from the Central Examination Committee, a procedure foreseen for high-risk operations and for certain highly privacy-intrusive measures.[198] Also, in contrast to all other special investigatory powers, the authorization for entering a dwelling cannot be given orally

---

[194] *Kamerstukken II* 1997/98, 25 403, no. 7, p. 66.
[195] *Kamerstukken II* 1997/98, 25 403, no. 7, p. 61.
[196] Investigation Powers Instructions (*Aanwijzing opsporingsbevoegdheden*), section 2.5.
[197] In the original Special Investigatory Powers Bill, dwellings were altogether excluded from entry to facilitate oral interception, in light of the high importance attached to inviolability of the home (*supra*). Parliament opposed the generic exclusion of the home from the special investigatory powers, particularly in relation to oral interception, arguing that the inviolability of the home was made too absolute, and that the home risked to become 'a safe haven for criminals'. Consequently, the minister amended the Bill, allowing entering dwellings for oral interception under strict safeguards. See *Kamerstukken II* 1997/98, 25 403, no. 7, p. 7-8 and *Kamerstukken II* 1997/98, 25 403, no. 8 (amendment).
[198] Investigation Powers Instructions (*Aanwijzing opsporingsbevoegdheden*), section 5.1.

in urgent circumstances (art. 126l para. 6). Altogether, the entry of dwellings for the purposes of oral interception has the highest safeguards of almost all investigatory powers.

The law does not give clear an explicit answer to what extent oral interception can be used to record conversations in the home without entering the home, for instance, by using a directional microphone with a recording device, or placing a bug on or near the outside of a dwelling. Article 126l Sv only speaks of *entering* a dwelling to place a bug, so a grammatical interpretation implies that recording in-home conversations without entering is possible on the regular conditions for oral interception (so pre-trial detention crimes rather than crimes carrying eight years or more imprisonment, and without explicit authorization from the investigative judge to record in-home). However, the historical and teleological interpretations override the grammatical interpretation here. When the amendment to allow entering dwellings for placing bugs was proposed, the minister explained this by talking of making an exception to the principle that special investigation powers could not be used inside dwellings. 'In the amendment memorandum, I propose to allow *recording confidential communication in a dwelling* under strict conditions. (...) I consider that an even stricter criterion has to apply for *recording confidential communication in a dwelling*, namely a crime carrying a punishment of at least eight years imprisonment.'[199] Since the minister does not speak of *entering* a dwelling in order to record confidential communications, but of *recording* confidential communications in a dwelling, it is clear that she meant to cover all forms of recording in-home communications, both from inside and from outside the home.[200] Hence, the law should be interpreted in such a way that recording of in-home communications from the outside is allowed, but only under the strict conditions of article 126l para. 2 Sv (eight-year crimes and with explicit authorization from the investigative judge to allow in-home recordings).

Aerial surveillance

Aerial surveillance is not explicitly regulated. It will be considered a form of observation, and hence will fall under article 126g Sv if it has a systematic character, i.e., if a more or less complete image of certain aspects of someone's private life may arise. That might be the case if, e.g., camera-equipped mini-drones are used to covertly follow certain persons during a certain period, but with most cases of aerial surveillance, this will not be the case. There is one case where aerial surveillance was used for law-enforcement purposes: tax investigation authorities (FIOD) used Google Earth to zoom in on, and make a picture of, a suspect's garden, observing the presence of two exclusive design ('Bubble Club') armchairs there (hence for private use instead of for work use). Since this involved a single observation of a garden, using a technology (Google Earth) that was open to the public (so that anyone could observe the garden in this way), this was considered only a minor privacy infringement.[201]

There is no specific case law or doctrine on the question whether surveillance of the home from the air differs from observation from the earth or buildings. The reasonable expectation of privacy will differ somewhat, since people with, e.g., a roof terrace that is not visible from the earth or other buildings will expect to be non-visible, in contrast to a balcony from which they can be observed from the building across the street. The latter is not considered to infringe the privacy of the home, since it can be freely observed from the outside. Although the privacy expectation might be higher with a roof terrace, it will not likely change the qualification in terms of home violations: since the roof terrace is not part of the inside of the home, the observation will likely be considered an infringement of the general right to privacy, but not of the right to inviolability of the home.

If aerial surveillance is used to observe inside (rather than the top of) a dwelling, the general rule for in-home observation from the outside applies (see the subsection above on 'Visual and aural monitoring'). If the aerial surveillance uses a device to observe something that would not be visible to investigation officers hiding in the bushes with a zoom lens-equipped camera – for instance, a camera-equipped drone looking through the windows of the tenth floor of an

---

[199] *Kamerstukken II* 1997/98, 25 403, no. 7, p. 7 (emphasis added).
[200] Also during the parliamentary debate, the issue was discussed, in relation to the constitutional protection of the home, in terms of 'oral interception in dwellings' and not in terms of 'entering dwellings for oral interception'. See *Handelingen II* 11 November 1998, 23-1458 et seq. and 19 November 1998, 27-1896.
[201] Rb. Den Haag, 23 December 2011, ECLI:NL:RBSGR:2011:BU9409.

apartment building – the privacy infringement is likely to go beyond what the legislator has allowed. One might, however, argue that if the drone does not record the in-home activities on the tenth floor, but only uses a camera that is remotely controlled and operated by investigation officers, who would record only those in-home activities that are relevant for the investigation but no other in-home activities, this would be equivalent to police officers hiding in the bushes rather than to the installation of a fixed camera that records everything. Case law will have to determine whether such an argument is convincing – the analogy seems close enough to be considered a defensible extensive interpretation, but since the legislator in the 1990s did not foresee drones or aerial surveillance, the interpretation might also be rejected on historical-interpretative grounds.

Olfactory surveillance

In contrast to visual and aural observation, olfactory observation is not as such regulated in Dutch law. (The only exception – not relevant here – is the use of sniffer dogs for identifying a suspect with a smell identification test (*geuridentificatieproef*), which is one of the allowed 'measures in the interest of the investigation' for pre-trial detention crimes (art. 61a under d Sv[202]).)

Occasionally, olfaction is relevant in criminal investigations, but there is little published case law on this, probably because it occurs only in relatively trivial ways and as such is hardly contested in court. One published case involved entering the front garden and lifting the flap of a letterbox in the dwelling's door in order to smell the air in the dwelling; according to the court, this does not constitute entering the dwelling and is considered a minor privacy intrusion, hence allowed on the basis of article 3 Police Act 2012. The fact that the police officer smelled hemp and heard a humming noise constituted sufficient probable cause for subsequently entering the dwelling on suspicion of a drugs crime.[203] The latter element occurs more often in case law, where the smell of hemp ('known *ex officio* to the investigation officers') coming from a dwelling, certainly in combination with a humming noise that indicates an extractor, is used as a reason to further investigate the dwelling.[204] For the rest, olfaction is largely used *during* searches of premises, e.g., to lead the investigation to a room where hemp is grown, or to identify the contents of containers as likely having been used to produce synthetic drugs because of a strong MDMA smell.[205]

Should olfaction be used to detect smells in a dwelling in a way that constitutes a more than minor infringement (hence going beyond the smelling through the flap of a letterbox, e.g., using devices with chemical sensors to monitor a home from the outside for a certain period), this would require an explicit legal basis. Although the law-maker has not excluded such olfactory surveillance in the home (since the law-maker only considered visual and aural surveillance in the context of the constitutional protection of the home), it is probably not allowed, since there is no specific legal basis that could be considered to include olfaction.

Police network searches and hacking

Dutch police can search computers located in a dwelling from the outside in two ways: a network search (which is an extension of a search being conducted at another place) and remote access (i.e., police 'hacking').

Network search

Investigation officers can extend a search of a certain computer located at some premises or in a vehicle that is being searched, to computers connected with that computer. According to article 125j, a search can be extended, from the place being searched, to a computer located elsewhere, if the connection is lawfully accessible to people regularly living, working, or staying at the searched location. This so-called 'double bond' criterion implies that there must be a) a

[202] Before art. 61a was introduced, the Supreme Court (HR 2 July 1990, NJ 1990, 751) had allowed suspects to be subjected to a sorting test using sniffer dogs, without a legal basis; apparently, such a test was then considered not to infringe any fundamental right. See G.J.M. Corstens and M.J. Borgers, *Het Nederlands strafprocesrecht* (8th edn., Kluwer 2014) 491.
[203] Hof 's-Hertogenbosch 15 April 2014, ECLI:NL:GHSHE:2014:1044, as referred to in Mevis (n 80) comment 5(c).
[204] See, e.g., Rb. Limburg 3 October 2017, ECLI:NL:RBLIM:2017:9532.
[205] Rb. Oost-Brabant 4 January 2018, ECLI:NL:RBOBR:2018:74.

factual connection between the person whose computer is being used and the location being searched (so connections from laptops of occasional visitors may not be investigated), and b) a legal connection (lawful accessibility) between the local and the remote computer (so the search cannot be extended to hacked computers accessible from the hacker's computer). The search of the connected computer must be reasonably necessary for the investigation, and only existing (stored) data may be investigated – the connection cannot be used for monitoring incoming or outgoing traffic. However, incidentally incoming data may be used as bycatch.[206]

While the network search was associated with a 'house search' (*huiszoeking*) at the time of introduction (1993), it was extended to other searches (*doorzoekingen*) in 2000, with partly lower safeguards. While the minister in 1991 argued that network connections were equally privacy-sensitive as the dwelling, in the current system of the law it is possible for an investigation officer, without authorisation from a judge or prosecutor, to investigate a computer (e.g., a smartphone, laptop, or tablet) found in a searched car, and then extend this investigation to lawfully accessible connections. This may include connections to private cloud accounts, but also to the personal computer located at home, or domotics devices in the Internet of Things (e.g. the home thermostat or a nannycam in the children's bedroom). While computers located in a dwelling are relatively strongly protected when they are investigated during a search of that dwelling (e.g., requiring authorization from the investigative judge, art. 97 para. 2 and 110 Sv), they are much less protected when they are investigated through a network search from another place, such as a car or an office, which can be searched by non-judicial authorities. Doctrinal literature argues that this constitutes a gap in protection of the home, and that network searches from other places than a dwelling should be adapted to at least the level of searches of non-residential areas and possibly the level of searches of dwellings.[207]

Hacking

Up to now, there is no general investigation power to access computers remotely and covertly (i.e., what in this paper is called police hacking or legal hacking by investigative authorities). Only in two specific situations can the police covertly access computers outside the context of a search, in order to intercept communications;[208] it is not possible to remotely search the (data stored on the) computer.

In June 2018, however, a law was passed to enable legal hacking. The Computer Crime III Act (Wet computercriminaliteit III) will introduce the special investigatory power of article 126nba in the Code of Criminal Procedure.[209] It allows computers to be covertly accessed remotely, in order to perform a variety of follow-up investigatory activities. These follow-up activities are exhaustively mentioned in art. 126nba para. 1:[210]

a. Determining certain characteristics (especially the identity or location) of the computer or the user – a digital variant of the physical sneak-and-peek.
b. Recording confidential communications (both telecommunications and oral interception), e.g. recording Skype conversations, copying in- or out-going email, keylogging communications typed on the keyboard, or turning on the computer's microphone.
c. Systematic observation, to facilitate observation (art. 126g Sv), e.g., secretly installing a GPS tracker that maps with high accuracy someone's smartphone's movements, or turning on the computers webcam.
d. Securing data, both data stored on the computer and data that enter the computer after the remote access, for the period authorised in the order. This is a remote search of the computer, but also a form of surveillance of computer use (e.g., monitoring the user's Internet use or email traffic) since the remote search is done over a period of time.

