TILT LAW & TECHNOLOGY
WORKING PAPER SERIES

Privacy Protection in German Criminal Procedure

Draft Version 0.7 (Please do not quote without authors' permission)

Cihan Parlar, Vrije Universiteit Brussel

cihankparlar@gmail.com

Ivan Škorvánek, Tilburg University, TILT

i.skorvanek@uvt.nl

February 2017

Contents

1. Introduction

The law of criminal procedure serves two main functions: it provides the public authorities the legal basis to intrude upon individual rights for the purposes of investigating and prosecuting criminal activity, and at the same time limits the power of these authorities by establishing clear boundaries of such power. From the perspective of privacy, it is therefore highly interesting to examine, where the law of criminal procedure, especially in the investigation stages, establishes the boundaries of police action interfering with the right to privacy. In this report, with an aim of gaining a better understanding of privacy, different types of privacy and how their protection is conceptualized by the legislators (and judiciary) in Germany will be described. The focus will especially lie on the protection of home and things inside private home, the body and mind of persons, personal communications, things and personal data. Special focus is given to those areas where recent technological advances challenge the traditional protections and provide the law enforcement authorities with a more focused lens into the private life of individuals. As a full and comprehensive description of all privacy related aspects of the criminal procedure would be enormous in scope, certain areas will only be briefly sketched and the report is rather selective in the array of topics that are given more focus.

2. Privacy and the contours of criminal procedure

2.1 A brief overview of criminal procedure

Norms are legal rules, determining whether the respective behavior is lawful or unlawful. Norms in the criminal law field thus provide a framework for citizens restricting the scope of allowed actions. They serve as a guardian of legally protected interests related to a free self-development of a person in society.[1] Criminal law prohibits any behavior which would endanger or harm these legally protected interests.

To evaluate whether a violation of criminal law has accrued, an investigation has to be carried out. The German Criminal Procedural Law serves two functions. It constitutes the legal basis for measure 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.[2]

The criminal procedural law's fundament is the German Constitution[3]. Specific provisions regulating the criminal procedure are based on the German Criminal

[1] Urs Kindhäuser, Strafprozessrecht, 4. Auflage, 2016, § 1, Rn 1.
[2] Urs Kindhäuser, Strafprozessrecht, 4. Auflage, 2016, § 1, Rn 7.
[3] So called Grundgesetz (GG). English version: https://www.bundestag.de/blob/284870/ce0d03414872b427e57fccb703634dcd/basic_law-data.pdf (last checked 17.05.16) and German version http://www.gesetze-im-internet.de/bundesrecht/gg/gesamt.pdf (last checked 17.05.16).

Procedure Code[4] (CPC) and Courts Constitution Act[5] (CCA). These provisions are supplemented by administrative law. The CPC and CCA were introduced together with the Code of Civil Procedure[6] (CCP), and were designed as complementary parts of a total procedural regime.[7]

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.

The criminal procedure can be roughly divided into recognition proceeding ("Erkenntnisverfahren") and enforcement proceeding ("Vollstreckungsverfahren").[8] During the "Erkenntnisverfahren" the prosecution office investigates whether the conditions for an imposition of sanctions are given and in what form these sanctions should be imposed.[9] The procedure itself can be separated in investigation proceedings ("Ermittlungsverfahren"), interlocutory proceedings ("Zwischenverfahren") and the main proceedings ("Hauptverfahren").[10] The "Vollstreckungsverfahren" deals with the actual enforcement of the imposed sanctions.[11] The cesura between "Erkenntnisverfahren" and "Vollstreckungsverfahren" is constituted by the verdict's obtainment of legal force.

2.2 Constitutional Law, Criminal Procedure, and Privacy

In Germany, the Constitution uses neither the term privacy nor private life and these terms are also not used in legal practice where the term Privatsphäre is employed to describe a combination of constitutional rights[12]. These include the general personality right in the form of a person's "right to free development of his personality"[13] upon which, in combination with the protection of human dignity, the Court has built to introduce a set of privacy rights including the right to informational self-determination, the right to absolute protection of the core area of the private life, and the right to the confidentiality and integrity of

[4] So called Strafprozeßordnung (StPO). English version: https://www.gesetze-im-internet.de/englisch_stpo/ (last checked 17.05.16) and German version: https://www.gesetze-im-internet.de/stpo/BJNR006290950.html (last checked 17.05.16).
[5] So called Gerichtsverfassungsgesetz (GVG). English version https://www.gesetze-im-internet.de/englisch_gvg/englisch_gvg.html (last checked 17.05.16) and German version: http://www.gesetze-im-internet.de/gvg/BJNR005130950.html (last checked 17.05.16).
[6] So called Zivilprozessordnung (ZPO). English version https://www.gesetze-im-internet.de/englisch_zpo/englisch_zpo.html (last checked 17.05.16) and German version https://www.gesetze-im-internet.de/zpo/BJNR005330950.html (last checked 17.05.16).
[7] Urs Kindhäuser, Strafprozessrecht, 4. Auflage, 2016, § 2, Rn 3.
[8] Urs Kindhäuser, Strafprozessrecht, 4. Auflage, 2016, § 3, Rn 1.
[9] Ibid.
[10] Ibid.
[11] Ibid.
[12] Christian Geminn & Alexander Roßnagel, *"Privatheit" und "Privatsphäre" aus der Perspective des Rechts – ein Überblick*, 70 JURISTEN ZEITUNG 703 (2015).
[13] Art. 2 GG.

information-technological systems. The Privatsphäre is also built by the protection of the home and mediated communications.

The protection of the core area of private life, an important concept in criminal procedure delimiting an area which is (in principle) deemed absolutely inviolable, is based on human dignity. It includes areas such as private sentiments and feelings, reflections, opinions, and experiences of strictly personal nature (sex, health, religion), in which the individual must have the opportunity to express themselves without monitoring by the government. [14] However, the absolute inviolability in practice cannot always be ensured. For example, monitoring of communications between persons sharing a special relationship, within the scope of the core are is not permitted unless there is clear indication that the communication will pertain to a criminal offence, [15] however in other cases, where capturing content related to the core area cannot be a priori excluded, only its utilization is prohibited.[16]

The protection of informational self-determination protects personal data. It gives individuals the right to decide on the use and disclosure of their personal data. Furthermore, the right to informational self-determination provides protection from the compiling, storing, and analysing together with other data such information as was acquired by screening publicly available content in the absence of a statutory basis.[17] The Constitutional Court also interpreted the general personality right to include the confidentiality and integrity of information technology systems. The protection primarily protects data stored in the computer against secret access, which would allow for monitoring of private life.[18]

Secrecy of telecommunications is protected in Article 10 of the Constitution, covering both the content and the circumstances of such communications.[19] Furthermore, Article 13 protects the inviolability of the home by setting limits against physical intrusions, but also surveillance of the home.

The criminal procedural law's fundament is the German Constitution[20]. Relevant provisions in the constitution are among others rule of law principle rooted in article 20 (3)[21], and provisions relating to judicature like right to be heard in article 103 (1), ne bis in idem principle (no legal action can be instituted twice for the same cause of action) in article 103 (3) as well as the guarantee of judicial review in case of deprivation of liberty in article 104.

---

14 BVerfG NJW 2004, 999 (1002).

15 BVerfG NJW 2004, 999 (1003), NJW 2008, 822 (833).

16 See BVerfG NJW 2012, 907 (908).

17 BVerfG NJW 2008, 822 (836).

18 BVerfG NJW 2008, 822.

19 BVerfG NJW 2006, 976 (978); NJW 2008, 822 (825).

20 So called Grundgesetz (GG). English version: https://www.bundestag.de/blob/284870/ce0d03414872b427e57fccb703634dcd/basic_law-data.pdf (last checked 17.05.16) and German version http://www.gesetze-im-internet.de/bundesrecht/gg/gesamt.pdf (last checked 17.05.16).

21 Urs Kindhäuser, Strafprozessrecht, 4. Auflage, 2016, § 2, Rn 2.

Furthermore, the correlation between fundamental rights concerned with privacy and provisions in the CPC constituting a legal basis for the interference with aforementioned are relevant in this section.

3. The Protection of Places

3.1 Investigation of Places

The inviolability of the home is protected in Art. 13 of the German Constitution:

> *Article 13*
>
> *[Inviolability of the home]*
>
> *(1) The home is inviolable.*
>
> *(2) Searches may be authorised only by a judge or, when time is of the essence, by other authorities designated by the laws, and may be carried out only in the manner therein prescribed.*
>
> *(3) If particular facts justify the suspicion that any person has committed an especially serious crime specifically defined by a law, technical means of acoustical surveillance of any home in which the suspect is supposedly staying may be employed pursuant to judicial order for the purpose of prosecuting the offence, provided that alternative methods of investigating the matter would be disproportionately difficult or unproductive. The authorisation shall be for a limited time. The order shall be issued by a panel composed of three judges. When time is of the essence, it may also be issued by a single judge.*
>
> *(4)To avert acute dangers to public safety, especially dangers to life or to the public, technical means of surveillance of the home may be employed only pursuant to judicial order. When time is of the essence, such measures may also be ordered by other authorities designated by a law; a judicial decision shall subsequently be obtained without delay.*
>
> *(5) If technical means are contemplated solely for the protection of persons officially deployed in a home, the measure may be ordered by an authority designated by a law. The information thereby obtained may be otherwise used only for purposes of criminal prosecution or to avert danger and only if the legality of the measure has been previously determined by a judge; when time is of the essence, a judicial decision shall subsequently be obtained without delay.*
>
> *(6) The Federal Government shall report to the Bundestag annually as to the employment of technical means pursuant to paragraph (3) and, within the jurisdiction of the Federation, pursuant to paragraph (4)*

and, insofar as judicial approval is required, pursuant to paragraph (5) of this Article. A panel elected by the Bundestag shall exercise parliamentary oversight on the basis of this report. A comparable parliamentary oversight shall be afforded by the Länder.

(7) Interferences and restrictions shall otherwise only be permissible to avert a danger to the public or to the life of an individual, or, pursuant to a law, to confront an acute danger to public safety and order, in particular to relieve a housing shortage, to combat the danger of an epidemic, or to protect young persons at risk.

The home as a place, can be interfered with according to the following provisions of the CPC. Section 102 ff CPC, deals with the search of the body, property and premises of a person. Section 102 CPC defines the terms for a search of the mentioned subjects and objects in respect of the suspect, section 103 CPC defines the terms in respect of other people. Section 104 CPC defines the requirements for a search during night hours and section 105, 106 CPC lists the procedure for a search including the use of witnesses when searching the home. Section 107 and 109 CPC deal with post hoc notification and inventory requirements. Section 108 CPC regulates accidental discoveries ("Zufallsfund"). Section 110 CPC deals with examination of papers and in paragraph 3 the legislature implemented Art. 19 II CCC through the "Law on the Revision of Telecommunications Monitoring and other Covert Investigation Measures and on the Implementation of Directive 2006/24/EC"[22].

Besides the above mentioned "traditional" forms of interference with the home or other places, section 100c ff. CPC deal with acoustical surveillance of residential space, sometimes called "der große Lauschangriff". Section 100c CPC concerns the requirements for eavesdropping and recording of non-public conversations[23] taking place within the home using technical measures. Section 100d CPC regulated the relevant procedure for measures based on section 100c CPC. Finally, section 100e CPC concerns reporting obligations.

Another relevant section regarding places is 111 dealing with the installation of checkpoints to publicly accessible places. Since this section aims not at protecting a private place but a public space not related to the individual, it will be considered under the relevant sections 4, 5 and 6.

Finally, section 110a ff. CPC concerns undercover investigators. Section 110b (2) Nr. 2 and 110c CPC stipulates a warrant requirement for the use of undercover investigators which involve the entering of private premises.

[22] "Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG".

[23] Correlating with the scope of article 13 German Constitution: Only such conversation or spoken word, which is not addressed to the public or undeterminable group of people. Self-conversations are protected. See Hegmann Beck'scher Online-Kommentar StPO mit RiStBV und MiStra, Graf
24. Edition Stand: 16.11.2015 100c Rn 5.

