Protection of a suspect’s privacy in criminal procedures

Does the conceptual approach of the German Federal Constitutional Court make a difference?

Michael Lindemann & Dave van Toor*

With the discussion on the new Dutch Code of Criminal Procedure and the introduction of new (technological) investigative methods (such as hacking), the question arises whether the protection of the suspect’s privacy in Dutch criminal procedure – which is somewhere between minimalistic and non-existent at the moment – needs to be revised. To this end, a comparison with German Constitutional Law and Criminal Procedural Law will be made. The focus will be on the German concept of ‘Kernbereich privater Lebensgestaltung’, which can be translated as the protection of the core aspect of a private life.

1 Introduction

The protection of a suspect’s privacy in Dutch criminal investigations is minimal. Firstly, the authorities do not need a specific and precise statutory provision for minor interferences with the right to respect for privacy. According to the Dutch Supreme Court, the authorities can use the general provision of article 3 Politiewet (law on the organization of the police) for all investigative methods that cause minor interferences with the right to respect of privacy.1 This also includes investigative measures without a reasonable suspicion, such as making photos in a public area.2 Because no specific provisions for numerous investigative methods are available, the possible interferences with privacy are not foreseeable. Secondly, the European Convention of Human Rights (hereinafter: the Convention or the ECHR) and the Dutch Constitution (hereinafter: Gw) do not acknowledge an absolute protection of a core or a part of the privacy of a person. In theory, every interference with Article 8 of the Convention and the Articles 10-13 Gw can be justified.3 Only interferences that also violate the prohibition of torture (Article 3 of the Convention) are forbidden in an absolute sense. This means that the right to respect for privacy (under Article 8 ECHR) only protects a suspect’s privacy in a relative, procedural way: namely that the interference should be in accordance with the law; that the interference is designed to pursue a legitimate aim; and that the interference is necessary in a democratic society. The first criterion requires Member States to provide for a published law that is accessible and the application of which is (in some way) foreseeable to justify the interference. The second criterion proposes no real challenge for Member States: Harris, O’Boyle and Warbrick state that Member States have been able to convince the European Court of Human Rights (ECHR) that they were acting for a proper purpose in almost all cases.4 The third criterion is a ‘fair balance’ assessment, centralized on the proportionality between the right protected and the pursued aim.5 All in all, the authorities do not need a specific and precise statutory provision for minor interferences with the right to respect for privacy.

1 HR 1 July 2014, ECLI:NL:HR:2014:1563, par. 2.4.
5 Harris, O’Boyle, Bates & Buckley 2014, p. 519.
8 D.A.G. van Toor, case note: ECHR, 31 October 2017, 22767/08 (Dragoš Ioan
The protection of a suspect's privacy in Dutch criminal investigations is minimal

This leads to the following situation under Dutch Criminal Procedural Law: (i) minor interferences with a suspect's privacy can be based on a general law that allows the police to do everything that potentially contributes to an effective enforcement of the law; (ii) other than minor interferences can be justified with a specific basis in the law, as Article 8 of the Convention does not constitute an area of absolute protection; and (iii) violations of privacy rights – (i) interferences that ex post do constitute minor interferences in violation of Article 3 Politiwet and (ii) other than major interferences whereby the Justice Department and the police acted in violation of the specific law – seldom lead to exclusion of evidence. With the discussion on the new Dutch Code of Criminal Procedure and the introduction of new (technological) investigative methods (such as hacking), the question arises whether the protection of the suspect's privacy in Dutch criminal procedure – which is somewhere between minimalistic and non-existent at the moment – needs to be revised. To this end, a comparison with German Constitutional Law and Criminal Procedural Law will be made. The focus will be on the German concept of ‘Kernbereich privater Lebensgestaltung’, which can be translated as the protection of the core aspect of a private life. In the second section, we will discuss this concept, and explain the extent to which it provides for an absolute protection of the core of a private life. In the third section, some examples will be given to explain differences of protection of a suspect’s privacy in Germany and the Netherlands. The fourth section will conclude this article with an assessment if the concept of the protection of the core aspect of a private life should be introduced in Dutch Criminal Procedural Law.