---

[206] F.P.E. Wiemans, 'Artikel 125j', in Melai/Groenhuijsen et al. (eds), *Het wetboek van strafvordering*, Deventer: Kluwer (online) (2006), comment 4.2.
[207] B.J. Koops, C. Conings and F. Verbruggen, *Zoeken in computers naar Nederlands en Belgisch recht. Welke plaats hebben 'digitale plaatsen' in de systematiek van opsporingsbevoegdheden?*, (Wolf Legal Publishers 2016) 43.
[208] One situation is entering a dwelling to place a bug for oral interception (*supra*, 0); the other is accessing a computer as a technical means to execute an order for intercepting telecommunications (art. 126m Sv).
[209] See *Kamerstukken I*, 2016/17, 34 372, A. The Act enters into force on 1 March 2019, see *Staatsblad* 2019, 67.
[210] See *Kamerstukken II* 2015/16, 34 372, no. 3, p. 20-26.

e. Rendering inaccessible data, for example to delete unlawful data from the user's computer. This power can be applied for a period of four weeks, which can be prolonged repeatedly with four-week periods. It requires authorization from the investigatory judge, as well as from the Council of Procurators-General.[211] It can be used for investigating serious crimes: remote access for the goals mentioned under a, b, and c is possible for pre-trial detention crimes that seriously breach the rule of law; access for the goals mentioned under d and e is only possible for crimes carrying a maximum penalty of at least eight years' imprisonment, and for specially designated felonies[212]. The power is to be executed by specifically designated technical investigation officers, while the collected data will be analysed by officers investigating the case. This functional separation between technical and tactical investigation officers is an important safeguard, because the technical officers do not have a direct interest in the investigation at hand and therefore can take (relatively) objective decisions on the scope and execution of the legal hacking.[213] Only computers 'in use with the suspect' can be remotely investigated. Depending on the circumstances, this might involve the laptop or smartphone of the suspect's co-inhabitants, friends, or relatives, if the suspect (more or less regularly, so more than just once or twice) uses them.

One reason (among many others) to introduce the power was the fact that current law allows placing a bug in a computer for oral interception purposes, but only by physical means (entering a place and installing a bug in the keyboard or computer). The law did not include the option of installing a bug remotely, which hindered the investigation if the location of the computer is unknown or if physical installation is too risky. By allowing remote access for this purpose, the advantage, according to the minister, is that it is not necessary to enter a dwelling to install the device, so that article 12 of the Constitution does not have to be infringed.[214]

Not much specific attention has been paid to the protection of the home in the legislative history of article 126nba Sv.[215] Since the safeguards for using legal hacking are high compared to most other investigation powers, it apparently is not very relevant whether remotely accessed computers are located in a dwelling or elsewhere – it is the computer that is being protected against intrusions through the relatively high safeguards. Interesting to note is that the high threshold for the remote search and remote deletion of data (crimes carrying at least eight years' imprisonment) was inspired by the conditions of oral interception inside a dwelling, since the remote search is considered the most privacy-intrusive form of remote access.[216] One could argue that the law-maker thus considers remote computer searches (regardless of where the computer is located) and oral interception in a dwelling as equally highly intrusive.

Visual observation inside the home as facilitated by hacking

One relevant aspect is the statement in the Explanatory Memorandum that the current prohibition of 'permanent' visual observation in the home remains in place. Since article 126nba para. 1 under c Sv refers to using hacking for the purpose of conducting systematic observation as regulated in article 126g Sv, the legal conditions of the latter also apply to systematic observation where facilitated through hacking, including the prohibition of in-home recordings by installed cameras (see subsection 'Visual and aural monitoring' above).[217] Thus, '*permanent* observation of what happens inside a dwelling through remotely turning on the webcam of, for instance, a smartphone or laptop, must be considered equally intrusive as entering a dwelling; that is not

[211] *Kamerstukken II* 2015/16, 34 372, no. 3, p. 37.
[212] That particularly involves felonies where 'there is often no other clue' than to use the present power, such as botnet infections, child pornography, grooming, and other computer-related crimes. *Kamerstukken II* 2015/16, 34 372, no. 3, p. 29.
[213] See *Kamerstukken II* 2015/16, 34 372, no. 3, p. 31.
[214] *Kamerstukken II* 2015/16, 34 372, no. 3, p. 13. Similarly, *Kamerstukken II* 2016/17, 34 372, no. 6, p. 24.
[215] Significantly, the lengthy discussion in the Explanatory Memorandum of the protection of constitutional rights in relation to art. 126nba Sv (*Kamerstukken II* 2015/16, 34 372, no. 3, p. 50-56) is limited to the general right to privacy and the right to secrecy of communications; nothing is said on a possible violation of the right to inviolability of the home.
[216] *Kamerstukken II* 2015/16, 34 372, no. 3, p. 29.
[217] *Kamerstukken II* 2015/16, 34 372, no. 3, p. 26.

allowed in the context of criminal investigation.'[218] As before, the law-maker here leaves open some form of incidental observation inside the dwelling from the outside: the prohibition explicitly sees to 'permanent' recordings, which likely refers to indiscriminate recording of everything over a certain period of time. The recording of webcam images for a short period might be allowed. Possibly, also the real-time watching of webcam images – without recording them – might be allowed if this is done with a view to start recording webcam footage when something happens that is relevant for the investigation (and stopping the recording as soon as the investigation-relevant activity ends). Such real-time watching might be compared with the police officer hiding in the bushes and taking snapshots of relevant in-home activities (see subsection 'Visual and aural monitoring' above). In the Explanatory Memorandum, the minister has not excluded such an interpretation in the remarks on the prohibition of 'permanent' recording.

However, the minister has later offered a more explicit prohibition of all forms of hacking-facilitated observation in a dwelling. When asked whether the minister agrees with the opinion that covertly remotely turning on a webcam is more intrusive than entering a dwelling, because it happens covertly, the minister replied the following. 'The execution of an order for systematic observation must, regardless of the mode of observation, take place within the framework of article 126g Sv. Covertly turning on a webcam in a dwelling, like covert entry of a dwelling, is not allowed when applying this power.'[219] Although not further elaborated, the statement is sufficiently emphatic to exclude the use of observation inside a dwelling through a remotely turned-on webcam, however incidental. One might observe that the statement only concerns *turning on* the webcam, but it would be inconsistent if the police could turn on a webcam on a mobile device outside a dwelling and then continue watching and recording when the device and webcam are brought inside a dwelling. A webcam should therefore be turned off as soon as a dwelling is entered.

This, however, raises the practical question how the police should recognize when a computer is inside a dwelling. This will not always be clear, particularly with mobile devices such as smartphones held close to the face or held in a vertical axis with the face (typically the position in which people check their smartphones, looking down) – in such situations, there is only limited background visible, or a ceiling or floor, which makes it difficult to distinguish dwellings from non-residential places. Moreover, there is the practical problem of when to turn on a webcam (if systematic observation is one of the purposes of the legal hacking): this is only allowed outside dwellings, but how is the police to know when a mobile device is inside or outside a dwelling if they cannot turn on the webcam to see where the device is? The location-tracking function can give an indication, but this depends considerably on the precision of the location and whether the device has a GPS function. In some cases, the police could use information from other investigation measures running in parallel, e.g., fairly precise location from communications metadata that are collected real-time and that could suggest that the device owner is inside a house. However, dwellings are not synonymous with residential houses: also caravans and houseboats are dwellings, and a car if it has a sleeping bag and pillow on the back seat, and such spaces cannot be recognized as dwellings based on their geographic coordinates. Altogether, the prohibition of using a remote-controlled webcam inside a dwelling raises questions on whether visual observation is feasible in the first place with mobile devices.

In that light, another interpretation of the minister's statement that webcams cannot be turned on inside dwellings, might be considered. Perhaps the prohibition is limited to computers located in dwellings, i.e., fixed computers such as desktop computers and IoT devices in the home. Such computers might be remotely accessed under article 126nba Sv for various purposes, but not for turning on their webcams. In this interpretation, turning on the webcam of mobile devices would simply be allowed; the only limitation would then likely be that, when it is evident that the webcam shows footage of the inside of a dwelling, the technical officers should exclude the images from the material forwarded to the tactical officers (but keep them preserved behind a Chinese wall to

[218] *Kamerstukken II* 2015/16, 34 372, no. 3, p. 27 (emphasis added).
[219] *Kamerstukken II* 2016/17, 34 372, no. 6, p. 50. The statement is (summarily) repeated in *Kamerstukken I* 2016/17, 34 372, D, p. 3.

enable the defence to request the court to check whether no exculpatory evidence has been deleted or left out of the file).

Which of these interpretations (the prohibition concerns all webcam recordings inside a dwelling or only those made with hacked fixed in-home computers) is correct, cannot be determined here, since there are no authoritative sources to prefer one to the other. Future case law and doctrinal discussions will have to determine this. Tentatively, based on dogmatic argumentation in view of the protected legal good (the inviolability of the home), we can suggest an intermediate interpretation: using webcams of fixed computers in the home is definitely prohibited, while using webcams of mobile computers is, in principle, allowed. In the latter case, however, as soon as footage from a mobile webcam appears or seems to be from inside a dwelling (based on any indicators that the police should reasonably be aware of, and make a reasonable effort to ascertain), this footage cannot be used and should, using the safeguard of functional separation, be excluded by the technical officers from the material forwarded to tactical officers (and be kept separate for potential review by the court at the request of the defence).

Other forms of accessing data generated in the home

Three forms of collecting data outside the home (may) give insight into activities inside the home: gathering data from publicly available sources, a production order, and stealthy collection of data.

Internet investigations

It is generally accepted that the police can acquire data from publicly available sources, as these data are publicly available; the primary form of this is Internet investigations (i.e., investigating what is available about a person or topic from the publicly available parts of the Internet, using search engines and data-analytic tools). Collecting and analysing data from publicly available sources can be based on article 3 Police Act 2012. Since so much information can nowadays be derived from publicly available sources, however, it has been suggested in the literature that open-source intelligence (OSINT) can constitute a more than minor privacy infringement, particularly if it is done systematically, over a longer period of time, and/or using sophisticated tools for data mining and analysis.[220] Systematic forms of Internet investigations might perhaps be based on the power of systematic observation (thus requiring an order from the Public Prosecutor), but it is questionable whether article 126g Sv provides a proper legal basis since Internet investigations do not really constitute *following* a person or monitoring their *behaviour*. Moreover, it can give insight into someone's past, as opposed to the present behaviour that is normally monitored through systematic observation. A *sui generis* regulation therefore is more appropriate. In the draft proposal for the modernized Code of Criminal Procedure, a power has been included to allow the police to systematically copy data from open sources (such as the Internet). The power could be used to investigate crimes with a maximum sentence of at least one year's imprisonment and requires an order from the Public Prosecutor.[221]

Gathering data from the (publicly accessible parts of) Internet can include data generated inside a home or about people's home life, for instance through tweets, webpages and photographs that people have published themselves. Data may also be put online by others, however, which might make the collection by the police more privacy-intrusive, particularly if the inhabitant of a dwelling has not consented to such publication or does not even know such data are available. An extreme example of this would be a website where a hacker live-streams the images of hacked webcams, such as nannycams. Although such images are publicly available, watching and/or recording their footage constitutes a considerable privacy intrusion and therefore cannot be based on article 3 Police Act 2012. Given the prohibition of watching inside homes with hacked webcams (see subsection 'Hacking' above), the police would also not be allowed to use such publicly available live-streams through systematic observation. For less intrusive forms of Internet monitoring, the police could gather data on the basis of article 3 Police Act 2012 as long as the

[220] J.J. Oerlemans and B.J. Koops, 'Surveilleren en opsporen in een internetomgeving' (2012) 38 Justitiële verkenningen 35.
[221] Proposed art. 2.8.2.4.1, *Wetsvoorstel tot vaststelling van Boek 2 van het nieuwe Wetboek van Strafvordering: Het opsporingsonderzoek*, 7 February 2017, available at https://www.rijksoverheid.nl/documenten/kamerstukken/2017/02/07/wetsvoorstel-tot-vaststelling-van-boek-2-van-het-nieuwe-wetboek-van-strafvordering.

collection does not constitute a more or less complete image of certain aspects of someone's private life. When that threshold is reached, the police should resort to systematic observation, for lack of a more appropriate investigative power on which Internet investigations can be based.