3.1.1 The Home

The home includes premises which the suspect actually uses or stays at for living purposes, without the need for any permission or authorization.[24] Furthermore it does not matter whether the suspect has sole or shared custody of the premise.[25] The home must be interpreted widely.[26] The home can also be a temporarily used hotel room.[27] The premises must possess over an extern recognizable purpose of spatial privacy.[28] Including weekend houses, summer houses, camper or caravan, boats, tents or a sleeping car cabin in a train,[29] but also offices and non-accessible business space.[30]

The entrance area in front of a home is not part of the home.[31] Furthermore accommodation of soldiers or police officer are not considered as home.[32] The same applies to prison cells.[33] Controversial discussed are visiting rooms in which prisoner and defense lawyer meet.[34]

According to section 102 and 103 (1) the search can be concentrated on the capture of the suspect (so called "Ergreifungsdurchsuchung") or discovery of evidence (so called "Ermittlungsdurchsuchung").[35] Object of a search can be the home and other premises. Depending on whether the search takes place in the home of the suspect (section 102 CPC) or in the premises of other persons (section 103 CPC) the requirements can differ.

In general, to conduct a search an order must be issued by a judge accordant to section 105 I. Such a warrant ("Durchsuchungsbeschluss") is maximal valid for 6 months[36] and should be issued in written form[37] (but can also be issued oral form[38]). Under exigent circumstances, a search can also be ordered by the public prosecution office and/or "investigative personnel" (Ermittlungspersonen). Investigative personnel are police officers acting on behalf of the prosecution office. Not all police forces can act as investigative personnel, this, however, depends on each federal state's Police Law. In general, it can be stated that all visible acting police officers, when investigating a crime, are also investigative personnel.

---

[24] Meyer-Goßner/Schmitt/Schmitt 102 Rn. 7; *Bruns* Karlsruher Kommentar zur Strafprozessordnung 7. Auflage 2013 102 Rn. 9.
[25] *Hegmann*, Beck'scher Online-Kommentar StPO mit RiStBV und MiStra, Graf 24. Edition Stand: 01.09.2015, 102 Rn 8; BGH NStZ 1986, 84.
[26] Ibid.
[27] Ibid.
[28] KK-StPO/Bruns Rn. 8 mwN
[29] *Bruns* Karlsruher Kommentar zur Strafprozessordnung 7. Auflage 2013, 102 Rn 8
[30] *Bruns* Karlsruher Kommentar zur Strafprozessordnung 7. Auflage 2013, 102 Rn 8
[31] *Hegmann*, Beck'scher Online-Kommentar StPO mit RiStBV und MiStra, Graf 24. Edition Stand: 01.09.2015, 102 Rn 9; BGH NStZ 1998, 629, 630.
[32] *Bruns*, Karlsruher Kommentar zur Strafprozessordnung 7. Auflage 2013, 102 Rn 8.
[33] BVerfG NStZ 1996, 511
[34] *Hegmann*, Beck'scher Online-Kommentar StPO mit RiStBV und MiStra, Graf 24. Edition Stand: 01.09.2015, 102 Rn 9; *Bruns* Karlsruher Kommentar zur Strafprozessordnung 7. Auflage 2013, 102 Rn 8.
[35] Urs Kindhäuser, Strafprozessrecht, 4. Auflage, 2016, § 8, Rn 138; Sommermeyer Jura 1992, 449, 449 f; Walther JA 2010, 32.
[36] BVerfGE 96, 44, 52 ff.
[37] BVerfGE 20, 223, 227.
[38] BGH StV 2006, 174, 175.

In light of the constitutionally rooted warrant requirement (art. 13 (2) German Constitution), exigent circumstances must be applied restrictively, thus requiring the police to at least try to contact a Judge.[39] Furthermore, according to section 102, a search must always be based on reasonable suspicion by the authorities. Pure presumptions are not enough.

For a search according to section 103 CPC besides the above mentioned reasonable suspicion, certain facts supporting the conclusion that the person, trace, or object sought is located on the premises to be searched must be given.

Furthermore, according to section 103 (1) 2 CPC a "search of private and other premises shall also be admissible if they are located in a building in which it may be assumed, on the basis of certain facts, that the accused is located". A search based on (1) 2 can only be committed to capture a suspect of a terrorism related crime and not to discover evidence.

A search of the home during night hours according to section 104 CPC is only possible under restrictive requirements such as a suspect is caught red handed and followed into the home etc.

According to section 108 of the procedural law, also other objects than the one searched for, can be searched when found during the initial search, when they "indicate the commission of another criminal offence".

Besides section 102 ff. CPC which is more a traditional view on interference with the home, section 100c ff CPC so called acoustical surveillance of residential spaces are relevant. Section 100c CPC empowers the authorities to listen to non-public[40] conversations taking place within the home or other premises and record the spoken word. The use of technical devices is also covered by this provision. This does not include tapping the phone or any visual surveillance measures[41].

The use of this provision is limited to the crimes stated in its paragraph 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.

The provision is based upon article 13 (3)-(4) German Constitution.[42] It is important to note that 100c (4) CPC explicitly forbids measures which would infringe the core of privacy. The provision reads: "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.

---

[39] Gusy, NStZ 2010, 353.

[40] Correlating with the scope of article 13 German Constitution: Only such conversation or spoken word, which is not addressed to the public or undeterminable group of people. Self-conversations are protected. See Hegmann Beck'scher Online-Kommentar StPO mit RiStBV und MiStra, Graf
24. Edition Stand: 16.11.2015 100c Rn 5.

[41] Eisenberg NStZ 2003, 638.

[42] Urs Kindhäuser, Strafprozessrecht, 4. Auflage, 2016, § 8, Rn 96.

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." Paragraph 5 than additional states: "The interception and recording is to be interrupted without delay if during 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" (see section 100d (1) 1). 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 CPC). An extension can be issued for 1 month, until a total period of 6 months is reached and the higher regional court needs to decide upon further extensions.

The need to enter the home for the purposes of installing the eavesdropping equipment is also covered by section 100c CPC.[43]

3.1.2 Places of employment

Home also includes work and office rooms which are not openly accessible.[44] Same applies for association, union or clubrooms.[45]

[43] *Hegmann*, Beck'scher Online-Kommentar StPO mit RiStBV und MiStra, Graf 24. Edition Stand: 16.11.2015, 100c Rn 3.
[44] BVerfG NJW 1971, 2299; 2003, 2669; *Hegmann*, Beck'scher Online-Kommentar StPO mit RiStBV und MiStra, Graf 24. Edition Stand: 01.09.2015, 102 Rn 8.
[45] Similar *Hegmann*, Beck'scher Online-Kommentar StPO mit RiStBV und MiStra, Graf 24. Edition Stand: 01.09.2015, 102 Rn 8.

3.1.3 Other non-residential (semi-) closed places

Enclosed estate like the front yard[46] and a hedged garden[47] or premises which are not used for another purpose than living in, like storage room[48] are also protected as part of home.

3.1.4 Public and quasi-public spaces

See reference to section 111 CPC in introduction of this chapter.

3.1.5 Vehicles

Vehicles like cars, except a camper or caravan, are not protected under the concept of home or other premises, because it does not serve as a living place but as a means of transportation.[49] But if it is mainly used as a living place, which is clearly recognizable from outside, it most likely will also fall under home.

The rationale is, that the place should be clearly definable, not open to the public and usable as a place of living, whether it is for work, watching a movie, listening to music or to sleep.

But the vehicle will fall under "property" according to section 102, 103 CPC and should therefore be considered under point 6.

3.1.5.1 Containers found in the vehicles

See point 6.

3.1.6 Computers and cell phones

Information systems are afforded special protection by the Constitutional Court, which interpreted Art. 2 GG to include the right to integrity and confidentiality of information-technology systems justified by the relevance of the use of information-technological systems for the expression of personality (Persönlichkeitsentfaltung) and from the dangers for personality that are connected to this use.[50] The Court defined the protected information-technical systems as "all systems that alone or in their technical interconnectedness can contain personal data of the affected person in a scope and multiplicity such that access to the system makes it possible to get insight into relevant parts of the

[46] *Hegmann,* Beck'scher Online-Kommentar StPO mit RiStBV und MiStra, Graf 24. Edition Stand: 01.09.2015, 102 Rn 8.
[47] BGH NStZ 1998, 157.
[48] *Hegmann,* Beck'scher Online-Kommentar StPO mit RiStBV und MiStra, Graf 24. Edition Stand: 01.09.2015, 102 Rn 8.
[49] *Hegmann,* Beck'scher Online-Kommentar StPO mit RiStBV und MiStra, Graf 24. Edition Stand: 01.09.2015, 102 Rn 9.
[50] BVerfG NJW 2008, 181.

conduct of life of a person or even gather a meaningful picture of the personality." However, the right protects primarily from covert monitoring and searching of the information systems, and not open measures such as searches and seizures.

Searches of Computers or cell-phones, including the so-called extended search, will partially fall under section 110 CPC[51] concerning the search of papers and documents:

> *Section 110*
> *[Examination of Papers]*
>
> *(1) The public prosecution office and, if it so orders, the officials assisting it (section 152 of the Courts Constitution Act), shall have the authority to examine documents belonging to the person affected by the search.*
>
> *(2) In all other cases, officials shall be authorized to examine papers found by them only if the holder permits such examination. In all other cases they shall deliver any papers, the examination of which they deem necessary, to the public prosecution office in an envelope which shall be sealed with the official seal in the presence of the holder.*
>
> *(3) 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; Section 98 subsection (2) shall apply mutatis mutandis.*

The general provision of 102 ff. CPC is also relevant for these searches.

As evident upon reading Section 110 COC, it is also possible to extend a search of data conducted on a local PC to a cloud storage according to section 110 III CPC. Art. 110 CPC, in general, speaks about the examination of papers. In regard to Art. 19 II CCC we must determine whether this can be interpreted as "data". Hegemann, states that "papers" must be interpreted broadly. He states that it should be interpreted as any "intellectual statement" incorporated into a medium like a Daily, Drawings, Hard Drives, Flashcards, etc.[52] Thus "data" can be seen as "papers". Furthermore, paragraph 3 of section 110 Procedural Code clearly mentions data in the context of an "electronic storage medium", which itself according the Hegemann's approach could be considered as "papers". An "electronic storage medium" can then be understood as a "device consisting of

[51] *Hegmann,* Beck'scher Online-Kommentar StPO mit RiStBV und MiStra, Graf 24. Edition Stand: 01.02.2016, 110 Rn 3.
[52] BeckOK StPO/*Hegemann* StPO § 110 Rn. 1, 3.

hardware and software developed for automatic processing of digital data" (Computer System) according to rn 23 of the explanatory report CCC, since section 110 (3) Procedural Code is, like shown above, clearly Art. 19 II CCC's implementation into the German legislation. Schlegel[53], on page 26, then refers to "documents" in regard to data on a computer system as consisting of "directories" and "files".

Exempt from such files and directories must be data which is be deemed to be published publicly like Books, Manuscripts or data which in paper form could not be seized (§ 97 Procedural Code).[54]

Paragraph 3 of section 110 Procedural Code must be read in context of section 102 and 103.[55] According to section 102, a search must always be based on reasonable suspicion by the authorities. It is already sufficient that there is a general possibility of finding relevant evidence on the "main" computer system.[56] The purpose of the search therefore must be the finding of evidence for a certain offence.57 A warrant is necessary according to section 105 CPC (‚in exigent circumstances the public prosecution office and the officials assisting it can order the search). Authorized to conduct such a search is the prosecution department but prosecutors can authorize "investigative personnel" (section 152 Courts Constitution Act)[58].[59] Only then the search can be extended according to section 110 III CPC.