2 The concept of Kernbereich privater Lebensgestaltung

German Constitutional Law – as it is interpreted by the German Federal Constitutional Court – offers a more conceptual approach to privacy protection than the European Convention of Human Rights. Firstly, the German Federal Constitutional Court defines three spheres of privacy (as will be explained below), whereas the ECtHR, in its well-established case-law, ‘does not consider it possible or necessary to attempt an exhaustive definition of the notion of “private life”’. Secondly, as already stated in the introduction, the protection of privacy under Article 8 of the Convention can be seen as a procedural protection: the court does not forbid any privacy interfering (criminal) method in an absolute sense, but only accepts a violation of the Convention when the Member States did not apply the justification criteria of Article 8 (2) of the Convention correctly. In contrast, the German approach to interferences with privacy is based on the so-called ‘Sphärentheorie’, and is of a conceptual nature. This theory distinguishes between three privacy spheres – the intimate sphere, the private sphere and the social sphere – each with a different protection regime. The ‘three-spheres-theory’ will be explained in this section. The description of this theory will make it possible to review if it offers a broader or better protection of the suspect’s privacy in criminal investigations than the Dutch regime, and to subsequently discuss if the new Dutch Code of Criminal Procedure should acknowledge the same or similar privacy protection.

The German approach to interferences with privacy is based on the so-called ‘Sphärentheorie’, and is of a conceptual nature

2.1 The three-spheres-theory

The main idea of the three-spheres-theory is that the areas that are more private and/or intimate require a more thorough protection against interference from the State or even an absolute protection against intrusion by the State. In the case law of the German Federal
Constitutional Court, the foundations of the theory are mainly derived from the general right to respect for privacy (allgemeines Persönlichkeitsrecht, Articles 2 (1) and 1 (1) German Basic Law, hereinafter: GG), but there are also references to the guarantee of the intrinsic nature of basic rights (Art. 19 (2) GG). Additionally, the close association of the inviolability of the home (Art. 13 GG) with the constitutional requirement of unconditional respect for the individual’s exclusively private sphere of – “strictly personal” – development has been stressed as well. 12

The first area, the so-called social sphere, consists of the social life as part of the public domain. This part of a person’s life is accessible for all other persons: the individual, as a community-bound person, interacts with other members of society as part of the public life. Because this part of life is assigned to the public domain, it is the least protected sphere. For example, Beulke states that this area of life ‘is not protected in any distinct way’. 13 This can be easily compared with the case-law of the ECtHR and the Dutch Supreme Court. The ECtHR uses the ‘reasonable expectation of privacy test’ in (some) of his case-law to assess if a person can have an expectation of privacy. 14 Usually, one cannot have an expectation of privacy in the public domain because one is visible and accessible for all other persons in the public domain. The Dutch Supreme Court also includes the location of the interference as one of the criteria to assess the nature and intensity of the interference in a person’s privacy. 15 In his dissertation, Van Toor has analyzed the case-law of the Dutch Supreme Court on the justification of privacy interferences in Dutch law and concluded that interferences with a person’s privacy in the public domain do not require any specific prerequisites other than those stipulated by the general provision of Article 3 Politiewet. 16 Thus, the protection of the social sphere in Germany, the Netherlands and under the ECHR is more or less equal.

The second area, the so-called private sphere, occupies an intermediate position between total seclusion and social interaction: it essentially covers the domestic sphere and the areas of life that are hidden from the public and that is only accessible to a selected group of persons. 17 However, this area is not restricted to social contact with those persons in secluded areas, but also consists of private conversations in public areas. So, it is the nature of the conversation that determines if a meeting is part of the social sphere or private sphere. A justification of interferences with a person’s privacy in the private sphere is only possible if the principle of proportionality is observed and the individual interest in the observance of secrecy is outweighed by public interests. 18 The leading principle to judge if interferences in the private sphere can be justified is thus the principle of proportionality (Verhältnismäßigkeitsprinzip). 19 This criterion is also focal in the ECtHR’s case-law. 20

The so-called intimate sphere (or Kernbereich privater Lebensgestaltung) is absolutely protected from interferences

The third area, the so-called intimate sphere (or Kernbereich privater Lebensgestaltung), 21 is absolutely protected from interferences. The intimate sphere includes inter alia sexuality, feelings and thoughts and similar personal non-public matters as well as personal health (care). This is the part of life where a person can have perfect seclusion. 22 In the case-law of the German Federal Constitutional Court, the essential features of the intimate sphere and its distinction from the private sphere are elaborated as follows:

The Federal Constitutional Court recognizes … a last and inviolable sphere of private life that is beyond the interference of government authority: Even severe public interests cannot justify an intrusion into this sphere; a balancing of interests on the basis of the principle of proportionality is prohibited. On the one hand, this ensues from the guarantee of the intrinsic nature of basic rights (Article 19 (2) GG), and on the other hand it can be traced back to the fact that the core of the personality is protected by the inviolable dignity of man. Yet the contact with the personal sphere of another party bestows a certain importance upon an act or information and makes it a possible subject of legal regulation. Nevertheless, communication with other people can be beyond the interference of government authority per se. As a person, the human being – even in the core of his personality – necessarily exists in a social context. The assignment of a situation to the inviolable intimate sphere or to the private sphere which will be accessible to state authorities under certain circumstances is not dependent upon whether a social meaning or relationship exists at all but upon its nature and intensity. This cannot be assessed in an abstract manner but has to be established while taking into consideration the specific features of the case at hand. 23

2.2 The (not so) inviolable intimate sphere

It is obvious that the protection regime sketched above is of particular importance in criminal procedures, since interferences with the personal sphere of the suspect and third parties are quite common in the course of a criminal investigation. In a decision from 1989, the German Federal Constitutional Court’s Second Senate had to assess if the
Gavison calls the complete seclusion ‘perfect privacy’ (where privacy is to be understood as a right to secrecy, and not a right to personality). Also Van Tour 2017, p. 221-226.

23 BVerfGE 80, 367 par. 15-16, our translation.

24 BVerfGE 80, 367 – Tagesbuchentscheidung.

25 BVerfGE 80, 367 (374f.).

The decision was based on a proportion of votes of 4:4. According to Section 13 (3) 3 Act of the Federal Constitutional Court (old version), this means that there was no violation of the Constitution or other domestic laws.

26 BVerfGE 80, 367 (375f.).

In contrast, the defeated minority of the Senate stressed the highly personal nature of the notes; see BVerfGE 80, 367 (380ff.) and – approvingly – J. Wolter, Repressive und präventive Verwahrung tagesbuchartiger Aufzeichnungen. Zugleich Besprechung der Tagebuchentscheidung des BVerfG, Strafaufsichtsbericht 1990, p. 177.

27 BVerfGE 109, 279 (319) – Großer Lauschangriff, see also BVerfGE 113, 348 (391) – Interception of Telecommunications (old version), this means that no violation of the Constitution or other domestic laws.


30 In BGHSt 50, 206, the soliloquy had taken place in a (single) hospital room of a rehabilitation clinic; in BGHSt 77, it had taken place in a car with the suspect as the only passenger.

use of diary-like notes were to be accepted as proof in a murder trial, and if the interference with the suspect’s privacy was compatible with Article 2 (1) and Article 1 (1) GG. The suspect, who was accused of having murdered a woman, had reflected upon emotional stress and his problems with women in notes that he had kept on his private premises.24 The Senate concluded that the Constitution does not strictly forbid the use of diaries and similar private notes as evidence in criminal proceedings, and that such texts are not to be assigned to the inviolable intimate sphere if they contain information about planned crimes or crimes that have already been committed.25 The admissibility of this sort of information in a criminal procedure should be assessed on the basis of the principle of proportionality – because it falls under the private sphere – which in this case, where the information was closely related to the crime and a murder charge was at hand, justified an affirmative decision.30

In a decision of 2004 that concerned the acoustic surveillance of private premises, the First Senate of the German Federal Constitutional Court has specified the aforementioned principles as follows:

The content of communication that contains information on criminal offences that have been committed does not fall into the inviolable core area of private conduct of life (see BVerfGE 80, 367 [375]). It does not, however, follow from this that just any given link between the suspicion of commission of a criminal offence and the statements of a suspect suffices to confirm the existence of a concern of society. Recordings or statements made in the context of a conversation between two individuals that, for example, convey exclusively personal impressions and feelings and contain no indications of any concrete criminal offence do not take on the nature of a public concern simply because they may reveal the origins or motives for criminal conduct. A concern of society can on the other hand be assumed to exist with sufficient certainty in the case of statements that relate directly to a concrete criminal offence.31

There is reason to believe that – based on these assumptions – the First Senate would have denied the admissibility of the diary-like notes in the case from 1989 since they were not directly related to the crime that was subject to the trial.29 Nevertheless, the revised concept sketched by the Senate still evokes criticism because it opens an opportunity for prosecutorial authorities to make use of private documents and conversations particularly in those cases where their interest is greatest – the consequence being an automatism of admissibility for crime related statements and a considerable weakening of the suspect’s fundamental rights position.29