Production orders

In 2006, a comprehensive regulation was enacted for the police asking people and organisations to provide them with personal data.[222] Powers were introduced for data production orders, differentiating between three types of data:

- identifying data about persons, which can be ordered by investigation officers for any felony (art. 126nc Sv);
- 'ordinary' personal data, which can be ordered by the Public Prosecutor for pre-trial detention crimes (art. 126nd Sv); also data that will be processed in the future can be ordered (article 126ne Sv) for an (extensible) period of four weeks;
- 'sensitive' personal data (i.e., concerning religion or belief, race, political affiliation, health, sexual life, or trade union membership), which can be ordered for pre-trial detention crimes that seriously breach the law, with authorization from the investigative judge (art. 126nf Sv).

Data production orders can include data generated in the home if they are accessible from service providers, e.g., data generated by IoT devices. In the Dutch context, particular discussions have taken place in relation to data generated by smart energy meters, since the Bill to roll-out smart meters initially made it mandatory for all households to accept a smart meter that would send electricity data every 15 minutes to providers. The Bill was rejected by the Senate because such high-density recordings could give considerable insight into home life and refusal of a smart meter was punishable with six months' imprisonment. The subsequent smart-metering Bill that was passed allowed more choice to consumers, including to refuse a smart meter or to have it function only in 'dumb' mode.[223] Nevertheless, the police, using the power of article 126nd Sv, can collect data about household electricity consumption through a production order to utility companies. Depending on the granularity of the data, this will then give more or less insight into in-home life (e.g., when inhabitants are at home or on holiday, how many people likely live in a dwelling).

Stealthy collection of data

Another method for acquiring data is to collect information from the circle of people around (and including) the suspect, without being recognizable as a police officer, through the power of 'systematic acquisition of information' (*stelselmatige inwinning van informatie*, art. 126j Sv). It can be ordered by the Public Prosecutor for any felony, for a maximum period of three months (which can be prolonged multiple times). The term 'systematic' is the same as in the power for systematic observation (*supra*, subsection 'Visual and aural monitoring'); the criterion of a more or less complete image of certain aspects of someone's private life applies here as well.[224] An investigation officer can thus maintain contacts with the suspect or with people from his immediate circle, and for instance participate in a sports club, Internet newsgroup, or go to the same nightclub as the suspect. Although of course not as such a form of monitoring the home from the outside, investigation officers can gather substantial information about the activities in the home and the family life of a suspect using this power.

4.4. Common-law cases[225]

This section will present a number of important common law cases from the US, Canada and the UK to illustrate how common law courts are dealing with the issues of surveillance of homes from

[222] Data Production Orders Act (*Wet bevoegdheden vorderen gegevens*), *Staatsblad* 2005, 390 (entry into force 1 January 2006).
[223] For an overview of the law and debate, see C.M.K.C. Cuijpers and E.J. Koops, 'Smart Metering and Privacy in Europe: Lessons from the Dutch Case' in S. Gutwirth and others (eds), *European data protection: Coming of age (*Springer 2012) 269.
[224] Y. Buruma, 'Stelselmatig: een sleutelbegrip in de wet bijzondere opsporingsbevoegdheden' (2000) 25 NJCM-bulletin 649.
[225] We gratefully acknowledge the input from Bryce Clayton Newell for this section.

the outside, to broaden the perspective offered by the civil law jurisdictions discussed in the previous sections. Our aim is not to extend our comparative legal research to these common-law jurisdictions, which falls outside the scope of this paper, since the primary countries involved in our research are Germany, Poland, and the Netherlands. Moreover, since these primary countries are civil-law jurisdictions, they do not easily compare with the common-law systems, so that an in-depth analysis of common-law jurisdictions is not useful for drawing conclusions on the legal frameworks in our civil-law jurisdictions. Instead, the aim of this section is to briefly scan how courts in common-law jurisdictions have dealt with cases involving monitoring the home from the outside, with a view to generating novel ideas or additional arguments that might shed new light on possible open questions regarding home monitoring; such novel ideas or arguments then serve to supplement the analysis in the primary jurisdictions in situations of legal uncertainty. We focus here on case-law rather than statutory law, partly because of the more important role of case-law in common-law systems, and partly because cases – since they are by definition case-specific – provide more insight into how the law applies to concrete manifestations of home monitoring.

In a decision from 1967, Katz v. United States,[226] the Supreme Court held that the use of an electronic listening device attached to the exterior of a public phone booth, without a warrant, violated individual privacy rights granted by the Fourth Amendment. Justice John Marshall Harlan II, in his concurring opinion, elaborated what has become known as the "reasonable expectations of privacy test."[227] The test announced by Justice Harlan requires that, for a warrantless search to be unreasonable (and thus violate the Fourth Amendment), the person subject to the search must "have exhibited an actual (subjective) expectation of privacy" and that such an expectation must also "be one that society is prepared to recognize as 'reasonable.'"[228] The Katz decision overruled the Supreme Court's earlier decision in Olmstead v. United States (1928)[229] and has remained the Court's predominant test for reasonableness ever since.

Katz demonstrated that he expected privacy—an expectation the majority of the justices found to be objectively reasonable. The two-pronged analysis was finally accepted as the appropriate test by the majority of the Court in the 1979 case of Smith v. Maryland.[230] Generally, the Court has not relied on empirical data when deciding what the society considers reasonable when using the Katz test, therefore, the test largely relies on a fiction of sorts.

Until 2012, the reasonable expectations of privacy test was generally employed by the Court in Fourth Amendment cases as the sole test for reasonableness. However, in United States v. Jones,[231] the Supreme Court held that because of the Fourth Amendment's historic ties to property, Katz had not actually overruled physical trespass as a means of implicating the Fourth Amendment's prohibition on unreasonable search or seizure; rather, Katz had merely expanded the scope of Fourth Amendment protections to some situations that did not involve trespass. Thus, both Justice Harlan's test and the historic trespass test could be invoked in future Fourth Amendment cases as means to invalidate government conduct and exclude evidence from criminal prosecutions.

In California v. Greenwood,[232] the US Supreme Court held that warrantless searches of garbage placed at the kerbside for collection by trash collectors did not violate the Fourth Amendment's prohibition on unreasonable searches. In the case, the police suspected the defendant of engaging in unlawful drug-related activities inside his home, but did not have probable cause to get a warrant to search his house. Instead, they decided to search his garbage, and then used the evidence they obtained from the garbage bags to generate probable cause and get a warrant to search the house. The Court held that Greenwood had no reasonable expectation of privacy in

[226] Katz v. United States, 389 U.S. 347 (1967).
[227] Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring).
[228] ibid.
[229] Olmstead v. United States, 227 U.S. 438 (1928).
[230] Smith v. Maryland, 442 U.S. 735 (1979).
[231] United States v. Jones, 565 U.S. 400 (2012).
[232] California v. Greenwood, 486 U.S. 35 (1988).

his garbage when it was left for collection on a public street that was "readily accessible to animals, children, scavengers, snoops, and other members of the public."

In Canada, the Supreme Court held in *R v. Patrick*[233] that there is no reasonable expectation of privacy in garbage placed outside the house for garbage collectors, since the garbage has been abandoned. According to the majority of the court, "[the defendant] abandoned his privacy interest in the information when he placed the garbage bags for collection at the back of his property adjacent to the lot line. He had done everything required of him to commit the bags to the municipal collection system. The bags were unprotected and within easy reach of anyone walking by in the public alleyway, including street people, bottle pickers, urban foragers, nosey neighbours and mischievous children, not to mention dogs and assorted wildlife, as well as the garbage collectors and the police. However, until garbage is placed at or within reach of the lot line, the householder retains an element of control over its disposition. It could not be said to have been unequivocally abandoned if it is placed on a porch or in a garage or within the immediate vicinity of a dwelling. Abandonment in this case is a function both of location and [the defendant's] intention." [234]

Related to thermal imaging, Kyllo v. United States is a U.S. Supreme Court decided on June 11, 2001.[235] In the case, the Court decided that the warrantless use of a thermal imaging device by government agents to detect levels of heat emanating from the exterior of a private residence violated the Fourth Amendment to the U.S. Constitution. The Fourth Amendment guarantees the right of the citizenry to be free from unreasonable searches and seizures, by government agents, of their persons, houses, papers, or effects. The Kyllo decision is important to questions of surveillance and privacy because the Court held, broadly, that the use of any technology (not just thermal imaging scanners) "not in general public use" to gather information about the interior of a person's home was presumptively unreasonable.

The Kyllo case thus departed from earlier cases holding that when officers gather information that is plainly visible from places where the officers have the right to be, no unreasonable search has occurred. Unlike aerial observation from public airspace, the Court stated, the technological enhancement offered by the thermal imaging device constituted "more than naked-eye surveillance,"[236] thus implicating the Fourth Amendment. Because the search was conducted without a warrant, it was presumptively unreasonable and violated the defendant's rights. Importantly, the opinion was not limited merely to thermal imagers. In fact, the Court found that any sense-enhancing technology that would allow law enforcement to gain information that would have traditionally been only discovered through a physical intrusion into a person's home would constitute a search, for Fourth Amendment purposes, as long as the technology was not in general public use. The Court rejected the contention that "off-the-wall" surveillance (measuring emanations from the outside of a home rather than viewing activity inside) should be treated differently than "through-the-wall" surveillance (which could actually peer through walls or windows to detect activity). Thus, the Kyllo decision was explicitly aimed at regulating the future use of a broad array of emerging and yet-to-be-invented technologies, based on a mix of traditional property-based Fourth Amendment ideas and the Supreme Court's reasoning in Katz.

In a Canadian case, R. v. Tessling (2003), the Court of Appeal of Ontario (later overruled by the SCC) ruled that an aerial scan of a home with infrared thermal imaging technology was a search because it "it reveals what cannot otherwise be seen and detects activities inside the home that would be undetectable without the aid of sophisticated technology" (para. 68).[237] On appeal in R. v. Tessling (2004), however, the SCC characterized the overhead thermal scan of a home "as an external search for information about the home which may or may not be capable of giving rise to an inference about what was actually going on inside, depending on what other information is available" (para. 27). Finding that the lower court had relied on the "theoretical capacity" of the thermal infrared system to find a reasonable expectation of privacy rather than examining the actual "inferences that may be justified are extremely limited" (para. 35), the court found that the

[233] R. v. Patrick, 2009 SCC 17, [2009] 1 S.C.R. 579.
[234] ibid.
[235] Kyllo v. United States, 533 U.S. 27 (2001).
[236] ibid.
[237] R. v. Tessling, [2004] 3 S.C.R. 432, 2004 SCC 67.

use of the FLIR technology had not violated the defendant's rights. Justice Binnie noted in R. v. Tessling (2004) that “If, as expected, the capability of FLIR and other technologies will improve and the nature and quality of the information hereafter changes, it will be a different case, and the courts will have to deal with its privacy implications at that time in light of the facts as they then exist” (para. 29). This choice to judge reasonableness on a case-by-case basis is partly an expected result within common law systems, but it also suggests that high courts are unwilling to craft broader, more overarching theories to regulate police searches.