Without an authorizing act, the examination mentioned in section 110 (3) CPC can only be conducted, considering section 110 (2), if the holder permits such an examination. If no permission is given "they shall deliver any papers, the examination of which they deem necessary, to the public prosecution office in an envelope which shall be sealed with the official seal in the presence of the holder" (section 110 (2)). Seen in the context of paragraph 3 this means copying the data and making sure it is not accessible for unauthorized persons, by e.g. encrypting it. According to Schlegel, to determine the relevant data, the "police" can only exanimate the directory listing but not the files themselves.[60] In this context, it is interesting to consider how the police will determine which data might be relevant, if the directory listing does not give any indications. A complete copy might be disproportional, but then again, copying data for an examination is not considered a seizure.[61]

---

[53] *Stephan Schlegel*, "Online-Durchsuchung light" – Die Änderung des § 110 StPO durch das Gesetz zur Neuregelung der Telekommunikationsüberwachung, page 26, 2008, http://www.hrr-strafrecht.de/hrr/archiv/08-01/index.php?sz=7#25 (last checked 29.10.15) (German)
[54] BeckOK StPO/*Hegemann* StPO § 110 Rn. 2.
[55] *Stephan Schlegel*, "Online-Durchsuchung light" – Die Änderung des § 110 StPO durch das Gesetz zur Neuregelung der Telekommunikationsüberwachung, page 25, 2008, http://www.hrr-strafrecht.de/hrr/archiv/08-01/index.php?sz=7#25 (last checked 29.10.15) (German)
[56] BeckOK StPO/*Hegemann* StPO § 102 Rn. 1.
[57] BeckOK StPO/*Hegemann* StPO § 102 Rn. 3.
[58] English version: http://www.gesetze-im-internet.de/englisch_gvg/englisch_gvg.html#p0723 (last checked 29.10.15) and German version: http://dejure.org/gesetze/GVG/152.html (last checked 29.10.15).
[59] *Stephan Schlegel*, "Online-Durchsuchung light" – Die Änderung des § 110 StPO durch das Gesetz zur Neuregelung der Telekommunikationsüberwachung, page 26, 2008, http://www.hrr-strafrecht.de/hrr/archiv/08-01/index.php?sz=7#25 (last checked 29.10.15) (German); see already section 110 (1) Procedural Code.
[60] Ibid, page 26 f.
[61] Ibid, page 26.

Section 110 III CPC reads: "…the search may be extended to cover also physically separate storage media insofar as they are accessible from the storage medium". Whether this is limited to the intranet LAN or WLAN connected devices or through internet connected devices is not per se stated. But since the provision is deemed to prohibit that "data sought would otherwise be lost" (section 110 (3)) it is seen as covering both intra- and internet connections.[62] Moreover when it is not possible to determine whether the "accessed" data on the connected device is stored on a computer system abroad, the subsequent securing of data can be conducted without the permission of the foreign state having jurisdiction upon the territory the device is located in.[63]

Another problem is, that the provision gives no restrictions towards the data that can be examined on the connected computer system. This seems to be especially critical considering that data accessed through such a connection, might not only be the data of the "suspect" but data of a "third" party. This would, in regard to section 103 CPC, result in a higher threshold to be met by the authorities with examining such data. Schlegel, on page 27 f., explains therefore, that in the case of accessing data stored in a connected device, to determine which data can be examined, we must not look at who owns the data but who has custody or shared custody upon the data. Only when it is evident that the data are not relevant or belong to a third party, such data are out of bounds.

Schlegel[64], furthermore states that although there is no real restriction towards which data can be examined, it must be always seen in the context of a search, thus relate to the purpose of the search. Any access to an "external" computer system through the main computer, can only be justified by section 110 (3) CPC, if the main computer already was adjusted to have such a connection, or if passwords were found during the examination or given by the "suspected person" and the therefore created access is on a similar quality level as an already existing connection.[65]

The so-called online searches in the meaning of covert remote searches of information systems for whichever purpose and by whichever means are not regulated in the CPC, and the powers of intervention currently found in the Code of Criminal Procedure are insufficient to justify the infiltration of computer systems.[66] Nevertheless, the power has been included in the Art. 20k of the Act on the Federal Criminal Police Office (BKAG) for the purposes of averting danger. These provisions have to comply with the limits set by the Constitutional Court. Section 20k of the BKAG authorises access to information technology systems and permits covert remote searches of information technology systems, by means of which data saved or stored on the affected person's private computer or other computers linked thereto can be collected and the person's online behaviour can be tracked. The provision thus permits interference with the fundamental right to the guarantee of the confidentiality and integrity of

[62] BeckOK StPO/Hegemann StPO § 110 Rn. 13.
[63] BeckOK StPO/Hegemann StPO § 110 Rn. 15.
[64] *Stephan Schlegel*, "Online-Durchsuchung light" – Die Änderung des § 110 StPO durch das Gesetz zur Neuregelung der Telekommunikationsüberwachung, page 28, 2008, http://www.hrr-strafrecht.de/hrr/archiv/08-01/index.php?sz=7#25 (last checked 29.10.15) (German).
[65] Ibid.
[66] *Benjamin Vogel, Patrick Köppen, Thoma Wahl* "INTLI Country Report Germany", Max Planck Institute for Foreign and International Criminal Law, 2016, p. 554.

information technology systems,[67] but only in restricted areas, mainly protection from terrorist attacks. The current provision has recently been declared (in part) unconstitutional, since it does not contain sufficient safeguards of proportionality and for the protection of the core area of private life. The Court emphasized that *"today, diary-like written expressions, intimate statements, or other written manifestations of highly personal experience, film or audio recordings are increasingly generated, saved and in part exchanged in electronic form. A large part of highly personal communication takes place electronically by means of communications services over the internet or in the context of internet-based social networks. This data, whose confidentiality the persons concerned depend upon and trust in, is largely no longer to be found on personal information technology systems alone but rather on that of third parties. The fundamental right to the guarantee of the confidentiality and integrity of information technology systems therefore protects against covert access to this data, and thus in particular against remote searches whereby private computers as well as other information technology systems are manipulated and read, and whereby personal data stored on external servers with a reasonable expectation of confidentiality is accessed and movements on the web of the persons concerned are tracked. Given the often highly personal nature of this data, which arises in particular when it is taken as a whole, this constitutes a particularly intense interference with this fundamental right. Its weight is commensurable with that of an interference with the inviolability of the home."*[68]

The Court also stressed different nature of the Core Area concept when applied to computers as opposed to the protection of home life: *"Here, protective measures to prevent violations of the core area do not aim primarily at preventing the collection and recording of a fleeting, highly confidential moment in a private space, but rather at preventing the reading of highly confidential information within a comprehensive data set of digital information that already exists, and that, taken as a whole, is typically not of a private nature the way behaviour or communication in a home would be. Here, the surveillance does not take place in the form of a chronologically ordered occurrence in different locations, but rather as access by means of a spy program which, as far as the access is concerned, presents only the alternatives of all or nothing."*[69] Whereas precluding any access to potential information pertaining to the core area would be practically impossible, the Court iterated that an independent body must filter out information relevant to the core area before it becomes available to the police authorities.70 The filtering serves as a safeguard of legality, but also to prevent the law enforcement from accessing information related to the core area, which is irrelevant for their investigation.[71]

[67] BVerfG1 BvR 966/09, 209.
[68] BVerfG1 BvR 966/09, 210.
[69] BVerfG1 BvR 966/09, 218.
[70] BVerfG1 BvR 966/09, 220.
[71] BVerfG1 BvR 966/09, 224.

4. The protection of persons

4.1 Protection from interference with the body

4.1.1 Limited detention/stops/frisks

The relevant provisions are:

Section 163b and 163c CPC dealing with the establishment of Identity and duration of a consequential custody. Section 163b CPC stipulates, that against a suspect of a crime, measures which are necessary to establish his/her identity can be taken by the police and prosecution office. The suspect might also be kept in custody if the identity cannot be established by other means or only with considerable difficulty. The custody according to section 163c CPC cannot take longer than it is necessary for the establishment of the identity and the person needs to be brought before a judge without delay. The maximum duration cannot exceed 12 hours (163c (2) CPC). According to (3) "If identity has been established the records prepared in connection with the establishment shall be destroyed (…)[72]".

The custody in this case does not constitute a provisional arrest, which is regulated in section 127 CPC.

Besides the suspect, the same measures can be taken against non-suspects, but only under the conditions determined in section 163b (2) CPC. Paragraph 2 stipulate that such measures can only be taken if and so far as this is necessary to clear up a criminal offence and taking a person into custody needs to be proportionate to the importance of the matter.

To establish the identity of a person, whether suspect or non-suspect, according to section 163b (1) 3 CPC, the relevant person can be searched. This is only allowed if the identity cannot be established by other means or only with considerable difficulty. Furthermore, in case of a non-suspect, such measures "may not be taken against the will of the person concerned" (see section 163 b (2)).

As was already mentioned under 3.1 and 3.1.1. section 102 ff. CPC are also of relevance. As explained, the section not only concerns the search of a home or other premises, but also a body search and search of the property is covered by this section. Regarding the section at hand (4.1.1.) the actual understanding of body as referred to in sections 102 and 10373 CPC is important. These sections must be read in context with section 81d, 81a CPC dealing with a physical

[72] Shortened.

[73] The provision does not explicitly mention the body but it is established that the body can be part of the search. See Meyer-Grossner/Schmitt 103 Rn 3; *Hegmann* Beck'scher Online-Kommentar StPO mit RiStBV und MiStra, Graf 24. Edition Stand: 01.02.2016, 103 Rn 3.

examination.[74] The search of the body must be focused on the discovery of evidence.[75] Only the worn clothing and/or the observation of body parts (even mouth and anus)[76] without the use of medical devices can undertaken.[77] If the search interferes with the sense of shame (intimacy) it can only be conducted by a physician or at least a police officer from the same gender as the searched person.[78] According to section 82d (2) CPC it is not possible to consent to a search conducted by an officer of the opposite gender. An interference with the sense of shame is assumed when the person is completely undressed in front of a person from the opposite gender, who is not a, or when the search includes genitals (anus would fall under this category).[79]

Based on section 81a CPC the accused can be taken into custody and brought to the physician.[80]

Finally, section 81 CPC should be mentioned here, which deals with the placement of the accused into a public psychiatric hospital for the preparation of an opinion on the accused's mental condition. (2) Stipulates: "The court shall make the order pursuant to subsection (1) only if the accused is strongly suspected of the offence."

4.1.2 Traffic stops and traffic checkpoints

Another relevant section regarding places is 111 dealing with the installation of checkpoints to publicly accessible places. Section 111 CPC is, as the majority of all provisions in the CPC, a repressive measure. The provision does only apply when *"certain facts substantiate the suspicion that a criminal offence"* has been committed, mainly related to terrorism. In such cases *"checkpoints may be established on public roads, squares and at other publicly accessible places"* and *"At a checkpoint all persons shall be obliged to establish their identity and to subject themselves or objects found on them to a search".*

"The order to establish a checkpoint shall be issued by the judge; in exigent circumstances, the public prosecution office and the officials assisting it (section 152 of the Courts Constitution Act) shall be authorized to make such an order."

[74] *Ritzert,* Beck'scher Online-Kommentar StPO mit RiStBV und MiStra, Graf 24. Edition Stand: 01.02.2016, 89d Rn 1.
[75] *Hegmann*, Beck'scher Online-Kommentar StPO mit RiStBV und MiStra, Graf 24. Edition Stand: 01.09.2015, 102 Rn 11.
[76] Urs Kindhäuser, Strafprozessrecht, 4. Auflage, 2016, § 8, Rn 45; Meyer-Grosner/Schmitt 81a Rn 15; different oppinion Bosch, Jura 2014, 50, 51.
[77] *Bruns*, Karlsruher Kommentar zur Strafprozessordnung 7. Auflage 2013, 102 Rn 10.
[78] *Ritzert*, Beck'scher Online-Kommentar StPO mit RiStBV und MiStra, Graf 24. Edition Stand: 01.02.2016, 81d Rn 1.
[79] *Ritzert*, Beck'scher Online-Kommentar StPO mit RiStBV und MiStra, Graf 24. Edition Stand: 01.02.2016 81d Rn 5.
[80] Urs Kindhäuser, Strafprozessrecht, 4. Auflage, 2016, § 8, Rn 42.