Remarkably (and to some extent in contradiction with the case law of the German Federal Constitutional Court), the German Federal Court of Justice has declared secret recordings of soliloquies inadmissible even though the content was directly related to specific crimes.30 The German Federal Court of Justice argued that soliloquies are a priori not meant to be overheard by other people and that the speaker – other than the author of a diary – does not put down his thoughts and thus does not release them from his inner sphere of influence.31

This case-law – where the nature of the information can ‘transfer’ the information from the intimate sphere to the social sphere – weakens the inviolability of the core protection of private life.

All in all, this case-law – where the nature of the information can ‘transfer’ the information from the intimate sphere to the social sphere – weakens the inviolability of the core protection of private life. Conversations with trustees on private premises are normally considered to be inviolable, but not when the content of the conversation is about committed or planned offences. That information has, due to the nature of the information, relevance for society (Sozialbezüge). From the view of the authors it would be preferable to abstain from such intricate distinctions and to generally declare intimate statements inadmissible – regardless of whether they were written down, expressed in a soliloquy or the subject of a conversation, and regardless of whether and to which extent they were related to a crime already committed.32

Finally, it has to be noted that the case-law of the German Federal Constitutional Court has established an obligation for the legislator to create a legal framework which effectively safeguards the intimate sphere against interferences of the prosecutorial authorities. To this end, on a first level precautions have to be taken against the unintended gathering of information which belongs to the ‘Kernbereich privater Lebensgestaltung’. On a second level, the consequences of an unintended gathering of such information have to be minimized, especially by implementing an obligation to delete them immediately regardless of the investigative method or legal provision.33
The legal provisions which were established pursuant to this case-law will be discussed in detail in the next section.

There are no absolute boundaries on privacy interferences in the case-law of the ECtHR and the Dutch Supreme Court under the right to respect for privacy.

3 (New) technologies and privacy protection

As explained in the last section, the German Federal Constitutional Court offers a conceptual approach to privacy protection, whereas the protection of the right to respect for privacy in the ECtHR’s case-law and the Dutch Supreme Court’s case-law can be considered a formal approach. There are no absolute boundaries on privacy interferences in the case-law of the last two mentioned courts under the right to respect for privacy. Instead, those courts only assess the quality of the laws that allow for interferences with a person’s right to respect for privacy and the balance between the government’s aim and the protected human right. It could be possible that the conceptual approach of the German Federal Constitutional Court leads to differences in the actual and practical protection of person’s privacy, especially in the so-called ‘core of private life’ (Kernbereich privater Lebensgestaltung). The protection of that part is absolute (at least in theory, as explained above in subsection 2.2).

In the next subsections, the privacy protection in German and Dutch criminal investigations in three methods will be compared. We selected the methods of Sections 100a, 100b and 100c of the German Code of Criminal Procedure (hereinafter: StPO, Strafprozessordnung), id est respectively interception of telecommunication, online search and seizure, and eavesdropping in a home. The government stated that the introduction of these specific investigative methods would lead to a more effective and practical criminal procedure. The introduction of these methods is necessary because of the role that small electronic devices play in daily life, also for criminals. These methods are selected because Sections 100a-c StPO are complemented by Section 100d StPO, which regulates the protection of the core of private life for these methods exclusively. It is noteworthy that Section 100d StPO was intended to codify the principles set out in the aforementioned case-law of the German Federal Constitutional Court. In the next three subsections a description will be given on the legal requirements to use the aforementioned investigative methods, which were revised (and partly introduced for the first time) in German criminal procedure mid-2017. In subsection d the privacy protection of all three methods will be discussed. Finally, in subsection e, some differences with the Dutch regulations on these topics will be discussed.

a) Interception of telecommunication

Section 100a StPO allows the German authorities to intercept and record telecommunication, which includes the use of messenger services, SMS and video and phone calls, without the knowledge of the persons concerned. Till 2017, telecommunication was usually intercepted via the telecommunication provider’s network. The new Section 100a StPO adds interception at the source, mainly because it is often the only way to circumvent encryption (the idea is to get to the information before it is encrypted). According to Section 100a (1) 2 StPO, which was introduced in 2017, this includes the infiltration of an information technology system if that step is necessary to overcome the encryption of communication contents (the so-called Quellen-TKÜ, designated to solve the problems of encrypted IP-telephoney). Section 100g StPO complements this with the seizure of traffic data.