In Tessling, the court stated that "The United States Supreme Court declared the use of FLIR technology to image the outside of a house to be unconstitutional in Kyllo v. United States, 533 U.S. 27 (2001), based largely on the “sanctity of the home” (p. 37). We do not go so far. The fact that it was the respondent’s home that was imaged using FLIR technology is an important factor but it is not controlling and must be looked at in context and in particular, in this case, in relation to the nature and quality of the information made accessible by FLIR technology to the police."

In another Canadian case *R. v. Plant* relating to energy consumption data[238] the court judged whether a warrantless search of computerised electrical consumption data violated section 8 of the Charter of Rights and Freedoms, which includes the right to be secure from unreasonable search and seizure. The court held that the police collection of computer records on electricity consumption was not unreasonable and that the accused had no reasonable expectation of privacy in the computer records on electricity consumption, primarily because these records “do not reveal intimate details of the accused’s life.” According to the Court in *R. v. Plant*, the Charter protects informational privacy by seeking “to protect a *biographical core of personal information* which individuals in a free and democratic society would wish to maintain and control from dissemination to the state. This would include information which tends to reveal intimate details of the lifestyle and personal choices of the individual.”[239]

Similarly, in *R. v. Gomboc*,[240] the Canadian Supreme Court built on *Plant*, in a case where the police had requested, without a warrant, that an electric utility company install a digital recording ammeter (DRA) to measure the flow of electricity into a residence suspected of housing a marijuana grow operation. The court held that collecting data from devices such as a DRA does not constitute a search under section 8 of the Charter and that there was no objective expectation of privacy in that information about electricity flow. In coming to this conclusion, the court majority held that a “critical factual consideration (...) is the degree to which the use of DRA technology reveals private information.” In this case, the “DRA is a technique that reveals nothing about the intimate or core personal activities of the occupants. It reveals nothing but one particular piece of information: the consumption of electricity”, because the electricity flow did not disclose any “biographical core data” or reveal “intimate and private information for which individuals rightly expect constitutional privacy protection.”[241]

In England and Wales, it is clear from the structure and language of the legislation regulating covert surveillance of the home that the interests it protects are those guaranteed by Article 8 of the European Convention on Human Rights. It adopts, for the purposes of determining whether surveillance should be authorized, the methodology established by the text of the Convention and the jurisprudence of the ECtHR. Those considering authorizing, and ultimately the courts determining the ‘constitutionality’ of any covert intrusive surveillance activity will be required to consider (i) whether the surveillance is (or was) necessary for one of the purposes set out in the legislation – the detection or prevention of serious crime, the interests of national security or the economic well-being of the United Kingdom, and (ii) whether the nature and scope of the surveillance is proportionate to what is sought to be achieved. This inevitably requires some consideration of the quantity and nature of the information about a person’s private and family life that is likely to be obtained as a consequence of the particular form and duration of the surveillance in question. The more intimate and sensitive the personal information likely to be

[238] R. v. Plant, [1993] 3 SCR 281 (1993).
[239] R. v. Plant, 3 S.C.R. 281, 293 (1993) (emphasis added).
[240] R. *v.* Gomboc, 2010 SCC 55, [2010] 3 S.C.R. 211.
[241] Ibid.

captured by the surveillance the greater the justification there will have to be in terms of the seriousness of suspected criminal activity or threat to national security.

Fewer cases are available in England and Wales than in the US or Canada when it comes to monitoring the home from the outside. Such monitoring is largely covered by the Regulation of Investigatory Powers Act (RIPA), but there is a scarcity of cases. We therefore limit ourselves to pointing out two interesting aspects of RIPA. First, it regulates only *covert* surveillance of the home (i.e., monitoring of which the monitored persons are calculated to remain unaware of). This implies that *overt* surveillance of the home, such as the non-covert use of (mobile) CCTV cameras directed at the windows of a house, camera-equipped drones, or visible thermal imaging devices, are unregulated by RIPA, and can presumably be conducted by police without an explicit legal basis or particular safeguards (although, of course, subject to the standards of Article 8 ECHR). Second, since "covert surveillance" is broadly defined, RIPA covers both surveillance of the inside and monitoring the outside of the home. What matters is whether the monitoring "is likely to result in the obtaining of private information about a person"; if that is the case, the specific safeguards of RIPA (including authorisation, subsidiarity, and proportionality requirements) apply.

What can we **conclude** from these common-law cases in terms of novel ideas or arguments that can supplement the comparative legal analysis of German, Polish, and Dutch law, in particular where the latter face situations of legal uncertainty? Our main conclusion is that the cases do not show radically or fundamentally different approaches to the regulation of monitoring the home from the outside; overall, there are considerable similarities in terms of the level of intrusiveness that various types of monitoring are considered to have. In that sense, common-law cases do not open up really novel perspectives.

What common-law cases do offer, however, are some nuances and supplementary arguments that may be useful for civil-law jurisdictions to consider when facing interpretation problems or when considering legislative changes in view of developments in home monitoring technologies. One interesting nuance is visible in the garbage search cases. Although common-law systems generally show the same approach as the civil-law systems we discussed, in considering garbage searches lowly intrusive, there is an interesting nuance in *Patrick* that the proximity of the garbage to the home territory matters, in combination with the owner's intent to really want to dispose of the garbage that can be inferred from the position of the garbage in relation to the house or the surrounding property. Garbage outside or on the boundary of one's property (such as the front yard) can be thought to be really left for others to collect, while garbage on the property (such as outside the front door but well within the perimeter of the front yard) still has a reasonable expectation of privacy, since it falls under the owner's control. This nuance is interesting when we consider how the argument would apply to sewage monitoring: perhaps it is less relevant to look at the legal ownership of the part of the sewage system where monitoring occurs (i.e., distinguishing between the private part and the public part of the sewage), and more relevant to look at the inferred intent to dispose of waste. While a garbage bag outside one's front door can be taken inside the house again, or taken along when the owner goes shopping to dispose of elsewhere, sewage waste cannot be retrieved once it is flushed down a toilet or down a drain. This is not to say that there is no reasonable expectation in waste flushed into the sewer (because, in contrast to garbage bags, sewage waste cannot just be picked up by any citizen passing by the house), but it does suggest that the ownership of a monitored part of the sewer matters less than the user's control over the waste flow.

Another interesting argument is *Kyllo*'s emphasis on the fact that thermal imagers were not a technology "in general public use", thus suggesting that people should expect the police to use technologies that many citizens are using as well; in other words, where police use technologies that are available off-the-shelf from the local Wal-Mart, there is less reason to require an explicit legal basis (and additional safeguards) for this use than when the police use sophisticated technologies that are tailor-made for investigation purposes. This could be an additional argument to distinguish sewage monitoring from garbage searching, since anyone can use a pick-up car and a knife to collect and cut open garbage bags, but the general public does not have access to sewage-monitoring devices that are developed specifically and tailor-made for law enforcement purposes.

Another argument – which is not completely new, since it is also (sometimes implicitly) used in the civil-law jurisdictions – is that one should not only consider the novelty or spread of a technology (as in *Kyllo*), but also at the actual capacities of the technology at issue. *Tessling* approached thermal imagers through the lens of the limited information that this technology yielded, and observing that if the nature and quality of information made available by this technology increases in the future, the conclusion might be different. This could be used as an argument to consider sewage monitoring a lowly-intrusive measure, if it is done using specialised and very substance-specific configurations, which only yield a very limited type of information (namely the presence of certain drug production-related chemicals).

More generally, particularly in Canada but also in England and Wales, we see an emphasis on the informational content of what a specific form of monitoring (in concrete cases) is capable of yielding. In Canada, courts particularly apply a criterion whether it concerns information "which tends to reveal intimate details of the lifestyle and personal choices of the individual" (*Plant*). Intimate details of lifestyle and personal choices are typically associated with domestic life, as the home is the place where traditionally intimacy can be enjoyed, and where one can do whatever one wants without fear of being seen. We think that a criterion whether a certain form of monitoring the home from the outside is capable of revealing intimate details of one's life, or more generally, is capable of sketching an actual picture of someone's home life, could be very useful to distinguish between a) investigation measures that are intrusive but not overly so (i.e., they yield certain information about private life, but not a real picture of domestic life) and b) measures that are highly intrusive (because the reveal a considerable part of someone's domestic life).

5. Conclusion and recommendations

The aims of this paper included (1) making an inventory of forms of covert surveillance of in-home activities similar to sewage monitoring; (2) assessing to what extent people are protected against non-physical intrusions of home life, based on legal analysis of how covert surveillance of in-home activities is qualified under constitutional and criminal procedure law in Germany Poland and the Netherlands; (3) scanning major cases in common-law countries to generate possible ideas for resolving issues relating home monitoring in addition to the comparative legal analysis of the primary jurisdictions; and (4) recommending improvements of legal protection of home life against non-physical intrusions.

5.1. Inventory of forms of monitoring of the home

We grouped the inventory of different forms of covert monitoring of in-home activities in five larger groups, each further divided into specific forms of monitoring. Although we do not claim full comprehensiveness as to the specific forms and focus only on the most relevant ones, the general grouping of these forms into higher-level forms should reasonably cover most new types of monitoring of the home that may be developed in the future.

The first higher-level form of intrusions is the monitoring of domestic waste; this includes sewage monitoring and garbage searches. These measures target waste that people (more or less consciously) discard into public space to be processed by public utility companies; for such waste, people exercise a certain level of control over what will be disclosed in public. Although the two specific forms are largely similar, we identified important differences between sewage monitoring and garbage searches including the more periodic disposal of garbage as opposed the more continuous disposal of sewage waste, the relative visibility of garbage searching compared to sewage monitoring, the need for technical tools for sewage monitoring and the more limited possibilities of obfuscation in case of sewage disposal.

The higher-level form of monitoring that is perhaps most similar to the monitoring of domestic waste is the monitoring of the emanations from the house, which includes the monitoring of heat, smell (olfactory surveillance) and electromagnetic emanations. Unlike the monitoring of domestic waste, which relies on active disposal of waste by the inhabitants, these emanations generally leave the protected space of the home without active involvement or (more or less) conscious

decisions of the inhabitants. Although there certainly are ways to prevent or limit these emanations, the inhabitants exercise less control over them than with regard to domestic waste.

Monitoring of waste and emanations from the home are generally considered less intrusive than the acoustic and visual monitoring of the home. Audio-visual monitoring constitutes the third higher-level form of surveillance of the home in our inventory. It is generally considered the most intrusive form, since seeing what happens inside the home, and hearing what is being said there, are the most direct and informative ways of observing home life. Acoustic surveillance, aiming to hear and/or record speech and sound from inside the home, relies either on eavesdropping or on aural-space interceptions or wiretapping. Visual monitoring, which is often combined with acoustic surveillance, obtains the image from inside the home, and can either take the form of naked-eye observation, technically-enhanced observation, or visual recordings. A special case of (audio-)visual monitoring is the aerial monitoring of the home.