4.1.3 Arrest/imprisonment

The central procedure for an arrest, based "upon suspicion of a crime", would be an arrest warrant ("Haftbefehl") in writing according to section 114 CPC, issued by a Judge and in the name of the suspect and enforced by the police.

Since any arrest always affects the freedom of a person crucially, an arrest warrant must meet the standards set in its legal basis. In Germany the material requirements are placed into section 112 CPC.

Thus the accused must be strongly suspected of the offence ("dringender Tatverdacht") and a ground for arrest ("Haftgrund") must be existing. Without going into too much detail, we will just shortly explain what these two terms mean.

"Dringender Tatverdacht" is given, when under the current state of investigation, a high likelihood is at hand, that the accused, in person of the perpetrator or accomplice, unlawfully and culpable committed a crime.[81]

Additionally, a ground for arrest must be at hand. The Procedural Code determines four grounds:

- Flight or risk of flight, section 112 II Nr.1 and 2
- Risk of tampering with evidence, section 112 II Nr. 3
- Suspicion in regard to a capital crime, section 112 III
- Danger of Repetition, section 112a

Other forms of remand detention can be found in section 127b ("Hauptverhandlungshaft"), section 453c ("Sicherungshaft"), section 457 (2) ("Vollstreckungshaft"), section 230 (2), 236, 329 (4) 1 ("Ungehormsamshaft") CPC.

In certain circumstances the Procedural Code allows for an arrest, although no arrest warrant was issued prior. The relevant sections of the code are 127 I and II, 127 b and 163 b I, all concerning a "provisional arrest".

Section 127 I CPC is a justification for anyone to arrest another person, which is caught in the act or is being pursued. It also creates a legal basis for arrests by the police, although only, if the ground for arrest is "reason to suspect flight", since section 163b (mentioned under 4.1.1.) is lex specialis for the police if the "ground for arrest is "establishment of identity".

The purpose of this exception to the general rule of an arrest warrant is, that a warrant in the situation "caught in the act" (in flagrante delicto) and "being

[81] Translated the definition cited by *Kindhäuser*, Strafprozessrecht, 3. Edition, § 9 Rn. 7: „Dringender Tatverdacht liegt vor, wenn nach dem bisherigen Ermittlungsstand eine hohe Wahrscheinlichkeit dafür besteht, dass der Beschuldigte als Täter oder Teilnehmer rechtswidrig und schuldhaft eine Straftat begangen hat."

pursued", will most likely be too late and therefore prohibit an arrest. "Caught in the act" is who is immediately caught at the scene of the crime.[82] They are "being pursued", if the suspect already left the scene of the crime, but can be traced immediately and pursued.[83]

Since the arrest is only provisional, according to section 128, the arrest personal must be brought before the judge within a day after his arrest.

Section 127 II is only applicable to the public prosecution office or the police. The provision consists of two main requirements.

There must be exigent circumstances and prerequisites for issuance of a warrant of arrest (or of a placement order). We examined the prerequisites for issuance of a warrant of arrest earlier, thus requiring a ground for arrest and "dringender Tatverdacht". Exigent circumstances are at hand, when the arrest as a result of the delay caused by a potential arrest warrant procedure would be endangered (prevented).[84]

Like section 127 I, the arrest in 127 II is only provisional, thus section 128 applies as well.

Without going into too much detail, we only mention section 127b CPC, which mainly allows the police to arrest someone (provisional) when section 127 I and II are not applicable and it is probable that an immediate decision will be taken in accelerated proceedings in addition to a fear that the arrested person will fail to appear the main hearing.

Again section 128 applies as well.

4.1.4 Identification measures

Please see remarks to section 163b and 163c CPC under 4.1.1. Also section 127 (1) and (2) CPC see 4.1.3.

Another relevant provision might be section 81b CPC dealing with photographs and fingerprints. The provision states: "Photographs and fingerprints of the accused may be taken, even against their will, and measurements may be made of them and other similar measures taken with regard to them insofar as is required for the purposes of conducting the criminal proceedings or of the police records department."

Section 81b CPC only applies to the accused and cannot be used to gather fingerprints etc. from the suspect.[85]

Similar measures only concern measures which concern the characteristics of a body, but only as they don't enter the sphere of section 81a (1) CPC86, and

[82] *Kindhäuser*, Strafprozessrecht, 3. Edition, § 8 Rn 25.
[83] Ibid.
[84] *Kindhäuser*, Strafprozessrecht, 3. Edition, § 8 Rn 31.
[85] Urs Kindhäuser, Strafprozessrecht, 4. Auflage, 2016, § 8, Rn14.
[86] BGHSt 34, 39, 44f; Meyer-Grossner/Schmitt, 81b Rn 8.

include e.g. writing samples, hand and foot prints.[87] The goal is to determine outer permanent characteristics of the body. It is unclear whether changes to the appearance by trimming the beard or cutting the hair of the accused can be seen as other measures.[88] The opposite opinion champions to use section 81a CPC, since the body is affected.[89] It is also discussed in literature whether voice recordings can be seen as other measures.[90]

4.1.5 DNA investigations

Already mentioned above (see 4.1.1.), section 81a CPC deals with physical examinations and blood tests. Not really a DNA investigation, but somehow related, the section will be mentioned here.

Both blood tests and physical examination, can only be ordered by a judge (section 81a (2) CPC). Under exigent circumstances the prosecution office or police can order the test, unless it is a serious interference with the body[91]. A formal order is dispensable if the accused consents to the measure.[92]

The purpose of the examination (including blood test), must be the establishment of facts which are of importance for the proceedings (see section 81a (1)).

The physical examination is divided into plain body examination according to section 81a (1) 1 CPC and physical interferences with the body according to (1) 2 CPC. Under plain body examination we can understand procedures like an EKG, EEG or just checking the blood pressure.[93] A typical physical interference is the taking of blood. In general, all injections, extractions or ever so small injuries to the body are regarded as physical interferences. Physical examinations must be conducted by a physician.[94]

It is important to note that the accused does not have to actively cooperate with the measures but has to tolerate them.95 Undressing is not seen as actively cooperating, and therefore must be undertaken by the accused if requested.[96] Blowing into a device to determine the alcohol level is regarded as actively cooperating behavior and therefore not covered by section 81a CPC.[97] Furthermore because of the nemo-tenetur principle emetics must not be

[87] Odenthal NStZ 1985, 433, 434.
[88] Arguing that such measures are just a different type of preparation measures for the identification process, see Geerds, Jura 1986, 7, 9; Meyer-Gossner/Schmitt 81b Rn 10; Urs Kindhäuser, Strafprozessrecht, 4. Auflage, 2016, § 8, Rn14
[89] BVerfGE 47, 239; Odenthal NStZ 1985, 433, 434.
[90] Positive: HK-Brauer 81b Rn 9; Restrictive KMR-Bosch 81b Rn 13; Negative: SK-Rogall 81b Rn 53. Judicature declares the so found evidence not usable BGH NJW 1986, 2261.
[91] Karlsruher Kommentar zur Strafprozessordnung 7. Auflage 2013, *Senge* 81a Rn8.
[92] Urs Kindhäuser, Strafprozessrecht, 4. Auflage, 2016, § 8, Rn35.
[93] Urs Kindhäuser, Strafprozessrecht, 4. Auflage, 2016, § 8, Rn37.
[94] Urs Kindhäuser, Strafprozessrecht, 4. Auflage, 2016, § 8, Rn40.
[95] Urs Kindhäuser, Strafprozessrecht, 4. Auflage, 2016, § 8, Rn41.
[96] Urs Kindhäuser, Strafprozessrecht, 4. Auflage, 2016, § 8, Rn41.
[97] Ibid.

swallowed by the accused. Whether they must tolerate the administration is debated.[98]

Other persons than the accused can only be examined if they consent, or under the restrictive requirements stipulated in section 81c CPC.

Drawn blood and other samples can only be used in the case at hand and need to be destroyed afterwards (section 81a III CPC).

On the samples taken according section 81a I CPC, molecular-genetic examinations can be undertaken according to section 81e and 81f CPC. But only in so far as such measures are necessary to establish descent or to ascertain whether traces found originate from the accused or the aggrieved person. Such examinations are also allowed on material obtained by measures pursuant to section 81c CPC. Furthermore examinations can be carried out on trace materials which have been found, secured or seized.

According to section 81f I 1 CPC molecular-genetic examinations can only be ordered by a judge, except in the case of consent. Under exigent circumstances, an examination can also be ordered by the public prosecution office and/or "investigative personnel". The warrant requirement is dropped when only trace material according to 81e II CPC is examined.

Section 81g CPC works as a legal basis to create a DNA-Databank, which is supposed to help identifying suspects in future crimes.[99] Paragraph 1 reads:

> *"If the accused person is suspected of a criminal offence of substantial significance or of a crime against sexual self-determination then, for the purposes of establishing identity in future criminal proceedings, cell tissue may be collected from him and subjected to molecular and genetic examination for the purposes of establishing the DNA profile or the gender if the nature of the offence or the way it was committed, the personality of the accused or other information provide grounds for assuming that criminal proceedings will be conducted against him in future in respect of a criminal offence of substantial significance. If the person concerned habitually commits other criminal offences, this may be deemed to be equivalent to a criminal offence of substantial significance by reference to the level of the injustice done."*

Paragraph 2 states "The cell tissue collected may be used only for the molecular and genetic examination referred to in subsection (1); it shall be destroyed without delay once it is no longer required for that purpose. Information other

[98] Pro: Rogall, NStZ 1998, 66, 67 f; Schuhr NJW 2006, 3538 ff; Schuman, StV 2006, 661 ff.; BGH NJW 2012, 2453, 2454; EGMR StV 2006, 617 ff. Contra: OLG Frankfurt NJW 1997, 1647; Hackethal, Der Einsatz von Vomitivmitteln zur Beweissicherung im Strafverfahren 2005, 147 ff, 167 ff; Renzikowski Amelung-FS 1986, 234, 236.

[99] *Ritzert*, Beck'scher Online-Kommentar StPO mit RiStBV und MiStra, Graf 24. Edition, 81g Rn Before 1.

than that required in order to establish the DNA profile or the gender may not be ascertained during the examination; tests to establish such information shall be inadmissible."

Only the judge can order the collection of cell tissue or in exigent circumstances, the public prosecution office and/or "investigative personnel" (paragraph 3). Consent makes the warrant obsolete. Importantly, any molecular or genetic examination of the cell tissue needs either consent or an order by a judge. No exigent circumstances exception apply.

The data may be transmitted only for the purposes of criminal proceedings, for threat prevention and for international mutual legal assistance in respect thereof (see last part paragraph 5).

Measures undertaken according to section 81g CPC can only be concentrated on the accused not third persons.[100]

Finally, section 81h CPC allows for serial molecular and genetic examinations ("DNA-Reihenuntersuchung"). Such mass screenings, for which cell tissue can be collected, subjected to a molecular and genetic examination to establish gender and the DNA profile and DNA profiles established can also automatically matched against the DNA profiles of trace materials. Such test can only be conducted with the consent of the person affected. Additionally a judge must order the measure (paragraph 2). 81h CPC is only applicable where "certain facts give rise to the suspicion that a felony against life, physical integrity, personal freedom or sexual self-determination has been committed", "the person affected must manifest certain significant features which may be assumed to apply to the perpetrator" and "insofar as this is necessary in order to ascertain whether the trace material(s) originated from such persons and the measure is not disproportionate to the gravity of the offence, particularly in view of the number of persons affected by the measure" (according to paragraph 1). Insofar as the data relating to the DNA profiles established by the measure is no longer necessary for clearing up the felony it shall be deleted without delay. The fact of the deletion shall be documented (paragraph 3).