The difference between Section 100a StPO on the one hand and Section 100b StPO (which will be discussed below) on the other hand, is that with the first method only communication content can be intercepted during and after its transmission (for the latter see Section 100a (1) 3 StPO), while with the second method every other kind of data stored on a digital device can be gathered. E-mails that are stored elsewhere fall under a different regime. According to the case-law of the German Federal Constitutional Court, e-mails that are stored by the service provider may be seized under the less restrictive requirements stipulated in Sections 94 and further StPO (the ‘normal’ provision allowing the authorities to seize goods).

For a lawful interception, Section 100a (1) 1 StPO requires (i) a concrete suspicion of a severe offence against a person, and that offence has to be explicitly mentioned in Paragraph 2; (ii) that the offence is one of particular gravity.
in the individual case as well;\textsuperscript{40} and (iii) compliance with the principle of subsidiarity, which means that the gathering of evidence through other methods is considered particularly difficult or hopeless. The principle of subsidiarity is complemented by case-law with the principle of proportionality. According to Section 100a (3) StPO, the order may be directed only against the suspect and/or the so-called Nachrichtenmittler. A Nachrichten­mittler is a person who, on the basis of certain facts, is suspected to be a message ‘mule’ for the suspect, or whose system and/or network is used by the suspect. In principle, the public prosecutor must acquire the permission of the court to use the method of Section 100a StPO (Section 100e (1) 1 StPO). Only in exigent circumstances, the public prosecutor may also issue an order that will become ineffective if the court does not confirm it within three working days (Section 100e (1) 2, 3 StPO). Paragraph 5 includes extensive technological requirements for the Quellen-TKÜ to ensure the authenticity of the telecommunication, and to ensure the least far-reaching interference.

According to the telephone tapping report of the German Federal Ministry of Justice, the German authorities tapped telephones in 5,738 cases with 17,510 taps in 2016, 5,945 cases with 18,640 taps in 2015, and 5,625 with 19,795 taps cases in 2014.\textsuperscript{41} In the Netherlands – where the legal regulation of the interception of telecommunications does not differentiate greatly – the prosecutorial authorities targeted 24,850 numbers in 2016, 24,063 numbers in 2015, and 25,181 numbers in 2014.\textsuperscript{42} As will be explained below, the German provisions offer a better protection for targeting third parties (non-suspects), for example family members and friends of the suspects. It is a possibility that this can explain the differences in taps between the Netherlands and Germany, but the German and Dutch wiretap reports do not offer insights on why the number of taps between the two countries differs largely.

\textbf{b Online search and seizure}

An online search and seizure is, according to the German government, ‘the covert access to foreign [in the sense of ‘strange’, ‘unfamiliar’, ML & DvT] information technology systems via communication networks by means of monitoring software’.\textsuperscript{43} This software will make it possible to monitor the use of the system and to seize data.\textsuperscript{44} The online search and seizure method was also introduced in 2017 (with an urgent procedure at the end of the Merkel III coalition), as a response to the German Federal Constitutional Court’s case-law on the right to informational self-determination.\textsuperscript{45} An introduction of a specific law was necessary because the interference in one’s privacy is extensive with an online search and seizure.\textsuperscript{46} According to the German Federal Constitutional Court, an online search and seizure can only be justified if very strict formal and substantive prerequisites are met.\textsuperscript{47} Although the legislator has tried to comply with the strict requirements established by the German Federal Constitutional Court and reduced the scope of application in comparison to Section 100a StPO,\textsuperscript{48} it seems doubtful that the attempt to create a regulation in accordance with the constitution was successful.\textsuperscript{49}

Section 100b StPO allows the prosecutorial authorities to access stored information. So for example, it is not allowed to use the system’s camera and microphone on the basis of this provision, only to passively register stored information. For a lawful seizure, Section 100b (1) 1 StPO requires (i) a concrete suspicion of a very severe offence\textsuperscript{50} against a person, and that offence has to be explicitly mentioned in Paragraph 2; (ii) that the offence is one of particular gravity in the individual case as well; and (iii) compliance with the principle of subsidiarity, which means that the gathering of evidence through other methods is considered particularly difficult or hopeless. Thus, only the first criterion of Section 100b (1) StPO is different in comparison with Section 100a (1) StPO, and reduces the application scope in a minimal sense – from severe offences to very severe offences. \textit{Mutatis mutandis} Section 100a (2) StPO, Section 100b StPO includes an exhaustive list of ‘very severe offences’. As mentioned
before, the online search and seizure is a more comprehensive interference with one’s privacy and therefore the application should be more limited than other investigative methods.