The last two higher-level forms of monitoring of home life rely on getting access to data relating to home life. We distinguish between access to data located inside the home, including network searches and police hacking, and data located outside the home but revealing relevant information about home life, which includes access to communication data generated in the home, search and seizure of data stored with third parties and data production orders to such third parties.

Table 1 shows summarises the inventory of forms of monitoring the home from the outside.

High-level type	Sub-type	Object of surveillance
Waste monitoring	Garbage search	Domestic solid waste
	Sewage monitoring	Domestic liquid waste, bodily excretions
Emanations monitoring	Thermal imaging	In-home/roof/wall temperature
	Olfactory surveillance	In-home smells
	Electromagnetic surveillance	In-home electromagnetic radiations
Audio-visual monitoring	Acoustic surveillance	In-home sounds
	Visual surveillance	In-home sights
	Aerial surveillance	Sights inside/on home not visible from street or buildings
In-home data acquisition	Network search	Data stored in/processed by computers/devices in the home
	Remote access to computers (police hacking)	Data stored in/processed by computers in the home
Outside-of-home data acquisition	Communications surveillance	Content/metadata of home-based telecommunications
	Searches at service providers	Data about home life stored with service providers
	Production orders to service providers	Data about home life stored with service providers

Table 1. Types of monitoring the home from the outside

5.2. Legal assessment of covert surveillance of in-home activities

In this section, we will provide a brief summary of the main structure of the law covering monitoring of the home in the context of criminal procedure in each of the three countries, and

then per higher-level form of intrusion compare the main similarities and differences in how these forms of intrusion are regulated. In the latter part of the section, we will refer to case law from the common-law countries where this provides interesting or inspiring additional insights compared to the main, civil-law, countries we studied for this paper.

5.2.1. Assessment per country

In Germany, the inviolability of the home (Art. 13 GG) protects primarily from physical entries, but the home's purpose as a spatial area of privacy can also be infringed if it is possible to monitor events in the dwelling by technical means.[242] This applies even when the home is monitored from the outside.[243] The surveillance of homes is considered to be a particularly serious intrusion of privacy. Surveillance that allows observing the outside of homes is clearly distinguished from that which targets the inside. The former interferes with constitutional protection of informational self-determination (not inviolability of the home); the surveillance measures undertaken pursuant to it will end at the doorstep, and this should be ensured by technical means if need be.[244] It is interesting to note that acoustic surveillance of the home is distinguished from other forms of monitoring (e.g. visual) and permitted in a wider array of situations. Furthermore, the core area of private life is (almost) absolutely inviolable and must not be infringed by surveillance measures. The core area applies regardless of where private life is taking place, but surveillance of the home is more likely to infringe the core area than surveillance outside of the home.

In German criminal procedure law, a legal basis does not need to consist of a single provision, but can, depending on the actual conduct, consist of several provisions. The legislator created Section 161 StPO (basis for conduct of the Prosecution Office) and Section 163 StPO (basis for Police or other investigative personnel's conduct) with the intention of providing a general legal basis for measures that interfere with fundamental rights in a less substantial way.[245] For surveillance taking longer than 24 hours or occurring during two or more days, Section 163f StPO (*lex specialis*) is most relevant; this applies when a "criminal offence of substantial significance" could have been committed. These legal bases may be used for those surveillance measures that stop at the doorstep and do not interfere with the inviolability of the home. Section 100h paragraph 1 under 2 of the StPO often acts as an additional legal basis when technical means for observations are needed.

Arguably, the only provision of the StPO that allows to directly monitor (in a covert manner) what is happening inside homes is Section 100c StPO, which regulates acoustic monitoring of private dwellings. Nevertheless, other covert investigation measures further permit to gain information from private homes, even if only in an indirect manner. This includes Section 100a StPO, which allows to intercept the content of telecommunications, a newly introduced Section 100b StPO, which permits covert access by technical means to information-technology systems (to collect data or monitor activity of the suspect), Section 100g StPO, which permits the collection of traffic data, and Section 100j StPO, which grants access to subscriber data stored with the service provider.

Lastly, the BKA (Federal Criminal Police) is permitted to conduct both acoustic and visual surveillance of private homes under Section 20h BKAG, in special cases where safety or security are under imminent threat.

In Poland, the usual understanding of the term inviolability of the home is a relative prohibition of search, unauthorized entry and stay in someone's closed house or any other space protected by the inviolability of the home (Art. 50 Constitution) without the consent of the owner or inhabitant. However, according to some authors, the protection of the home extends beyond the prohibition of physical intrusion. It would also contain protections against more remote techniques and measures, such as installation of video cameras, wiretapping systems, or peeping in.

In Polish criminal procedure, with the exception of wiretapping, the powers of covert surveillance are not regulated in the Code of Criminal Procedure, but in the Police Act. The relevant provisions

[242] BVerfGE 65, 1 (40) = NJW 1984, 419, BVerfGE 109 , 279 (309) = NJW 2004, 999 ff.
[243] BeckOK Grundgesetz, Epping/Hillgruber, 8.
[244] BVerfG, Judgment of the First Senate of 20 April 2016 - 1 BvR 966/09, para. 148.
[245] Wohlers, before § 94, Rn. 1.

of the Police Act (Art. 14-22) regulate the so-called operational reconnaissance activities. This term is understood as an array of activities aiming at gathering information about a crime and obtaining evidence that will allow or facilitate to establish the course of events.[246] The key provision here is Art. 19, which regulates operational surveillance (covering an array of covert surveillance powers), which includes the most intrusive forms of surveillance, such as those that infringe upon the inviolability of the home, that are subject to rather strict procedural requirements. Interestingly, the requirement of judicial authorization for visual and acoustic monitoring of the home is even stricter than the requirement for house searches.

The means and measures that the Police can use in the exercise of operational surveillance have been recently reformed, following a decision of the Constitutional Tribunal that contested the specificity and precision of provisions that empower authorities to use them. In the judgement, recommendations were made to specify not only the methods and means that can be used, but also the crimes that justify such a severe interference; time limits; the procedure to be followed; and the subsequent use of the findings. Moreover, what was highlighted by the Tribunal is that such measures should be employed in line with the subsidiarity principle, and hence only when there is no alternative available. Moreover, there should be an independent controlling authority.

Much of the literature on operational surveillance in Poland is outdated and comments on the previous wording of the provision, so that doctrinal discussions do not provide a good source for interpretation. Furthermore, the secretive nature of these powers and their scarce use as evidence in criminal proceedings (and resulting lack of case law) has created a situation where it is difficult to describe clear limits of these powers. The list of means of operational surveillance remains to a large extent technologically neutral. It does not actually specify the means, tools and techniques, but only the type of evidence that can be obtained, i.e. contents of communications, picture and sound from private places, contents of correspondence, data from data carriers and IT systems and content of packages. Such regulation could be seen as too specific in some ways (excluding relevant types of evidence, e.g. chemical substances), but too broad at the same time, not providing any limits on how the evidence can be collected.

Further surveillance powers are included in Article 19a and 19b of the Police Act. Art. 19a provides a legal basis for controlled purchase, controlled delivery and covert surveillance of the objects of crimes. While this legal basis could be used for less infringing means, the relatively loose procedural safeguards would probably not be sufficient for measures interfering with the inviolability of the home. From the existing provisions, it is often not clear what exactly the police is allowed and not allowed to do.

In the Netherlands, Article 12 Constitution provides special protection to the dwelling, but only against entering without the inhabitant's consent. The limitation to entering implies that generally, observing the inside from the outside is not considered to fall under the constitutional protection. This is criticised in the literature, since observation from the outside can also impact on the peace of the home. Since monitoring the home from the outside (without physical entering) does not infringe article 12 of the Dutch Constitution, there are no specific constitutional requirements for monitoring the home from the outside from the perspective of the sanctity of the home. Nevertheless, there may be limitations based on the general right to privacy, and the law-maker has also sometimes opted for specific limitations in the Code of Criminal Procedure because of the sensitivity of monitoring the home from the outside

According to Dutch case law and doctrine, minor privacy infringements can be based on the general task description of the police (art. 3 Police Act 2012 in conjunction with the designation of investigation officers in art. 141-142 Sv). What is considered minor, depends on the circumstances; the law-maker has not clarified when the threshold between minor and significant privacy intrusions is met. The level of intrusion is significant (i.e., more than minor) where the surveillance measure reveals a more or less complete image of certain aspects of someone's private life; then, surveillance becomes, in Dutch legal terms, "systematic", and requires an explicit legal basis in the Code of Criminal Procedure. The concept of systematicness has been

[246] Wojciech Kotowski, 'Ustawa o Policji. Komentarz' 441; *80/7/A/2014 Wyrok z dnia 30 lipca 2014 r. (Sygn. akt K 23/11)* (n 135) [6.1.4].

particularly developed in the context of systematic observation (art. 126g Sv), where a set of factors have been identified that, usually in combination, determine whether a police activity constitutes a more than minor privacy intrusion, and thus requires an explicit legal basis. These factors are: use of a technical device; place; intrusiveness, continuity, or frequency; duration; and possibly the degree of suspicion.

For monitoring the home from the outside, this implies that the legal basis can be found in article 3 Police Act 2012 as long as the monitoring constitutes a minor infringement of the right to privacy. As soon as the infringement is more than minor, an explicit legal basis in the Code of Criminal Procedure is required. Depending on the technology used, this may be the power of systematic observation (art. 126g Sv), oral interception (art. 126l Sv), hacking (art. 126nba Sv), production orders (art. 126n et seq. Sv), or another specific basis.

Protection of the home against monitoring from the outside has been particular discussed in relation to audio-visual surveillance. While visual surveillance from the outside is generally forbidden (except when done by police officers who look inside and take pictures only when they observe something relevant for the investigation), acoustic surveillance inside the home is allowed. The latter has strict conditions, however (only being allowed for the most serious crimes), and this applies both to covertly entering the house to place a bug and to recording conversations from the outside.

5.2.2. Assessment per higher-level type of monitoring

Monitoring of domestic waste, whether in the form of sewage monitoring or a garbage search, would likely not constitute a major intrusion of home life in any of the jurisdictions we studied. However, none of the countries offer specific regulation of sewage monitoring or garbage search, and therefore these measures must be based on other, more general provisions.

This is clear in the Netherlands with regard to garbage searches, where available Supreme Court case law indicates that people cannot objectively have a reasonable expectation of privacy with respect to the contents of garbage bags they put on the street. Therefore, a garbage search can be based on the task description of the police. Although we are not aware of published case law on garbage searches in Poland and Germany, it can reasonably be assumed that the police could similarly inspect garbage located in public places based on general provisions, and that a more specific legal basis with additional procedural requirements would not be required. Arguably, however, in Germany, repeated garbage searches over a period longer than 24 hours would require the use of Section 163f StPO as a legal basis, making it subject to judicial authorisation.

Similar conclusions about the intrusiveness of garbage searches have been reached by courts in the USA and Canada. In both cases, the courts found no reasonable expectation of privacy in the garbage placed outside the house for garbage collectors, since the waste has been made accessible to the members of the public. The Canadian court, however, stressed that until garbage is placed at or within reach of the lot line, the householder retains an element of control over its disposition. It could not be said to have been unequivocally abandoned if it is placed on a porch, in a garage or within the immediate vicinity of a dwelling. The exact placing of the garbage might be also be of relevance in the civil-law countries. Were the garbage placed outside the house, but still within the borders of the property, it would likely enjoy similar protection against searches as objects inside the house (the adjacent, clearly delineated space around the house such as the garden, porch, front yard, is often considered part of the home, or otherwise more strongly protected than public places).