4.2 Protection from interference with the mind

4.2.1 Protection from interference with personal choices

4.2.1.1 The right to counsel

The right to counsel ("Das Recht auf Verteidigung") is a core requirement for the proceedings to be in line with the "Rechtsstaatprinzip" (state based on justice

[100] Urs Kindhäuser, Strafprozessrecht, 4. Auflage, 2016, § 8, Rn. 53.

and integrity) located in Art. 20 together with Art. 2 German Constitution. The right to council or defend oneself is also stated in Art. 6 III (c) ECHR. The relevant provision in the CPC is article 137. Whether by choice or mandatory the defense counsel is obligated to defend the accused in the best form possible.

The defense counsel has the following rights:

- Right to be present ("Answesenheitsrecht") (during all interrogations by a judge or the prosecutor of the accused (section 163a III 2, 168c I CPC), interrogations of a witness (section 168c II CPC), during judicial inspection (section 168d CPC) and during the main hearings)

- The right to speak and defend the accused ("Äußerungsrecht") section 137

- Access to records (Akteneinsichtsrecht) section 147 CPC

- Free Contact ("Freier Kontakt"). During the criminal procedure the accused must be allowed to have free, not monitored oral and written contact to his/her defense counsel. The right to have not monitored written contact can be restricted in case of criminal offenses according to sections 129a ff. German Criminal Code[101] (see section 148 II CPC).

- Right to adduce evidence

The accused furthermore has the right to request a translator, if they have trouble understanding German (section 187 I CCA, Art. 6 III e ECHR). Additionally they have the right to contact the consulate of his/her home country (section 114b II 4 CPC).

4.2.1.2 The right against self-incrimination

The so called "Schweigerecht" ("Right to keep silent") is located in Art. 2 I together with Art. 1 I German Constitution and is often cited together with the above explained Rechtsstaatsprinzip Art. 20 III German Constitution. Nemo tenetur se ipsum accusare also allows him to lie when questioned if that does not result in pretending to committed a crime or an insult.

4.2.2 Other protections for intellecual activity and thought

Another section relevant for the protection of thoughts and intellectual activity is the section 136a CPC Prohibited Methods of Examination:

Paragraph 1 reads: "The accused's freedom to make up his mind and to manifest his will shall not be impaired by ill-treatment, induced fatigue, physical interference, administration of drugs, torment, deception or hypnosis. Coercion

[101] Terrorism related crimes.

may be used only as far as this is permitted by criminal procedure law. Threatening the accused with measures not permitted under its provisions or holding out the prospect of an advantage not envisaged by statute shall be prohibited."

Paragraph 2: "Measures which impair the accused's memory or his ability to understand shall not be permitted."

Paragraph 3: "The prohibition under subsections (1) and (2) shall apply irrespective of the accused's consent. Statements which were obtained in breach of this prohibition shall not be used, even if the accused consents to their use."

4.3 Protections of behavioral privacy

Only indirectly affecting behavioral privacy, section 163e CPC covers Police Observation. The goal of the measures taken in accordance with section 163e CPC is to create a full movement pattern of the accused or his/her contact person.[102] Already existing police controls are used to "search" for the accused. The measures are aimed at the accused and establishing his/her identity, travel pattern or route, means of transportation, carried goods and companions.[103] Against other people (contact persons) the measures are only permitted under the restrictive requirements of section 163e I 3 CPC. Additional car plates can be included into the observation if the car is registered to the accused or if the car is used by the accused or by a thus far not identified person, provided he/she has committed a criminal offence of substantial significance (section 163e II CPC). Paragraph III allows to include non-related third parties personal data into the observation in case the person is with the accused. Section 163e IV 1 CPC stipulates that the judge has to order the measures. Under exigent circumstances, the measures can also be ordered by the public prosecution office but not by the "investigative personnel" (Ermittlungspersonen). The measures can be taken out up until a year after issuance of the order (section 163e IV 5 CPC).

Furthermore, according to sections 131 ff CPC an arrest notice, notice to determine whereabouts, publication of pictures and other measures can be taken.

Ausschreibung zur Festnahme (Arrest Notive) section 131

Ausschreibung zur Aufenthaltsermittlung (Notice to Determine Whereabouts) section 131a

Ausschreibung zur Identitätsfeststellung und zu sonstigen Maßnahmen (Notice to determine identity and other measures) sections 131a II, 131b

[102] Urs Kindhäuser, Strafprozessrecht, 4. Auflage, 2016, § 8, Rn. 18.
[103] Urs Kindhäuser, Strafprozessrecht, 4. Auflage, 2016, § 8, Rn. 19.

The notices can be published in newspapers or otherwise broadcasted. Furthermore pictures can be published according to section 131b CPC. Without going into detail, in general all measures must be ordered by a judge except under exigent circumstances.

Another only indirect measure is the seizure of the driver's license according to section 94 III, 111a CPC. Briefly, one has to separate between the document and the license that gives the actual permit. The paper can be seized according to section 94 CPC. The license is temporarily pulled according to section 111a CPC. Goal of the section is to safeguard the general traffic and public against a potential threat even if the suspect is not yet accused or judged. The pulling of the license can only be ordered by a judge. But under exigent circumstances, not the license but the seizure of the paper can also be ordered by the public prosecution office and/or "investigative personnel" (Ermittlungspersonen).

Section 110a ff. CPC concerns undercover investigators as already discussed above. Section 110b (2) Nr. 2 and 110c CPC stipulates a warrant requirement for the use of undercover investigators which involve the entering of private premises. The possible usage of undercover agents might also have an effect on people's behavioral privacy.

Observations measures aimed at the suspect or contact persons, as well as general measures carried out under the general legal basis for measures which interfere with fundamental rights in a less substantive way, will be placed best under this point.

Observation measures in general can be divided according to the term of the measure. Up until 24 hours the general provision of sections 161, 163 CPC is sufficient. These sections do not require a judge to issue a warrant or an order and can be carried out purely by the prosecution office and the police. The observation can only take place outside the home, cannot involve any listening to communication and in general does not cover the use of special observation technology except e.g. binoculars.

For observation measures of more than 24 hours section 163f CPC is applicable. The criminal offence must be of "substantial significance." Unfortunately, the legislator gave no list of such crimes, although this kind of requirement is often used throughout the procedural code.[104] It can be claimed that the threshold is most likely met when the offense is related to organized crime.[105] The measure may be ordered only where other means of establishing the facts or determining the perpetrator's whereabouts would offer much less prospect of success or be much more difficult." The legislator included this requirement, to diminish arbitrariness of investigation measures and minimize the interference with privacy rights.[106] In practice, however, such general subsidiarity rules are often not used.[107] Nevertheless, the current trend in academia points towards a consideration of the subsidiarity rules within the mandatory proportionality test

[104] See also SSW-StPO/*Plöd* § 163f Rn 5.
[105] KK-*Moldenhauer* § 163f Rn 13; *Hilger*, NStZ 2000, 561, 564; see also Meyer-Großner/*Schmitt* § 163f Rn. 8.
[106] KK-*Moldenhauer* § 163f Rn 14.
[107] Meyer-Großner/*Schmitt* § 163f Rn. 5.

(as mentioned above).[108] Courts, however, tend to accept appeals based on this reasoning if the act was completely arbitrary.[109]

Beyond the general subsidiarity rule described above, Section 163f of the CPC contains another subsidiarity rule regarding persons other than the targeted persons. The Section differentiates between targeted persons and other persons (also called contact persons). According to the first paragraph of the Section, measures "shall be admissible against other persons" (persons other than the targeted persons) only if a link between the perpetrator and the other person can be established and "the measure will lead to establishment of the facts or to determination of the perpetrator's whereabouts" and "using other means would offer much less prospect of success or be much more difficult". A targeted person is a suspect in the ongoing investigation. The contact person is not a suspect but is somehow related or in contact with the targeted person.[110]

Observation measures carried out in accordance with Section 163f of the CPC 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 3 days after ordering the measures.[111] If such an order is not confirmed by the court within 3 days, it will become ineffective.

Finally, section 100h CPC might be worthy of being mentioned in this section (Taking of Photographs; Technical Devices for Surveillance). Any surveillance measure based upon section 100h CPC can only be undertaken outside the home. Paragraph 1 Nr. 1 deals with the taking of surveillance picture were Nr. 2 just talks about other special technical devices. What counts as a "Technical Devices Intended Specifically for Surveillance Purposes" (hereinafter "Technical Device") according to Section 100h I Nr. 2 CPC, is only defined in a negative way – excluding measures 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.[112] Measures that fall under this provision include: determining the location of a person by e.g. RFID[113] or stealthy ping,[114] investigating facts and circumstances by e.g. night-vision devices[115] or drones.[116] The scope of this provision is, thus, quite broad.

The same as in Section 163f of the CPC, the low threshold of reasonable suspicion in Section 100h of the CPC is again combined with the need for a criminal offence of substantial significance. The things mentioned above, in

[108] KK-*Moldenhauer* § 163f Rn 15.
[109] Meyer-Großner/*Schmitt* § 163f Rn. 10.
[110] SK-StPO/*Wolter* § 163f StPO Rn. 9.
[111] BGHSt 44, 246; see especially Heidelberger Kommentar zur StPO/*Zöllner*, § 163f, Rn 7.
[112] BeckOK/*Hegmann*, 2012, § 100h, Rn 6 (print version); similar BGHSt 46, 266, 271.
[113] Heidelberger Kommentar zur StPO/*Gercke*, § 100h, Rn 4.
[114] BeckOK/*Hegmann*, 2012, § 100h, Rn 6 (print version).
[115] Meyer-Großner/*Schmitt* § 100h Rn. 2.
[116] Singelnstein, NStZ 14, 305, 306.

general apply here as well. The threshold should be met, when the criminal offence is of mid-tier quality and noticeably disturbs law and order (peace).[117]

4.4 Protection from interference with identity, reputation or honor

As explained above, all searches must also consider section 81d StPO. If the search interference with the sense of shame (intimacy) it can only be conducted by a physician or at least a police officer from the same gender as the searched person.[118] According to section 82d (2) CPC it is not possible to consent to a search conducted by an officer of the opposite gender. An interference with the sense of shame is assumed when the person is completely undressed in front of a person from the opposite gender, who is not a physician, or when the search includes genitals.[119]

As was also explained above, section 81h CPC allowed for serial molecular and genetic examinations ("DNA-Reihenuntersuchung"). Such mass screenings, for which cell tissue can be collected, subjected to a molecular and genetic examination to establish gender and the DNA profile and DNA profiles established can also automatically matched against the DNA profiles of trace materials. The identify of a person is put under protection by a higher threshold that has to be met: "the person affected must manifest certain significant features which may be assumed to apply to the perpetrator" and "insofar as this is necessary in order to ascertain whether the trace material(s) originated from such persons and the measure is not disproportionate to the gravity of the offence, particularly in view of the number of persons affected by the measure" (according to paragraph 1).

4.5 Protection for personal communications

The Constitutional protects personal communications in Article 10:

> *"Article 10*
> *[Privacy of correspondence, posts and telecommunications]*
>
> *(1) The privacy of correspondence, posts and telecommunications shall be inviolable.*
>
> *(2) Restrictions may be ordered only pursuant to a law. If the restriction serves to protect the free democratic basic order or the existence or*

[117] Ibid.
[118] *Ritzert*, Beck'scher Online-Kommentar StPO mit RiStBV und MiStra, Graf 24. Edition Stand: 01.02.2016, 81d Rn 1.
[119] *Ritzert*, Beck'scher Online-Kommentar StPO mit RiStBV und MiStra, Graf 24. Edition Stand: 01.02.2016, 81d Rn 5.

security of the Federation or of a Land, the law may provide that the person affected shall not be informed of the restriction and that recourse to the courts shall be replaced by a review of the case by agencies and auxiliary agencies appointed by the legislature."