According to Section 100b (3) StPO, the order may be directed only against the suspect, or against another person when the suspect is using that person’s system. This – the third party ‘object’ – is the second difference between the interception of telecommunication and the online search and seizure. Thus, the interception of telecommunication has another third party object application than the online search and seizure. Finally, the limitations mentioned in Section 100a (5) StPO also apply to the online search and seizure (Section 100b (4) StPO).

c Eavesdropping methods

Section 100c StPO provides a legal basis for the interception and recording of private speech on private premises without the knowledge of the person concerned, whereas Section 100f StPO must be used to eavesdrop on conversations outside homes. As in the ECtHR’s case-law, the concept ‘home’ has a broader connotation and covers also certain professional or business premises. All criteria of Section 100c StPO can be found in Sections 100a and 100b StPO as well, id est the criteria for eavesdropping in homes are almost completely a combination of some of the criteria of the interception of telecommunication and of the online search and seizure. For a lawful interception, Section 100c (1) 1 StPO requires (i) a concrete suspicion of a very severe offence against a person, and that offence has to be explicitly mentioned in paragraph 2; (ii) that the offence is one of particular gravity in the individual case as well; and (iii) compliance with the principle of subsidiarity, which means that the gathering of evidence through other methods is considered particularly difficult or hopeless. In addition, Section 100c (1) 3 StPO requires that it is reasonably foreseeable, on the basis of actual facts, that the method will lead to the gathering of statements made by the suspect about an offence or the location of a co-conspirator.

**d The protection of the core of private life according to Section 100d StPO**

The above-mentioned methods are interesting from a human rights perspective, because they are combined with a provision especially designed to protect the core of private life during the application of those methods. This is remarkable, because usually the protection of human rights is based on the respective articles of the constitution or treaties. In addition to the ‘normal’ human rights approach, Section 100d StPO entails several elaborations on how the protection of the core of private life should be achieved during the application of the measures of Sections 100a through 100c StPO.

The above-mentioned methods are interesting from a human rights perspective, because they are combined with a provision especially designed to protect the core of private life during the application of those methods.

Paragraph 1 of Section 100d StPO contains a prohibition to use the methods of interception of telecommunication, online search and seizure and eavesdropping in homes when it is to be expected that only information that is part of the core of private life would be gathered. The authorities must prognosticate if this is the case before applying the methods. But, as has repeatedly been criticized in the literature, it is highly unlikely that nothing outside of the core protection will be gathered. Even more, the German Federal Court of Justice appears to be wholehearted with accepting a prognosis that the information will not be protected under the Kernbereich; for example, in a murder case, the communication between the suspect and his wife was intercepted – communication that normally falls under the inviolable core of private life, but apparently the authorities prognosticated that the suspect would also talk about non-core information – but the judgment of the German Federal Court of Justice does not offer any relevant facts for an ex ante prognosis that the suspect will talk about (a) criminal offence(s). The German Federal Court of Justice (ex post and with hindsight bias) accepted the interception and the prognosis that not only communication that is part of the...
Kernbereich will be intercepted nonetheless, because it is foreseeable for the authorities that a suspect will talk about the possibility to obstruct justice.55 Thus, it is very unlikely in theory and practice to imagine a situation where all the gathered information would be part of the Kernbereich.

More important for the actual protection of the core of private life, Section 100d (2) StPO establishes an obligation to delete all information about the core of private life that has been gathered (sentence 2) and a prohibition to evaluate this information in criminal cases (sentence 1).56 Section 100d (3) StPO complements this with an obligation to do all that is technically possible to not seize data about the core of private life during an online search and seizure. For example, the authorities should try to distinguish between photos and videos that are part of the criminal offence and photos and videos that are part of the non-criminal core of private life.57 Section 100d (4) StPO imposes several limitations on the use of eavesdropping technologies in homes. For example, the method may only be used when information about the core of private life will not be gathered (sentence 1), and the eavesdropping has to be interrupted immediately when information about the core of private life is being gathered (sentence 2). When it is doubtful that the method continually will lead to the gathering of statements made by the suspect about an offence or the location of a co-conspirator, then the public prosecutor needs a court’s permission to continue the eavesdropping.