Although sewage monitoring seems similar to garbage searches, in the absence of regulation and case law relating to sewage monitoring, we should be careful in applying the same reasoning for sewage monitoring as courts have applied to garbage searches. The level of intrusion, and thus the legal basis, will depend on what exactly is monitored (e.g., which materials are being detected), how closely to the home, during which period, and how sophisticated the technology is. The type of monitoring usually involved in sewage monitoring (at least in the use case of targeted, suspicion-based monitoring) would likely not imply a more than minor privacy infringement in the Netherlands and Poland, since it is limited to the detection of specific chemicals associated with illegal drugs production. In Germany, the specific legal basis will depend on the period of time during which the monitoring takes place. The use of technology also requires combining the

general observation legal basis with the legal basis that allows the use of technical means. This last point somewhat complicates the use of sewage monitoring in Poland, since the Polish provisions allowing the use of technical means do not cover the collection of sewage waste (they are limited to electronic data, and visual and acoustic types of evidence). For Poland, it remains unclear whether provisions that do not provide for use of technical means can be applied to types of monitoring that deploy such technical means.

Doubts about the legal basis notwithstanding, it does not appear that either garbage searches or sewage monitoring would interfere with constitutional protection of the inviolability of the home, since the monitoring takes place outside homes, either on the street or in the public sewage system. That does not mean that facts relevant to home life will not be revealed by these forms of monitoring, but these will possibly fall under other protective provisions, such as the general right to privacy or the right to informational self-determination, or (as in the Dutch garbage case) fall completely outside the protection regime.

With regard to the monitoring of emanations from the house, where available case law exists, different conclusions can be reached for different countries. In the Netherlands, the question of inviolability of the home does not come into play with these surveillance measures. The more relevant question is whether the particular form of monitoring constitutes a systematic form of observation. Thermal imaging is not considered a more than minor privacy intrusion and can thus be based on the general task description of the police, since the technology only generally indicates a heat source that makes the walls or the roof warmer, but does not record heat waves from the inside of the home to the outside. Therefore, it can be argued that a thermal imager only monitors the outside of the dwelling. However, the available case law related only to a single use of thermal imaging, and the same reasoning might not apply to the use of such a technology over an extended time. The same is true for olfactory surveillance, where incidental human smell perception at the doorstep is not considered a more than minor intrusion of privacy; in contrast, using devices with chemical sensing for an extended period of time might require an explicit legal basis. However, although such surveillance would not be more intrusive than, e.g., audio-visual surveillance, it might not be permitted because no explicit specific legal basis for olfactory surveillance exists.

The use of tools monitoring emanations from the house under both German and Polish law is unclear. If these surveillance measures constitute an interference with the inviolability of the home, as suggested by some German authors in the case of heat imaging[247], there does not appear to be a legal basis in the Code of Criminal Procedure to conduct such surveillance, even though the Basic Law permits technical monitoring of the home in strictly defined cases. If the monitoring, however, is not deemed to interfere with the home, and is only considered to be monitoring the outside of the dwelling, the general observation powers, in combination with Section 100h StPO allowing to use technical means of surveillance outside dwellings, could form a legal basis in Germany. The assessment would probably depend on the particular set-up of the monitoring. In Poland, the collection of olfactory or heat imaging evidence is not covered by provisions allowing the use of technical means of surveillance. Therefore, only non-technical forms of heat monitoring and olfactory surveillance appear to be covered, although until recently, a more technologically neutral provision existed that could cover both types of monitoring. The use of technical means might require extended interpretation of existing provisions, which is rarely permitted in the law of criminal procedure.

The issue of thermal imaging has also been covered by the case law in the US and Canada. In Kyllo v. United States, the Supreme Court held that the warrantless use of thermal imaging by government agents violated the Fourth Amendment guaranteeing the right to be free from unreasonable searches and seizures. The Court held that the use of technology “not in general public use” was presumptively unreasonable. The judgement departed from previous decisions that allowed officers to gather information that is plainly visible from places where the officers have a right to be. Importantly, the Court rejected the contention that “off-the-wall” surveillance should be treated differently than “through-the-wall surveillance”, and thus reached a very

[247] Zöller/Ihwas, Rechtliche Rahmenbedingungen des polizeilichen Flugdrohneneinsatzes (NVwZ 2014, 408) 414.

different conclusion than the Dutch Court in a similar case. Interestingly, the same argument about technology not in general public use could be applied to sewage monitoring.

In Canada, the SCC on appeal in R. v. Tessling overruled the lower Court, which essentially had ruled along the same lines as *Kyllo*, and decided that the use of thermal imaging in the particular case did not violate the defendant's rights. However, it noted that if the nature and quality of information made available by this technology increases in the future, the conclusion might be different, and the reasonableness is to be judged on a case-by-case basis.

Visual and acoustic surveillance of the home, unlike the forms of monitoring described above, is more clearly regulated in all three jurisdictions we studied. Interestingly, both in Germany and the Netherlands visual surveillance seems to be considered more intrusive than acoustic surveillance, or at least it appears so due to the fact that visual surveillance of the home by technical means is excluded in both jurisdictions, while acoustic surveillance is allowed, albeit under very strict conditions. While the constitutional protection of the home in the Netherlands only protects against physical entry, the argumentation excluding visual intrusions into the home (other than naked-eye observation, which is allowed) has been based on the strong protection of the home. In Germany, the structure of Article 13 GG makes a distinction between acoustic surveillance and other forms of technical surveillance of the home, which are only allowed to avert acute dangers to public safety, especially dangers to life of individuals or to the public. In contrast, in Poland visual and acoustic surveillance and recording are allowed under the same provision and no legal distinction is made between the two. Perhaps, in that light, we should consider a different interpretation of German and Dutch law, namely that in-home visual observation is not per se considered more intrusive than in-home eavesdropping, but that the legal exceptions introduced by the law-maker to allow for in-home acoustic surveillance were induced by a greater need for law enforcement. After all, interception of communications is one of the most important means of gathering intelligence and evidence, particularly in organised-crime investigations, and both in Germany and the Netherlands, the law-maker did not want to allow homes to become a safe haven for (organised) crime perpetrators to communicate without any possibility for law enforcement to overhear the communication. Visual observation is generally less vital in organised-crime investigations, so that there was less incentive to create an exception to the inviolability of the home for in-home visual surveillance. In Poland, the law-maker seems to have considered both acoustic and visual surveillance important to be possible inside the home, and thus has allowed both forms under relatively strict conditions.

All three jurisdictions allow acoustic surveillance of the home, both from the outside and by covertly installing eavesdropping and recording devices inside the dwelling. These measures are generally restricted to a particular set of more serious criminal offences and subject to judicial authorization. While the Polish and Dutch provisions place strict procedural limitations on acoustic surveillance and recording in the home, German law goes further by excluding certain types of conversations from monitoring because they fall under the core area of private life, which is considered out of bounds for the law enforcement. The measure may be ordered only if—on the basis of factual indications, in particular concerning the type of premises to be kept under surveillance and the relationship between the persons to be kept under surveillance—it may be assumed that statements concerning the core area of the private conduct of life will not be covered by the surveillance.

Interferences combining audio and visual surveillance is possible under Section 20h BKAG (although that provision is currently unconstitutional because it has insufficient safeguards to protect the core area of private life, which needs to be repaired by the law-maker). However, according to the German Constitutional Court, interference combining audio and visual surveillance carries substantially more weight than, for example, audio surveillance only, and requires special justification. Accordingly, when ordering these measures, the suitability, necessity and appropriateness requirements for each form of surveillance must be examined individually, as well as with a view to their combination with one another. It will normally not be sufficient for the additional ordering of visual surveillance to cite merely the increased ease at matching voices with persons; more significant grounds relevant to the necessity of the

surveillance are needed. In the context of applying the law, these requirements can and must be taken into consideration.[248]

Network searches are regulated in Germany and the Netherlands in a similar way, while in Poland they are not regulated at all. Both in Germany and in the Netherlands, a search can be extended from the place being searched to a computer located elsewhere, if the connection is lawfully accessible from the local computer. Dutch law (in an apparent legal lacuna) allows computers in homes to be searched from computers located in vehicles, without particular safeguards for home protection. Lawfully accessible means that practices such as hacking or using a hacker's connection to hacked computers are excluded from such extensions of the search to remote computers.

However, recent reforms have introduced such powers, so-called police hacking, in the laws of all three jurisdictions[249] we studied. The police hacking laws in the three countries differ from each other in some important aspects. The clear outlier is Poland, which unlike the more precise and elaborate formulation of the Dutch and German laws, only includes a vague and open-ended provision that allows the police to covertly obtain data from information systems, as one of the forms of operational surveillance under the Police Act. Considering the intrusiveness of such a measure, from a doctrinal perspective it is still questionable whether the present legal framework is sufficiently clear and precise to provide a legal basis for such a measure. Comparing the German and Dutch provisions, the new law in the Netherlands appears to allow a broader range of activities to the police once they covertly gain access to a computer. German law limits access to gathering existing data; the investigators cannot generate new data by for example turning on the computer's microphone or camera. Dutch law permits a wider range of uses, including determination of certain characteristics of the user or the computer, recording confidential communications, securing data stored on the computer and those entering the computer over the period of surveillance, and unlike Germany, also systematic observation and oral interception by for instance turning on the camera or microphone, as well as the possibility to delete unlawful data from the user's computer.

It should be noted that very strict safeguards (among the strictest for any investigative powers) are placed upon police hacking in all three countries. Interestingly, in all three countries, the safeguards and procedural requirements are by and large the same for police hacking as they are for oral interception in the home. However, these strict requirements do not seem to be based on the protection of the home, since the location of the computer (in the home or elsewhere) does not play a role in the exercise of police hacking powers. The fact that the computer is located in the home does not increase procedural requirements, since it is the computer, not the home, that is being protected. Because covert remote computer searches are considered among the most intrusive measures, comparable to surveillance of the home, computers are afforded comparable protection regardless of their location. That is why the inviolability of the home does not really come into play here. In Germany, police hacking is not considered an interference with the home, but with the right to integrity and confidentiality of information technology systems, which is based on the general personality right protected in Art. 2 GG.

Furthermore, in Germany, the same rules about the protection of the core area of private life that apply to acoustic surveillance (see 4.1.2 under 'Visual and aural monitoring') apply (with small exceptions) to police hacking. Therefore, it must be, as far as possible, technically ensured that data concerning the core area of private life are not collected.

Production orders are another possible way of obtaining information about home life. All three countries regulate the obligations of third parties (individuals or organisations) to produce data they hold, if it is of relevance to the criminal investigation. In the Netherlands, a distinction is made between identifying data, which can be ordered by investigation officers, 'ordinary' personal data, which can be ordered by the Public Prosecutor (including data processed in the future), and 'sensitive' personal data, which can be ordered with the authorisation from the investigative judge.

---

[248] BVerfG, Judgment of the First Senate of 20 April 2016 - 1 BvR 966/09, para. 185.
[249] The Dutch provision was only passed into the law in June 2018 and will be in effect only as of 1 March 2019.