Provisions in the CPC concerning communications are subject to frequent change and controversy. A complete overhaul was conducted with the Law on the Reform of Telecommunications Surveillance 21.12.2007 ("Gesetz zur Neuregelung der Telekommunikationsüberwachung v. 21.12.2007 (BGBl. 2007 I 3198"), which entered into force 1.1.2008. Especially the protection of core area of private life („Kernbereichs privater Lebensgestaltung") was introduced into section 100a IV CPC.

In consequence of the annulment of data retention related provisions, on European and national level, certain provision were not fully applicable. On 16.10.2015 the German Parliament decided upon the Law on the introduction of storage obligations and maximum retention period for traffic data („Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten"). The provisions changing the CPC, mainly sections 100g, 101a und 101b, entered into force 17.12.2015. The storage obligation, changing 113a–113g Telecommunications Acts, will enter into force latest 1.7.2017. Provieders can already obey the respective provisions, but will only obliged to do so after 1.7.2017.

The term telecommunication is not defined in the CPC, but a definition can be found in the telecommunications act under section 3 Nr. 22:

„ "telecommunications" means the technical process of sending, transmitting and receiving signals by means of telecommunications systems"

But this does not mean that the term cannot be subject to change. Since it correlates with the fundamental right of secrecy of communications in art. 10 German Constitution, it also must meet its requirement of being open for change in light of new developments.[120]

Art. 10 German Constitution only protects the communication process, starting by the sender and ending in the moment the message is received. Nonetheless, besides the actual transportation process of the data by the provider, the provisions in the CPC also cover surveillance measures conducted directly at the source. Data which is not transmitted, is not considered telecommunication, e.g. already received SMS or messages saved on the answering machine.

[120] *Graf*, Beck'scher Online-Kommentar StPO mit RiStBV und MiStra, Graf 24. Edition Stand: 01.02.2016, 100a Rn 6.

Finally section 20k BKAG (Bundeskriminalamtgesetz = Federal Criminal Police Office Law) allows for online searches and surveillance in matters that are related mainly to terrorism.

4.5.1 Search of communication providers

A search can also be conducted at the service provider. Usually, this will be based upon section 94 or 99 CPC. Such searches could concern email conversations or stored data in the cloud.

In case of emails, see section 4.5.2.1. In most of the cases a seizure will be conducted according to section 94 CPC. We will briefly elaborate about the most relevant problems with this section:

Section 94 of the CPC regulates the securing or seizing an object. Objects are all mobile or immobile items, which are somehow physically embodied or at least can be embodied and therefore controlled, like e.g. blood, urine and excrements.[121] But it also accepted that data can be seized, by copying it or seizing the harddrive itself.[122]

The legal provision of Section 94 of the CPC uses the expression „otherwise secured" as a hypernym – standing for all possible types of conduct to secure evidence including seizure.[123] The main difference between seizure and objects being otherwise secured is explained in Section 94 II of the CPC, which states that if an object is in the custody of a person and not surrendered voluntarily, the police needs to seize the object, since it cannot secure it in another and informal way. When the object is, thus, not in possession of a person that does not surrender it voluntarily, it will be otherwise secured (rather than seized). Seizure is a formal act, which need to be ordered by a judge in a warrant. Other types of securing the object (otherwise secured) are informal acts and not no require a warrant, meaning that they can be ordered directly by the prosecution office or investigative personal.

The sufficient degree of suspicion is, the lowest threshold – reasonable suspicion (Anfangsverdacht). In case of a seizure, section 98 of the CPC (regulating the warrant issued by a court) does apply and a warrant is required. Seizure may be ordered only by the court and, in exigent circumstances, by the public prosecution office and the officials assisting it.

4.5.2 Content-based investigations

Content based investigations of an ongoing telecommunication process can be based on sections 100a, 100b CPC. Usually such investigation measure includes the involvement of the service provider (see section 100b III CPC). But the respective sections also constitute a legal basis, if the police or prosecution

[121] SK-StPO/*Wohlers* § 94 StPO Rn. 20; KK-*Greven* § 94 Rn. 3; SSW-StPO/*Eschelbach* § 94 Rn 6.
[122] For emails see Graf, Beck'scher Online-Kommentar StPO mit RiStBV und MiStra, Graf 24. Edition Stand: 01.02.2016, 100a Rn 29.
[123] KK-*Greven* § 94 Rn. 1.

office uses other surveillance measures that don't require the involvement of the service provider, like taping at the source.

According to section 100b I 1, 2 CPC measures based on these sections must be ordered by a judge or in exigent circumstances ordered by the public prosecution office. Section 100b I 3 CPC states, that "an order issued by the public prosecution office shall become ineffective, if it is not confirmed by the court within three working days".

Measures pursuant to the respective sections can only be ordered if a serious criminal offence according to section 100a II CPC was conducted. The listed offences are conclusive.[124] Additionally section 100a I Nr. 2 CPC requires that "the offence is one of particular gravity in the individual case as well", meaning that although the requirement of a seruous criminal offence according to section 100a II CPC might be fullfiled, the offence in the partifuclar case must be more severe.[125]

Especially important in the context of 100a CPC is the protection of core area of private life („Kernbereichs privater Lebensgestaltung") which was introduced into section 100a IV CPC. The section reads:

If there are factual indications for assuming that only information concerning the core area of the private conduct of life would be acquired through a measure pursuant to subsection (1), the measure shall be inadmissible. Information concerning the core area of the private conduct of life which is acquired during a measure pursuant to subsection (1) shall not be used. Any records thereof shall be deleted without delay. The fact that they were obtained and deleted shall be documented.

Measures conducted pursuant to section 100a, 100b CPC can be directed against the suspect, even if the suspect is yet not identified. Other persons can be subjected to this measures, if they somehow receive or send messages for the suspect or the suspect uses their phones etc.

The order of the measures "shall be limited to a maximum duration of three months. An extension by not more than three months each time shall be admissible if the conditions for the order continue to exist, taking into account the information acquired during the investigation".[126]

Sections 100a, 100b CPC cover the taping of landline, phone, sms and other communications forms. As already mentioned in the introduction to this chapter, the protection only applies to data in transmission. Taping at the source is generally already seen as interfering with data in transmission.[127] In light of new encryption technologies and the shift to conduct all kind of communications by the internet, source taping will become more and more important in the near

[124] Urs Kindhäuser, Strafprozessrecht, 4. Auflage, 2016, § 8, Rn 77.
[125] This additional requirement was actually introduced by the legislatur in response to the supremecourt decision BVerfGE 107, 299, 322; see also Urs Kindhäuser, Strafprozessrecht, 4. Auflage, 2016, § 8, Rn 78 and footnote 136..
[126] see section 100b I 4, 5 CPC.
[127] *Graf*, Beck'scher Online-Kommentar StPO mit RiStBV und MiStra, Graf
24. Edition Stand: 01.02.2016, 100a Rn 107c.

future. Unfortunately the legislature so far did not explicitly commented on this issue, which is criticized by the scholarship.[128]

The monitoring or search of data from a distance without any communication process present, is not covered by section 100a, 100b CPC (so called "Online Durchsuchung").[129]

Taping by the provider in consequence of a court order must be conducted on the providers own expense.[130]

4.5.2.1 Mail

Surveillance measures concerning email correspondence or email in general are controversially discussed. In general, all email in the hands of the provider, is still considered to be protected by art. 10 German Constitution and therefore subject to section 100a, 100b CPC.[131] Data which is already downloaded and therefore in the hands of the subject can be seized according to section 94 CPC or can also be subject to section 110 III CPC dealing with extension of a PC search to the connected devices (see also art. 19 II Cybercrime Convention). Whether stored emails on the provider's server should be subject to sections 100a CPC or 94 CPC is being discussed. Since sections 94 ff CPC sufficiently meet the requirements posed by art. 10 German Consitution[132], and the data is not really "live" monitored, such data should be subject to sections 94 ff CPC.[133] Within the view to subject such data to sections 94 ff. CPC there is also a discussion whether section 94 ff CPC itself is sufficent enough or section 99 CPC should be used, which has slightly higher requirements (see at the bottom of this section).[134]

Some scholars argue that the explained general view is too broad and not precise enough. They prefer to divide the assessment in different phases and whether or not the email is saved on a device of the suspect or on a provider's server. Email correspondence can be devided into up seven different stages:

- Creation of the email on the suspects PC
- Sending of the Mail
- Arrival at the provider's server (of the suspect)

---

[128] *Graf*, Beck'scher Online-Kommentar StPO mit RiStBV und MiStra, Graf 24. Edition Stand: 01.02.2016, 100a Rn 5c.
[129] *Graf*, Beck'scher Online-Kommentar StPO mit RiStBV und MiStra, Graf 24. Edition Stand: 01.02.2016, 100a Rn 107c
[130] Urs Kindhäuser, Strafprozessrecht, 4. Auflage, 2016, § 8, Rn 81.
[131] Urs Kindhäuser, Strafprozessrecht, 4. Auflage, 2016, § 8, Rn 83. See also *Graf* Beck'scher Online-Kommentar StPO mit RiStBV und MiStra, Graf 24. Edition Stand: 01.02.2016, 100a Rn 28a.
[132] Klein, NJW 2009, 2996 ff.
[133] *Graf*, Beck'scher Online-Kommentar StPO mit RiStBV und MiStra, Graf 24. Edition Stand: 01.02.2016, 100a Rn 29.
[134] *Graf*, Beck'scher Online-Kommentar StPO mit RiStBV und MiStra, Graf 24. Edition Stand: 01.02.2016, 100a Rn 30.

- Sending to the receiver's provider
- Arrival at the receiver's provider
- Fatching of the email or reading it while still saved on the provider's server
- Saving on the local PC of the receiver or continued stay of the email on the provider's server

Stage 1 and 7 are not considered to be communication in the sense of sections 100a.[135] 100b CPC (consequently also not covered by art. 10 German Constitution).[136] Such emails are only protected by the general personality right based on Art. 2 I together with Art. 1 I German Constitution and can therefore be seized according to section 94 CPC.[137]

For stages 2, 4 and 6 the email or data is in transmission, thus are protected by the respective provisions.[138]

The status of stages 3 and 5 is unclear. During this stages the emails are (temporarily) saved on the providers server. During this stage the email is, even if only seconds, not perceivable by the receiver nor by the sender. Some scholars therefore argue, that during this timeframe no communication process in the technical sense is present, and therefore sections 100a, 100b CPC are not applicable.[139]

Furthermore, the protection of email stored at the provider is being debated, in case it is not used for sending and receiving email, but for conversations between different parties using the same log in. These kind of conversations can be done by leaving a draft email or sending an email to oneself. Scholars argue that in such a case sections 94 ff. CPC will be sufficient since the mail service is only used as a cloud service and thus as an external storage device.[140]

As already mentioned in the beginning of this section, emails saved at the service provider can be subjected to section 99 CPC "Seizure of Postal Items".[141] The first sentence of the provision reads:

> *"Seizure of postal items and telegrams addressed to the accused which are held in the custody of persons or enterprises providing, or*

[135] *Graf* Beck'scher Online-Kommentar StPO mit RiStBV und MiStra, Graf 24. Edition Stand: 01.02.2016, 100a Rn 27.
[136] Ibid.
[137] Ibid.
[138] *Graf* Beck'scher Online-Kommentar StPO mit RiStBV und MiStra, Graf 24. Edition Stand: 01.02.2016, 100a Rn 28.
[139] See with more footnotes *Graf*, Beck'scher Online-Kommentar StPO mit RiStBV und MiStra, Graf 24. Edition Stand: 01.02.2016, 100a Rn 28.
[140] *Graf*, Beck'scher Online-Kommentar StPO mit RiStBV und MiStra, Graf 24. Edition Stand: 01.02.2016, 100a Rn 10.
[141] The supreme court in such cases used section 99 CPC BVerfGE124, 43, 53 ff.; see also Zimmermann JA 2014, 321, 324 and critic by Kudlich GA 2011, 193, 201 ff.

collaborating in the provision of, postal or telecommunications services on a commercial basis shall be admissible."