The main differences between the Dutch and German laws on the methods discussed regard the ‘object’ of these measures.

Comparison with the Dutch special investigative measures (‘bijzondere opsporingsmethoden’)

The comparable provisions in Dutch criminal procedural law on the interception of telecommunications, the online search and seizure and eavesdropping in homes are respectively based in Articles 126l, 126nba58 and 126m and further Dutch Code of Criminal Procedure (hereinafter Sv).59 The Dutch and German laws on those topics are largely the same regarding the application criteria, in the sense that they both are limited to (very) severe offences, limited in time, subject to judicial permission and subject to a subsidiary and proportionality assessment.

The main differences between the Dutch and German laws on the methods discussed in this paragraph regard the ‘object’ of these measures. The German measures can be used against a suspect and his home and devices, or places and systems if it is reasonably foreseeable that he uses them for communication purposes. The only exception is the interception of telecommunication, which can also target a communication ‘mule’. German law only allows the authorities to target third parties, such as family members, colleagues and friends, when the suspect uses the system or home of that person. Therefore, there is always a direct link between the targeting of a third person and the suspect.

This is not the case in Dutch law. For example, Articles 126l Sv and 126m Sv (resp. interception of telecommunication and eavesdropping), but not Article 126nba Sv,60 allow the authorities to target any person (see paragraphs 3c and 2c resp.) when it is strictly necessary (dringend onderzoeksbelang). If the suspect is still a nomen nescio, but family members are known, Dutch law allows the authorities to target the family members to get information about the suspect. For example, targeting people close to the suspect can lead to information about his whereabouts or about the offence. It is even theoretically possible that the gathering of evidence is completely based on third parties, for example friends and family members who carelessly use electronic devices and phones, without ever targeting the suspect with an investigative method directly or any evidence that the suspect will use the devices of third persons or contact those persons.

A second distinction is based on the core of private life protection (Section 100d of the StPO) that complements the measures of Sections 100a through 100c StPO. The aforementioned articles in the Dutch Code of Criminal Procedure have no provisions regarding the nature of the information that is gathered. In contrast, the German Code of Criminal Procedure obliges the authorities to try to limit the seizure to information that is not part of the core of private life when they use an online search and seizure, or that the transmission of the microphone has to be interrupted when information that is part of the core of private life is heard. The Dutch Code of Criminal Procedure evidently regards all information as equal, and does not offer different
protection regimes for relevant information for the crime and non-criminal information; there is no limitation in the law regarding the seizure of specific categories of information or intercepting of specific communication.

The three-spheres-theory (or another more conceptual approach) could improve privacy protection in Dutch criminal procedures, especially regarding third persons and non-criminal information.

4 Conclusion
Although the conceptual approach on the protection of a person’s (including a suspect’s) privacy of the German Federal Constitutional Court is completely different from the formal approach of the Dutch Supreme Court and the ECtHR, there appears to be little difference in the actual protection of the suspect’s privacy. The German Federal Constitutional Court defines the concept of privacy, and offers a gradually increasing protection of three distinct privacy spheres, but allows interferences even in the intimate sphere when the information is related to a criminal offence. That information has, due to the nature of the information, relevance for society (Sozialbezug), and is therefore ‘transferred’ from the intimate sphere to the social sphere. Furthermore, the German Federal Court of Justice appears to be wholehearted in accepting a negative decision on the Kernbereich prognosis, id est accepting that not all the gathered information is part of the core protection of private life. This means that the idea of an absolute inviolable sphere of private life of suspects becomes theoretical, maybe even illusory.

However, this does not mean that there are no differences in the privacy protection between German and Dutch criminal procedures. The main practical differences are, as mentioned in the last subsection, that the German Code of Criminal Procedure (i) offers a better protection of the privacy of third persons and (ii) offers different regimes for different natures of the information. That last part could be used to improve the differentiation in data seizures, when the suspect stored non-criminal private data and, for example, child pornography on the same device. Thus, the three-spheres-theory (or another more conceptual approach) could improve privacy protection in Dutch criminal procedures, especially regarding third persons and non-criminal information.

61 See also fn. 57.