In Poland, two regimes for production orders exist, one under the Code of Criminal Procedure for accessing telecommunications data (ordered by a judge or a prosecutor, depending on the stage of the proceedings), and another under the Police Act for data not including content of transmissions (ordered directly by the police, although the use of data is supervised by the Public Prosecutor). Furthermore, under Art. 15(1)(6-7) of the Police Act, the police can request assistance from any government body or entrepreneur in the field of public utility, and in urgent cases from any person, with the lowest threshold of legal safeguards. In Germany, stored data can be obtained on the basis of seizure provisions under Section 94 et seq. StPO. Section 100g(1) StPO allows for long-term collection of traffic data, which has to be ordered by a judge. Service providers are obliged to cooperate in the exercise of this measure.

The regulation of communications investigation is very complex in the jurisdictions we studied; a detailed analysis falls outside the scope of this paper, considering that it is generally less comparable to sewage monitoring than other forms of home surveillance and that it concerns other constitutional safeguards than the protection of home life. Briefly put, unlike the access to meta-data for which different regimes exists depending on type and mode of access, the content of communications is subject to judicial approval in all three jurisdictions.

5.3. Recommendations

Traditional constitutional protection of the home focuses primarily on physical intrusions, but more and more, the walls of the home are ‘evaporating’ and home life becomes visible to government agents equipped by surveillance technologies from the outside. The three jurisdictions we studied (Germany, Poland and the Netherlands) responded to these developments in very different ways.

In the Netherlands, despite the developments described above, the constitutional protection of the home remains a protection from physical intrusions and surveillance from the outside is not considered an interference with the home right. Since covert surveillance measures are generally considered more intrusive than open measures, this means that the constitutional protection of the home may not protect against some intrusions of home life that may be more serious than the traditional forms of physical entering by government agents. However, the fact that the home right does not cover out-of-home monitoring activities does not necessarily mean that the private life of Dutch residents in their home is less protected, since to a certain extent, people are protected from unreasonable monitoring of their activities in other ways, by the general prohibition of in-home visual observation and the very strict safeguards for in-home acoustic surveillance. The Dutch approach to systematic monitoring, using the criterion whether an investigation activity reveals a more or less complete image or certain aspects of someone’s private life, may perhaps be better suited for the 21st century than an approach that protects a certain place from surveillance but that does not clearly distinguish between more and less intrusive forms of such surveillance. However, this criterion is used especially to distinguish minor from non-minor intrusions; it is not used to distinguish, within the category of non-minor intrusions, between substantial and very serious forms of intrusion. In that sense, it falls short as an alternative approach to protecting home life, seeing that intrusions of the home (including outside audio-visual monitoring) are considered highly intrusive measures. Perhaps the main lesson to be drawn from Dutch law is rather that protection of home life does not necessarily have to be sought in *constitutional* protection, but can also be achieved by adequate safeguards in non-constitutional law, such as strict conditions in the Code of Criminal Procedure.

Poland’s constitutional provision still appears to focus solely on physical intrusion, but the doctrine has extended this to cover monitoring from the outside. However, the actual importance of this doctrinal opinion in practice is unclear, since the only legal provisions that seems to follow this line of reasoning is the visual and acoustic monitoring of people in private places. It is rather unclear whether a distinction is made, and if so how, between on the one hand, monitoring of the inside of the home and, on the other, monitoring that does not penetrate the walls but significantly intrudes upon home life by revealing a clear picture of it to the authorities. It is desirable for legal doctrine and practice to pick up on these issues and clarify the scope of what is protected by the inviolability of the home in Poland.

In Germany, the situation is clearer since Art. 13 GG specifically regulates the use of acoustic and other forms of technical surveillance. It is therefore clear that inviolability of the home does

not only protect against physical penetration, but also against surveillance of the home. The text of the provision as well as the judgements of the Constitutional Court seem to indicate that a distinction is made between surveillance that 'looks' inside the dwelling and that infringes the inviolability of the home, and surveillance that stays on the outside, even though it may reveal relevant facts about home life, and which does not infringe the inviolability of the dwelling (although it may, of course, infringe other rights). This distinction, however, is not always easy to make. For instance, does heat imaging 'look' inside the home? The temperature is measured on the outside walls, however it reveals something that is going on inside the walls. In the case of acoustic surveillance it is accepted that it monitors the inside of the dwelling, even though the police may be located outside and the sound leave the home, just as heat does, through the boundary of the home and may be thus be registered outside by technical means. Although the intrusiveness of acoustic surveillance is in most cases higher than the intrusiveness of thermal imaging, this is due to the kind of information that is obtained and not due to the exact location where the registration occurs. Surveillance focused on the outside may often reveal just as much about home life as surveillance penetrating through the walls, and the capabilities of the police to gather information on home life while remaining outside will only increase with technological development.

It may eventually become obsolete to distinguish between surveillance of the inside and surveillance that reveals facts about the inside of the home by monitoring the outside of it, since both types may include tools that are similarly intrusive into home life. Rather, a distinction similar to the Dutch one, between measures that intrude upon home life in a minor way and those that create a more or less complete image of home life could become more useful in distinguishing between measures that do not infringe the inviolability of the home and those that do. Such a criterion might actually be useful to supplement the existing Dutch criterion of systematicness (which, as observed above, does not distinguish within the category of non-minor intrusions), in the sense that if the more or less complete image resulting from government monitoring is an image of aspects of *home* life (rather than of other aspects of private life), this would constitute a kind of "enhanced systematicness" calling for stricter safeguards than for "ordinary" systematicness.[250] The Canadian criterion of protecting a "biographical core of personal information" is also useful to further develop such a regulatory approach.

In criminal procedure, visual and acoustic surveillance of the home is strictly regulated in all three countries. It does not appear necessary to suggest strengthening home protection here, since acoustic surveillance of the home is among the most strictly regulated investigative tools available to the law enforcement, and technical visual surveillance of the home is not permitted at all in German and Dutch criminal procedure. Even though the constitutional protection of the home does not apply to surveillance in the Netherlands, the standard of protection of the home with respect to acoustic and visual surveillance appears to be very high, almost comparable to Germany, which additionally makes the core area of private life inaccessible to investigators. However, the protection of the core area of private life is independent of the inviolability of the home and finds its basis in the protection of human dignity.

Procedurally, the powers of police hacking are also strictly regulated in all countries, in the sense that the procedural requirements placed upon such powers are comparably stringent to the requirements placed on acoustic surveillance, and thus it appears that a high level protection is already offered by existing law. However, the wide range of uses of covert remote access to computers allowed in the Netherlands, and the vague and unspecific way the power is regulated in Poland, could be criticized as giving too much discretionary power to law enforcement. Even in Germany, where the power is regulated more restrictively, some authors have criticized its introduction. Nevertheless, the law-makers had good reasons to introduce police hacking powers, in light of technical developments (such as increased end-to-end encryption and cloud computing), so that police hacking powers are to be welcomed, as long as they have sufficient safeguards in view of their high intrusiveness. In this sense, the German regulation could serve

[250] This approach would fit in well with the advice of the recent Committee on modernising criminal investigation in the digital age, which proposes a threefold criterion of non-systematic intrusions, systematic intrusions, and far-reaching systematic intrusions. See Commissie modernisering opsporingsonderzoek in het digitale tijdperk (2018), *Regulering van opsporingsbevoegdheden in een digitale omgeving*, s.l.: June 2018.

as a model for other countries, since it seems more limited to what is strictly necessary for law enforcement than the broad powers introduced in the Netherlands and Poland. It is also interesting to note here that the protection of computers from remote access is place-independent; rather than connecting computers to the inviolability of the home or communications secrecy, computers seem to be considered a "space" of their own in terms of protection-worthiness. The German establishment of a *sui generis* constitutional right protecting computers is a significant recognition of the role (mobile) computers have in today's world, and could also inspire similar constitutional protection in other countries. For the protection of the home – which also includes computers, even as yet location-fixed computers such as desktops – the protection of computers against remote covert access provides an additional protective layer, where the (logical) boundaries of the computer system seem to take over the role that the "evaporating" walls of the dwelling used to have against monitoring from the outside.

With regard to surveillance measures that do not obtain data in the home, nor focus on visual and acoustic monitoring, there appears to be less legal clarity as to their lawfulness, intrusiveness and possible interference with the inviolability of the home. While acoustic and visual surveillance are generally regulated more specifically, sewage monitoring, heat imaging, garbage searches and olfactory surveillance are not specifically regulated and, with some exceptions, authoritative case law on the applicability of more general provisions to these measures is lacking. This may simply be the result of these measures not being used as much by the investigative authorities or being of lower relevance to them. If that is the case, should their prominence increase in the future, for instance through increased technical capabilities, legal practice may find a clear place for them in the criminal law system through (re-)interpretation of existing law by courts, and even the legislator may provide more specific regulations in case substantially new forms of such monitoring of the home are put in practice. Specific regulations may be welcome, but in many cases unnecessary, if the monitoring of the home does not 'look' inside the home in a similarly intrusive way as audio-visual surveillance is capable of doing. However, if the monitoring – be it through 'looking' inside or through inferring information on what happens inside from data captured outside the home – yields an informative image of home life, the monitoring will constitute a more than minor privacy infringement and will require an explicit legal basis (and hence cannot be based on the general powers of the police) and particular safeguards.

If, however, the lack of legal clarity on the less visible monitoring methods is due not to these measures not being used, but to the fact that they enjoy a certain degree of legal obscurity (and hence are also not being contested by the defence in court, for lack of knowledge or understanding of the implications of these covert measures), more attention needs to be given to clear interpretation and regulation of these surveillance measures. The European Court of Human Rights requires that monitoring of the home is based on clear legal provisions, which contain sufficient mechanisms for control and oversight on their use, and which make it sufficiently foreseeable for the citizens as to its effect and application.

The lack of legal clarity is especially striking in Poland where from the existing provisions, it is not clear what exactly the police is allowed and not allowed to do. Some of the provisions give a clear picture of what is allowed, but some of them are open to broad interpretation, which is problematic considering the potentially high intrusiveness of the measure (such as Article 19(6)(4) Police Act, covert access to computer data). This is exacerbated by the increasingly blurry distinction between operational and procedural activities. Furthermore, while the forms of operational control under Art. 19 subject to stricter safeguards are now more limited by the text of the provisions (compared to the previous technology-neutral provision), other surveillance provisions such as Art. 19b Police Act remain vague and potentially over-inclusive. This creates a risk that the police will only apply the stricter requirements when there is no doubt that some activity is regulated by it, and apply the less rigid regime under the vaguely worded provisions to conduct forms of surveillance of comparable intrusiveness that do not explicitly fall under the stricter regime. This is problematic since it undermines the protection of the home. This problem could be solved by opening the wording of the relevant provisions slightly to allow interpretation including comparable forms of surveillance. Even in the absence of legislative change, the involvement of scholars and academia in shaping and commenting on the legal system should be a lot more prominent. From the available information, it seems that most of the doctrinal debate does not go into the discussion of new technologies and their intersection with the law; doctrinal

accounts related to operational surveillance by the police remain scarce, outdated and lacking depth. This contributes to the existing lack of transparency, legal clarity and certainty in the field. The issues raised in this paper could therefore be usefully taken up in Polish law and practice, to debate and decide where the exact limits should be to broadly formulated police powers that infringe, in various ways and to varying degrees, the inviolability of the home.