If section 99 CPC is applied, the court orders the service provider to hand over the respective emails. The measure can also be ordered by the prosecution office but needs to be confirmed by a judge according to section 100 II CPC within three working days. The actual opening and thus reading of the email can only be conducted by the judge (section 100 III CPC). In certain circumstances the judge can transfer this authority to the prosecution office.

Different from a seizure according to section 94 CPC, the measures according to section 99 CPC need a more concrete degree of suspicion.[142]

For seizures in cases of section 94 ff. CPC see above.

4.5.2.2 Telephony (POTS) and Internet communications

Both the surveillance of POTS and Internet communications is subject to sections 100a, 100b CPC.[143]

4.5.3 Metadata-based investigations

As already mentioned above: In consequence of the annulment of data retention related provisions, on European and national level, certain provision were not fully applicable. On 16.10.2015 the German Parliament decided upon the Law on the introduction of storage obligations and maximum retention period for traffic data („Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten"). The provisions changing the CPC, mainly sections 100g, 101a und 101b, entered into force 17.12.2015. The storage obligation, changing 113a–113g Telecommunications Acts, will enter into force latest 1.7.2017. Providers can already obey the respective provisions, but will only obliged to do so after 1.7.2017.

Provision 100g CPC allows for the collection of traffic data. Traffic data is defined in section 3 I Nr. 30Telecommunications act as:

"data collected, processed or used in the provision of a telecommunications service"

The actual collecting is usually done by the providers, although section 100g I CPC also allows for live collection of traffic data. Section 100g V CPC also states that after the communication process, the collection of traffic data is

[142] Urs Kindhäuser, Strafprozessrecht, 4. Auflage, 2016, § 8, Rn 130.
[143] *Graf*, Beck'scher Online-Kommentar StPO mit RiStBV und MiStra, Graf 24. Edition Stand: 01.02.2016, 100a Rn 31a.

subject to the general provisions, thus section 94 ff CPC. Section 113b Telecommunications act was, as stated above, revised because the old storage obligation was nullified by the Supreme Court. The new provision will become binding mid 2017. Under the higher threshold requirements stated in 100g II CPC it will then be possible to also access stored traffic data.

Furthermore, section 100g III CPC allows for a "Funkzellenabfrage", which enables do determine which mobile phone was located at which time in which cell site. It is not per se the collection of location data, but much more the collection of all traffic data independent of a respective suspect within the relevant cell site.[144] Collecting e.g. 24hours of cell site X will show which traffic data of all users was produced within this cell site.

The collection of traffic data according to 100g CPC needs a warrant according to section 101a I 1 together with 100b I CPC. Section 100b I 1, 2 CPC further more states that: "In exigent circumstances, the public prosecution office may also issue an order. An order issued by the public prosecution office shall become ineffective, if it is not confirmed by the court within three working days." But section 101a I 2 CPC restricts this authority of the prosecution office to measures according to section 100g I (collecting traffic data in real time) and section 100g III "Funkzellenabfragen". For the accessing of stored traffic data, the prosecution office possesses no authority.

In case of the collection of live traffic data, the order shall be limited to a maximum duration of three months. An extension by not more than three months each time shall be admissible if the conditions for the order continue to exist, taking into account the information acquired during the investigation (see section 100b I 4 together with section 101a I CPC.

Section 101a VI CPC determines notification obligations. Section 101b CPC is similar to the old section 100g IV CPC and concerns statistic and report obligations for the law enforcement authorities.

Section 100i CPC concerns the ISMI-Catcher. In case of an offence of substantial significance, particularly one of the offences referred to in section 100a II CPC, technical means may be used to determine the device ID of a mobile and the card number (SIM) and/or the location of the mobile. Respective measures can be ordered by the court or in exigent circumstances the order may be issued by the public prosecution office.[145] An order issued by the public prosecution office shall become ineffective if it is not confirmed by the court within three working days. The order shall be limited to a maximum period of six months. An extension of not more than six months in each case shall be admissible if the conditions set out in paragraph I of the respective provision continue to exist.

[144] *Bär,* Beck'scher Online-Kommentar StPO mit RiStBV und MiStra, Graf 24. Edition Stand: 01.02.2016, 100g Rn 38.
[145] *Hegmann,* Beck'scher Online-Kommentar StPO mit RiStBV und MiStra, Graf 24. Edition Stand: 16.11.2015, 100i Rn 12.

Finally, section 100j CPC deals with “Bestandsdaten” (“Customer Data”) defined in section 3 Nr. 3 Telecommunications act as:

> *“the data of a subscriber collected for the purpose of establishing, framing*
>
> *the contents of, modifying or terminating a contract for telecommunications services”*

Besides such consumer data, data like passwords, pin, puk, etc. can also be requested (100j I 2 CPC) if statutory requirements for the use of such data have been met.

Paragraph II allows for information request regarding dynamic IP-addresses. Both consumer and IP-addresses related data can only be requested if the minimum level of suspicion of an offence is given.

Requests concerning data according to section 100j I 2 CPC (passwords, pin etc.) can only be ordered by a judge according to section 100j III CPC. In exigent circumstances the order may also be issued by the public prosecution office or by the officials assisting it. In this case a court decision is to be sought without delay. The first to third sentences shall not apply if the person concerned already has or must have knowledge of the request for information or if the use of the data has already been permitted by a court decision. For the other data like IP addresses or consumer data, such a warrant is not necessary.

Paragraph IV concerns notification obligations and V determines the obligation for the service provider to obey such an order by the courts.

4.5.4 Stored communications data

See elaborations in previous chapters. Stored data in general is seizable according to section 94 ff. CPC. If it concerns mail and similar conversations, section 100a, 100b CPC might be necessary.

For metadata see previous section.

4.5.5 Oral interception (face to face communications)

Oral interception in face to face communications is separated between the so called “kleine Lauschangriff” (small eavesdropping operation) and “große Lauschangriff” (big eavesdropping operation).

The kleine Lauschangriff is regulated in section 100f CPC and concerned eavesdropping of the not publicly spoken word outside the home. The große Lauschangriff however is regulated in section 100c CPC and concerns eavesdropping within the home.

According to section 100f IV together with section 100b I CPC, the kleine Lauschangriff is subject to a warrant requirement. In exigent circumstances, the public prosecution office and the officials assisting it shall be authorized to order such measures. The order of the measures "shall be limited to a maximum duration of three months. An extension by not more than three months each time shall be admissible if the conditions for the order continue to exist, taking into account the information acquired during the investigation".[146] Regarding the degree of suspicion and weight of the respective offence section 100f I CPC states:

> *" (...) if certain facts give rise to the suspicion that a person, either as perpetrator or as inciter or accessory, has committed a criminal offence referred to in Section 100a subsection (2), being a criminal offence of particular gravity in the individual case as well, or, in cases where there is criminal liability for attempt, has attempted to commit such an offence, and other means of establishing the facts or determining the accused's whereabouts would offer no prospect of success or be much more difficult."*

Only the suspect can be the target of such measures. "Such a measure may only be ordered against other persons, if it is to be assumed, on the basis of certain facts, that they are in contact with the suspect or that such contact will be established, the measure will result in the establishment of the facts or the determination of an suspect's whereabouts, and other means of establishing the facts or determining an suspect's whereabouts would offer no prospect of success or be much more difficult."[147] "The measure may be implemented even if it unavoidably affects third persons."[148]

Unfortunately, the provision does not make any reference to the already explained core of private life. In light of the threats posed to fundamental rights by measures conducted on the base of section 100f CPC, scholarship argues that section 100a IV CPC should be applied analogue.[149]

Preparation measures, like opening the car to implement bugs are covered by the provision.[150]

---

[146] see section 100b I 4, 5 CPC.
[147] see section 100f II.
[148] see section 100f III.
[149] Urs Kindhäuser, Strafprozessrecht, 4. Auflage, 2016, § 8, Rn 93; Singelnstein, NStZ 2014, 305, 311.
[150] Urs Kindhäuser, Strafprozessrecht, 4. Auflage, 2016, § 8, Rn 94.

The grosser Lauschangriff, regulated in section 100c CPC bears the requirements for communication surveillance within the home. The correlating fundamental right of the home can be found in art. 13 (especially III-IV) German Constitution. Optical surveillance measures are not covered by the provision.[151]

According to section 100d I CPC measures pursuant to section 100c CPC can only be ordered by the division of the Regional Court stipulated in section 74a IV of the Courts Constitution Act in the district where the public prosecution office is located. Furthermore: "in exigent circumstances the order may also be issued by the presiding judge. His order shall become ineffective unless confirmed by the criminal division within three working days. The order shall be limited to a maximum duration of one month. An extension of the measure for subsequent periods of up to one month shall be admissible providing the conditions for the measure continue to exist, taking into account the information acquired during the investigation. If the duration of the order has been extended for a total period of six months, the Higher Regional Court shall decide on any further extension orders."

The measures may only be directed against the accused and only implemented on his/her private premises. Section 100c III CPC than continues to allow for measures on the private premises of other people, if it can be assumed that the accused is present of the premises and applying the measure on the accused's premises alone will not lead to the establishment of the facts or the determination of a co-accused person's whereabouts. The measures may be implemented even if they unavoidably affect third persons.

For information about the term home see the elaborations under protection of places.

According to section 100d V CPC:

> *Personal data obtained by means of acoustic surveillance of private premises may be used for other purposes subject to the following conditions:*
>
> *1. The usable personal data obtained through a measure pursuant to Section 100c may be used in other criminal proceedings without the consent of the persons being monitored only for the purposes of resolving a criminal offence in respect of which measures pursuant to Section 100c could have been ordered, or to establish the whereabouts of a person accused of such a criminal offence.*
>
> *2. The use of personal data obtained through a measure pursuant to Section 100c, even such data as is acquired pursuant to Section 100c subsection (6), first sentence, second part of the sentence, for the purposes of averting danger is only admissible to avert an existing danger of death in an individual case or to avert an imminent danger to the life or liberty of a person or to objects of significant value which*

[151] Eisenberg NStZ 2002, 638; Urs Kindhäuser, Strafprozessrecht, 4. Auflage, 2016, § 8, Rn 101.

serve to supply the population, are of culturally outstanding value, or are referred to in section 305 of the Criminal Code. The usable personal data obtained through a measure pursuant to Section 100c may also be used to avert an imminent danger to other significant assets in individual cases. If the data is no longer required for the purposes of averting the danger or for a pre-judicial or court examination of the measures implemented to avert the danger, recordings of such data are to be deleted without delay by the institution responsible for averting the danger. The fact of deletion is to be documented. Insofar as deletion is postponed merely for an eventual pre-judicial or court examination, the data may be used solely for this purpose; access is to be denied for any use for other purposes. Service provided by the Federal Ministry of Justice and Consumer Protection in cooperation with juris GmbH – www.juris.de Page 41 of 203

3. Insofar as usable personal data has been obtained by means of a respective police measure, such data may not be used in criminal proceedings without the consent of the person under surveillance by virtue of such measure, except for the purpose of clearing up a criminal offence in respect of which the measure pursuant to Section 100c could have been ordered, or to determine the whereabouts of a person accused of such criminal offence.

Section 100c VI CPC also excludes all information gathered by the respective measures in cases referred to in section 53a CPC (Lawyers etc.).

Different then the respective section for the kleine Lauschangriff, section 100c V CPC, makes reference to the core of private life, similar to the already explained section 100a IV CPC.

Paragraph V reads:

"The interception and recording is to be interrupted without delay if during 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. If a measure pursuant to the first sentence has been interrupted, it may be re-continued subject to the conditions set out in subsection (4). If in doubt, a court decision on the interruption or continuation of the measures should be sought without delay; Section 100d subsection (4) shall apply mutatis mutandis"

And is supplemented by paragraph VII:

"Insofar as a prohibition on use pursuant to subsection (5) is conceivable, the public prosecution office shall obtain a decision without delay from the court which made the order, as to whether the information acquired may be used. Insofar as the court does not approve such use, the decision shall be binding for the further proceedings."

Finally, section 100e CPC determines report obligations.

5. The Protection of Data

Section 163d CPC provides a legal bases to create a database, collect and process data. The so called Schleppnetzfahndung (Dragnet surveillance/search), allows to collect for e.g. data at mass controls (when passing the border) which is difficult to be immediately checked by the authorities. Through creating small data bases, it is possible to run the data against already existing criminal data bases and thereby catching offenders.

> *"Measures of the nature designated in subsection (1) may be ordered only by the judge, in exigent circumstances also by the public prosecution office and the officials assisting it (section 152 of the Courts Constitution Act). If the public prosecution office or one of the officials assisting it has made the order, the public prosecution office shall apply for judicial confirmation of the order without delay" (section 163d II CPC). "It shall be limited to a particular area and to a maximum period of three months. One extension of not more than three further months shall be admissible if the conditions designated in subsection (1) continue to apply"* (paragraph III).

According to paragraph III "the order shall be given in writing. It shall describe the person whose data are to be stored as precisely as possible, by reference to particular features or characteristics, in the light of the information available about the suspect or suspects at the time of the order."

Furthermore a more qualified suspicion degree for certain criminal offences must be given.[152]

According to section 163d IV CPC the data must be deleted after the term or when the requirements are not fulfilled anymore. Furthermore, notification requirements are regulated.

Information relevant for this provision are data relating to the identity of a person (Name, Birthdate, Birthplace and Address) and circumstances which could help to clear up the respective criminal offence.[153]

Other relevant provisions are sections 98a, b CPC. The so called "Rasterfahndung" allows for cross-checking different databases. Important is that here personal data is automatically matched against other data " in order to exclude individuals who are not under suspicion or to identify individuals who manifest other significant characteristics relevant to the investigations." This measure may be ordered only where other means of establishing the facts or

[152] Urs Kindhäuser, Strafprozessrecht, 4. Auflage, 2016, § 8, Rn 3.
[153] *von Häfen*, Beck'scher Online-Kommentar StPO mit RiStBV und MiStra, Graf24. Edition Stand: 01.02.2016, 163d, Rn 2.

determining the perpetrator's whereabouts would offer much less prospect of success or be much more difficult

Required is a criminal offence of substantial significance (see list in the respective section). Furthermore section 98b I CPC states: "Matching and transmission of data may be ordered only by the court and, in exigent circumstances, also by the public prosecution office. Where the public prosecution office has made the order, it shall request court confirmation without delay. The order shall become ineffective if it is not confirmed by the court within three working days."

Upon the request by the authorities the storing agency will extract the required data from their database and transmit it to the authorities (prosecution office) (see section 98a II CPC). Where data was transmitted on data media these shall be returned without delay once matching has been completed. Personal data transferred to other data media shall be deleted without delay once it is no longer required for the criminal proceedings (section 98b III CPC).

In that context another provision is section 98c CPC. Here data is compared to clear up a criminal offence as well. In order to clear up a criminal offence or to determine the whereabouts of a person sought in connection with criminal proceedings, personal data from criminal proceedings may be automatically matched with other data stored for the purposes of criminal prosecution or execution of sentence, or in order to avert danger. The data used is data related to criminal proceedings, e.g. INPOL (Database for the Police "Informationssystem of the Police") or SPUDOK ("Spurendokumentation", freely translated "Tracerecording"). Different from the "Rasterfahndung" measures undertaken pursuant to section 98c CPC are directed against a specific person.[154] Since the relevant data is already data collected according to prosecution purposes, no court order etc. is relevant for its use. [155]

Section 163b and 163c CPC dealing with the establishment of Identity and duration of a consequential custody (See above).

Another relevant provision might be section 81b CPC dealing with photographs and fingerprints. The provision states: "Photographs and fingerprints of the accused may be taken, even against his will, and measurements may be made of him and other similar measures taken with regard to him insofar as is required for the purposes of conducting the criminal proceedings or of the police records department."

Section 81b CPC only applies for the accused and cannot be used to gather fingerprints etc. from the suspect (see above for more information).[156]

Another relevant section is 111 dealing with the installation of checkpoints to publicly accessible places. Section 111 CPC is, as the majority of all provisions in the CPC, a repressive measure. The provision does only apply when "certain facts substantiate the suspicion that a criminal offence" mainly related to

[154] Urs Kindhäuser, Strafprozessrecht, 4. Auflage, 2016, § 8, Rn 8.
[155] Urs Kindhäuser, Strafprozessrecht, 4. Auflage, 2016, § 8, Rn 8.
[156] Urs Kindhäuser, Strafprozessrecht, 4. Auflage, 2016, § 8, Rn14.

terrorism. In such cases “checkpoints may be established on public roads, squares and at other publicly accessible places” and “At a checkpoint all persons shall be obliged to establish their identity and to subject themselves or objects found on them to a search” (see above for more information).

Only indirect affecting behavioral privacy is section 163e CPC Police Observation. The goal of measures taken in accordance with section 163e CPC is to create a full movement pattern of the accused or his/her contact person.[157] Already existing police controls are used to “search” for the accused. The measures are aimed at the accused and establishing his/her identity, travel pattern or route, means of transportation, carried goods and companions (see above).[158]

In certain circumstances the Procedural Code allows for an arrest, although no arrest warrant was issued prior. The relevant sections of the code are 127 I and II, 127 b and 163 b I, all concerning a “provisional arrest” (see above).

Already mentioned above (see 4.1.1.), section 81a CPC deals with physical examinations and blood tests. On the samples taken according section 81a I CPC, molecular-genetic examinations can be undertaken according to section 81e and 81f CPC (see above). Section 81g CPC works as a legal base to create a DNA-Databank, which is supposed to help identifying suspects in future crimes (see above).[159]

According to section 101 CPC specific procedural requirements exist for undercover measures. Paragraph 1 states: “) Unless otherwise provided, measures pursuant to Sections 98a, 99, 100a, 100c to 100i, 110a and 163d to 163f shall be subject to the following conditions.” Paragraph III: “) Personal data which was acquired by means of measures pursuant to subsection (1) is to be labelled accordingly. Following a transfer of the data to another agency, the labelling is to be maintained by such agency.” According to IV certain persons shall be notified in cases of measures conducted according to the provisions mentioned in paragraph 1. Paragraph VIII states: “Personal data acquired by means of the measure which is no longer necessary for the purposes of criminal prosecution or a possible court review of the measure shall be deleted without delay. The fact of the deletion is to be documented. Insofar Service provided by the Federal Ministry of Justice and Consumer Protection in cooperation with juris GmbH – www.juris.de Page 47 of 203 as deletion of the data has been deferred merely for the purposes of a possible court review of the measure, the data shall not be used for any other purpose without the consent of the persons concerned; access to the data is to be restricted accordingly.”

Additionally, several provision themselves have deletion requirements or notification requirements. See especially sections regarding telecommunication surveillance.

[157] Urs Kindhäuser, Strafprozessrecht, 4. Auflage, 2016, § 8, Rn. 18.
[158] Urs Kindhäuser, Strafprozessrecht, 4. Auflage, 2016, § 8, Rn. 19.
[159] *Ritzert*, Beck'scher Online-Kommentar StPO mit RiStBV und MiStra, Graf 24. Edition, 81g Rn Before 1.

6. The protection of things

6.1 Seizure and search of things

Section 94 of the CPC regulates the securing or seizing an object. Objects are all mobile or immobile items, which are somehow physically embodied or at least can be embodied and therefore controlled, like e.g. blood, urine and excrements.[160] But it also accepted that data can be seized, by copying it or seizing the hard drive itself.[161]

The legal provision of Section 94 of the CPC uses the expression „otherwise secured" as a hypernym – standing for all possible types of conduct to secure evidence including seizure.[162] The main difference between seizure and objects being otherwise secured is explained in Section 94 II of the CPC, which states that if an object is in the custody of a person and not surrendered voluntarily, the police needs to seize the object, since it cannot secure it in another and informal way. When the object is, thus, not in possession of a person that does not surrender it voluntarily, it will be otherwise secured (rather than seized). Seizure is a formal act, which needs to be ordered by a judge in a warrant. Other types of securing the object (otherwise secured) are informal acts and not no require a warrant, meaning that they can be ordered directly by the prosecution office or investigative personal.

The sufficient degree of suspicion is, the lowest threshold – reasonable suspicion (Anfangsverdacht). In case of a seizure, section 98 of the CPC (regulating the warrant issued by a court) does apply and a warrant is required. Seizure may be ordered only by the court and, in exigent circumstances, by the public prosecution office and the officials assisting it.

The actual search of the object itself is regulated in section 102 ff. CPC and the examination of documents and data in section 110 CPC. For both provisions see please the elaborations in the above sections and below 6.1.2.. Objects are such things that the suspect or the contact person is carrying with them or on them. It is not required that they own the objects, but that he/she possesses them.[163]

6.1.1 Weapons, drugs and contraband

Besides section 94 ff CPC, in case of weapons, drugs and contraband sections 111b ff. CPC might also be relevant. Where section 94 ff. CPC is aimed at

[160] SK-StPO/*Wohlers* § 94 StPO Rn. 20; KK-*Greven* § 94 Rn. 3; SSW-StPO/*Eschelbach* § 94 Rn 6.
[161] For emails see *Graf*, Beck'scher Online-Kommentar StPO mit RiStBV und MiStra, Graf 24. Edition Stand: 01.02.2016, 100a Rn 29.
[162] KK-*Greven* § 94 Rn. 1.
[163] *Hegmann*, Beck'scher Online-Kommentar StPO mit RiStBV und MiStra, Graf 24. Edition Stand: 01.09.2015, 102 Rn 12.

seizing evidence, sections 111b ff. CPC is aimed at seizing objects that there are grounds to assume that the conditions for their forfeiture (sections 77a-e German Criminal Code) or for their confiscation (sections 74 ff. German Criminal Code) have been fulfilled. The securing of objects pursuant to section 111b CPC can only be conducted by seizing the objects. For a better understanding see 6.1.

6.1.2 Computers and cell phones

We have to differentiate between the search of the device according to sections 102 ff. CPC or the actual "reading" of the data according 110 CPC. According to section 102 ff. CPC the PC or Mobile phone may be activated, powered on etc. and be searched. In contrast to section 102 ff. CPC, section 110 CPC concerns the actual examination of the data. The provision talks about papers but it is established that electronically or otherwise saved data are covered by the provision.[164] The examination is actually a step before the seizure of the data. But often it is not possible to scan all required data in a short time, therefore it is also allowed to take the device or data to the respective station for further examination.

Important to note is that the examination is part of the actual search (see section 110 I CPC). Since the actual search according to section 102 ff. CPC needs a warrant according to section 105 CPC, section 110 CPC is indirectly covered as well. For more details regarding section 105 CPC see the sections above.

Since all measures must always be proportionate and within the framework of the purpose for the search, a complete search, examination or seizure of all data and documents can be judged disproportionate.

Another ground for a search can be found in section 163b CPC. The first sentence of the provision states: "If somebody is suspected of a criminal offence the public prosecution office and the officials in the police force may take the measures which are necessary to establish his identity". Covered from such measures are also the search of objects carried by the suspect, but only in so far as it helps to establish the identity of the suspect. But since section 108 CPC allows for accidental discoveries, and section 163b CPC does not possess a warrant requirement, the search of devices to establish the identity of the suspect might be subject to misuse by authorities. The search of the home is not covered by the provision.[165] Arguably, the device possess almost as much information if not more than the home about the individual, therefore this provision should be interpreted restrictively.

[164] *Hegmann,* Beck'scher Online-Kommentar StPO mit RiStBV und MiStra, Graf 24. Edition Stand: 01.02.2016, 110 Rn 3.
[165] *von Häfen,* Beck'scher Online-Kommentar StPO mit RiStBV und MiStra, Graf 24. Edition Stand: 01.02.2016, 163b Rn 9.

6.1.3 Documents

See above, especially sections 102 ff CPC togther with 110 CPC. For the seizure 94 ff. CPC.

7. Conclusion

t.b.a.