Bibliography

Bentham J, *Panopticon Or the Inspection House* (Dublin 1791)

Blom T, 'Titels IVA-VE. Inleidende opmerkingen' in CPM Cleiren, JH Crijns and MJM Vrepalen (eds), *Tekst & Commentaar Strafvordering* (11th edn, Wolters Kluwer 2015)

Buisman SS and Kierkels SBG, 'Artikel 12 – Binnentreden Woning' in E. Hirsch Ballin and G.J. Leenknegt (eds), *De Grondwet. Artikelsgewijs commentaar,* http://www.nederlandrechtsstaat.nl/grondwet.html, last accessed 18 February 2019

Buruma Y, 'Stelselmatig: een sleutelbegrip in de wet bijzondere opsporingsbevoegdheden' (2000) 25 NJCM-bulletin 649

Chmaj M, *Wolności i Prawa Człowieka w Konstytucji Rzeczypospolitej Polskiej* (Seria Akademicka Prawo)

Chynoweth P, 'Legal Research' in A Knight and L Ruddock (eds), *Advanced Research Methods in the Built Environment* (Wiley-Blackwell 2008)

Corstens GJM and Borgers MJ, *Het Nederlands strafprocesrecht* (8th edn, Kluwer 2014)

Cuijpers CMKC and Koops EJ, 'Smart Metering and Privacy in Europe: Lessons from the Dutch Case', in *S. Gutwirth and others (Eds), European data protection: Coming of age* (Springer 2012)

Czuryk M and others, *Prawo Policyjne* (Difin 2014)

Dembowska I, 'Wykorzystanie Materiałów Zgromadzonych Podczas Stosowania Operacyjnej i Procesowej Kontroli Rozmów (Postulaty de Lege Lata)' in Maciej Szostak and Izabela Dembowska (eds), *Innowacyjne metody wykrywania sprawców przestępstw. Materiały z konferencji* (Wroclaw University 2014)

Eschelbach, 'StPO § 100h Weitere Maßnahmen Außerhalb von Wohnraum' in Satzger, Schluckebier and Widmaier (eds), *StPO* (3rd edn, 2018)

Foucault M, *Surveiller et punir: naissance de la prison* (Gallimard 1975)

Garlicki L and Gołyński K, *Polskie Prawo Konstytucyjne: Wykłady* (Liber)

Gercke, '§ 100h', *Heidelberger Kommentar zur StPO* (online)

Grabowska S, Grabowski R and Skrzydło W, *Konstytucja Rzeczypospolitej Polskiej. Komentarz Encyklopedyczny* (Wolters Kluwer 2009)

Hegmann, 'StPO § 100c Akustische Wohnraumüberwachung' in Graf (ed), *BeckOK StPO mit RiStBV und MiStra* (29th edn, 2018)

——, 'StPO § 100h Weitere Maßnahmen Außerhalb von Wohnraum' in Graf (ed), *BeckOK StPO mit RiStBV und MiStra* (29th edn, 2018)

Hutchinson TC, 'Valé Bunny Watson? Law Librarians, Law Libraries, and Legal Research in the Post-Internet Era' (2014) 106 Law Library Journal 579

Jacobs FG, White R and Ovey C, *Jacobs and White, the European Convention on Human Rights.* (3rd ed. /, Oxford University Press 2002)

Jurczak T, 'Inteligentne Liczniki Prądu: Korzyści i Zagrożenia Związane Ze Smart Meteringiem' *Gazeta Prawna* (2014), http://serwisy.gazetaprawna.pl/energetyka/artykuly/771379,inteligentne-liczniki-pradu-korzysci-i-zagrozenia-zwiazane-ze-smart-meteringiem.html, accessed 18 February 2019

Kaczkowski Ł, 'Nienaruszalność Mieszkania' in Mariusz Jabłoński (ed), *Realizacja i ochrona konstytucyjnych wolności i praw jednostki w polskim porządku prawnym* (E-Wydawnictwo 2014)

Kindhäuser U, *Strafprozessrecht* (4th edn, Nomos 2015)

Kluckert and Fink, 'GG Art. 13 [Unverletzlichkeit Der Wohnung]' in Epping and Hillgruber (eds), *BeckOK Grundgesetz* (37th edn, 2018)

Komenda Glowna Policji, 'Ogloszenie o Udzieleniu Zamowienia 2017/S 246-514418'

Koops B-J, 'Criminal Investigation and Privacy in Dutch Law' (Social Science Research Network 2016), https://papers.ssrn.com/abstract=2837483 accessed 18 February 2019

Koops B-J, Conings C and Verbruggen F, *Zoeken in computers naar Nederlands en Belgisch recht: Welke plaats hebben 'digitale plaatsen' in de systematiek van opsporingsbevoegdheden?* (Wolf Legal Publishers (WLP) 2016)

Koops BJ, Van Schooten H and Prinsen M, *Recht naar binnen kijken. Een toekomstverkenning van huisrecht, lichamelijke integriteit en nieuwe opsporingstechnieken* (Sdu 2004)

Kotowski W, *Ustawa o Policji. Komentarz* (Wolters Kluwer 2012)
Maludy M, 'Specjalistyczny Dron Trafia Do Lubuskiej Policji' (*Informacyjny Serwis Policyjny*, 2017) http://isp.policja.pl/isp/aktualnosci/12221,SPECJALISTYCZNY-DRON-TRAFIA-DO-LUBUSKIEJ-POLICJI.html, accessed 18 February 2019
Mevis PAM, 'De bescherming van de woning 25 jaar later' in EJ Hofstee, OJDML Jansen and AMG Smit (eds) *Kringgedachten Opstellen van de Kring Corstens* (Kluwer 2014)
——, 'Algemene Wet op het binnentreden. Inleidende opmerkingen' in CPM Cleiren, JH Crijns and MJM Verpalen (eds), *Tekst & Commentaar Strafvordering*, vol 11 (Wolters KLuwer 2015)
Niemczyk Z, 'Czynności Operacyjno-Rozpoznawcze i Możliwość Wykorzystania Ich Rezultatów w Postępowaniu Karnym' (2013) 3 Kwartalnik Krajowej Szkoły Sądownictwa i Prokuratury
Oerlemans JJ and Koops BJ, 'Surveilleren en opsporen in een internetomgeving' (2012) 38 Justitiële verkenningen 35
Opaliński B, Rogalski M and Szustakiewicz P, *Ustawa o Policji. Komentarz* (CH Beck 2015)
Ośrodek Badań Studiów i Legislacji, 'Stanowisko Ośrodka Badań, Studiów i Legislacji Krajowej Rady Radców Prawnych Dotyczące Poselskiego Projektu Ustawy o Zmianie Ustawy o Policji Oraz Niektórych Innych Ustaw'
Pazdan M, 'Komentarz Do Art. 23' in Krzysztof Pietrzykowski (ed), *Maksymilian Pazdan, 'Komentarz Do Art. 23' in Krzysztof Pietrzykowski (ed), Kodeks cywilny. Tom I. Komentarz do artykułów 1–449* (CH Beck 2011)
Pietraszewski M, 'Śląska Policja Kupuje Drony. Będą Latały Nad Całą Aglomeracją' *Gazeta Wyborcza* (2017), http://katowice.wyborcza.pl/katowice/7,35063,21887904,slaska-policja-kupuje-drony-beda-lataly-nad-cala-aglomeracja.html, accessed 18 February 2019
Plöd, 'StPO § 163f Längerfristige Observation' in Satzger, Schluckebier and Widmaier (eds), *StPO* (3rd edn, 2018)
Pochodyla P and Franc S, 'Kontrola Operacyjna Oraz Zakres Jej Stosowania' (2011) 1 Zeszyty Naukowe WSEI 197
Posytek A, 'Wartość Dowodowa Czynności Operacyjno- Rozpoznawczych' (2011) 23 Prokuratura i Prawo
Safjan M and Bosek L, *Konstytucja RP. Tom I. Komentarz do art. 1–86* (CH Beck 2016)
Schmitt, '§ 100h' in Meyer-Großner, *Beck'sche Kurz-Kommentare Strafprozessordnung*
Sierpowska I, *Socjalne Aspekty Ochrony Prawa Do Mieszkania* (Koło Naukowe Doktryn Politycznych i Prawnych 2010)
Singelnstein T, 'Bildaufnahmen, Orten, Abhören – Entwicklungen Und Streitfragen Beim Einsatz Technischer Mittel Zur Strafverfolgung' [2014] Neue Zeitschrift für Strafrecht 305
Singelnstein T and Derin B, 'Singelnstein/Derin: Das Gesetz Zur Effektiveren Und Praxistauglicheren Ausgestaltung Des Strafverfahrens' [2017] Neue Juristische Wochenschrift 2646
Skorupka J, *Kodeks Postępowania Karnego. Komentarz* (3rd edn, CH Beck 2017)
Škorvánek, I, Koops BJ and Timan T, *Surveillance, Criminal Procedure, and Regulatory Connection: the Case of Sewage Monitoring*, TILT Law & Technology Working Paper Series, version 1.0, April 2019, available at https://ssrn.com/abstract=3377466
Sławicki P, *Prawo Człowieka Do Mieszkania i Jego Miejsce w Systemie Praw Człowieka* (Currenda 2015)
Szumski A, 'Rola Czynności Operacyjno-Rozpoznawczych w Uzyskiwaniu Dowodów w Procesie Karnym' in Leszek Bogunia (ed), *Nowa Kodyfikacja Prawa Karnego. Tom XXVI* (Wydawnictwo Uniwersytetu Wrocławskiego 2010)
Tak AQC, *Het huisrecht* (diss. Utrecht) (Hoenderloo's Uitgeverij en Drukkerij 1973)
Van der Sloot B, 'How to Assess Privacy Violations in the Age of Big Data? Analysing the Three Different Tests Developed by the ECtHR and Adding for a Fourth One' (2015) 24 Information & Communications Technology Law 74
——, 'Is the Human Rights Framework Still Fit for the Big Data Era? A Discussion of the ECtHR's Case Law on Privacy Violations Arising from Surveillance Activities' in S. Gutwirth, R. Leenes and P. De

Hert (eds), *Data protection on the move: current developments in ICT and privacy/data protection* (Springer 2016)

——, 'Privacy as Personality Right: Why the ECtHR's Focus on Ulterior Interests Might Prove Indispensable in the Age of "Big Data"' (2015) 31 Utrecht Journal of International and European Law 25

——, 'Where Is the Harm in a Privacy Violation? Calculating the Damages Afforded in Privacy Cases by the European Court of Human Rights' (2017) 8 JIPITEC 322

Vuagnoux M and Pasini S, 'Compromising Electromagnetic Emanations of Wired and Wireless Keyboards', *Proceedings of the 18th Conference on USENIX Security Symposium* (USENIX Association 2009), http://dl.acm.org/citation.cfm?id=1855768.1855769, accessed 18 February 2019

Walsh CE, 'Surveillance Technology and the Loss of Something a Lot Like Privacy: An Examination of the Mosaic Theory and the Limits of the Fourth Amendment Criminal Law Issue: Features Contributors' (2011) 24 St. Thomas Law Review 169

Weßlau, '§ 152', *Systematischer Kommentar zur Strafprozessordung* (online)

Wiemans FPE, 'Artikel 125j' in Melai/Groenhuijsen (ed), *Het Wetboek van Strafvordering* (Kluwer (Online) 2006)

Wohlers, '(Vor)§ 94', *Systematischer Kommentar zur Strafprozessordung* (online)

Zöllner, '§ 163f', *Heidelberger Kommentar zur StPO* (online)

Zöller MA and Ihwas RSR, 'Rechtliche Rahmenbedingungen des polizeilichen Flugdrohneneinsatzes' [2014] Neue Zeitschrift für Verwaltungsrecht 408