Information Society and Penal Law
German National Report
to the Fourth Section of the XIXth Congress of Penal Law*

Florian JEßBERGER*

(A) Preliminary Remarks

A number of specific offences dealing with cybercrime exist under German law (see below). However, the provisions dealing with jurisdiction, mutual legal assistance, and other relevant procedural matters only exceptionally reflect the particular challenges of cyberspace. Thus, a key problem of tackling cyber crime under German law is to determine whether and under what circumstances the general provisions apply (or do not apply). At the same time, German law on cybercrime is significantly determined by international and/or European rules. Germany is a state party to the Council of Europe's Convention on Cybercrime (entered into force 5 November 2008) and the Additional Protocol (entered into force 16 March 2011). Since Germany is a Member State of the European Union, the various EU instruments dealing with jurisdiction, mutual legal assistance and other procedural matters apply.

In order to provide for the information requested by the general rapporteur, the report follows closely the structure of the questionnaire. The questionnaire points to the major area of concern: localisation – of conduct, effects and evidence on the one hand and of authority (to regulate/prescribe and to enforce) on the other.

(B) Jurisdictional Issues

The rules on criminal jurisdiction are laid down, in particular, in Sections 3 to 7 and 9 of the German Criminal Code (StGB).

The principle of territoriality constitutes the basic principle of German criminal jurisdiction. According to Section 3 StGB, German criminal law applies to acts which were committed on German territory. An offence is deemed to have been committed in every place where the offender acted or in which the result if it is an element of the offence occurred (Section 9 (1) StGB; principle of ubiquity).

In addition to the principle of territoriality, other principles of jurisdiction, such as the flag principle (Section 4 StGB), the protection principle (e.g. Section 5 No. 1 – No. 5 StGB), the active personality principle (e.g. Section 5 No. 8 lit. b StGB, Section 7 (2) No. 1 StGB), the passive personality principle (e.g. Section 5 No. 6 StGB, Section 7 (1) StGB), the principle of vicarious administration of justice (Section 7 (2) No. 2 StGB) and the principle of universality (e.g. Section 1 VStGB and, arguably, Section 6 StGB) apply.

In the present context, two provisions deserve special mention:

First, according to Section 6 No. 6 StGB German criminal law applies, regardless of the law of the place of commission, to the dissemination of pornographic writings in cases under Sections 184a and 184b subsections (1) to (3), also in connection with Section 184c sentence 1. This provision extends German criminal jurisdiction universally to acts involving "hard pornography" (violence, animals, children). The element "writings" (see also Section 11 (3)) also covers data storage media. Given that trafficking in pornographic materials is a relatively widespread form of cybercrime, the fact that German criminal law applies universally in this regard may be noteworthy (for a critical view on this see below).

Second, according to Section 9 StGB an offence is committed in every place where the offender acted or, in the case of an omission, should have acted, or in which the result which is an element of the offence occurred or should have occurred according to the understanding of the offender. According to this principle of ubiquity, a crime is committed in Germany even if the offender acted outside Germany or if the consequences of the crime occur outside Germany only. The significance of this far-reaching concept with regard to cybercrime is still not fully clear (see below).

(1)

(a) How does your country locate the place of the commission of a crime in cyberspace?

Under German law there is no special rule for the determination of the locus of a crime committed in cyberspace. Under Section 9 of the German Criminal Code an offence is committed in every place where the offender acted or, in the case of an omission, should have acted, or in which the result which is an element of the offence occurred or should have occurred according to the understanding of the offender.

Hence, despite certain particularities specific to crimes committed in cyber space, both, the place where the offender acted ("Handlungsort") and the place where the result occurred ("Erfolgsort"), are decisive for the question where the respective act has been committed. A place where the offender acted ("Handlungsort") is any place where he or she performs an activity with a view to the materialization of the elements of the offence ("eine auf Tatbestandsverwirklichung gerichtete Tätigkeit entfaltet oder versucht").

---

* Important notice: this text is the last original version of the national report sent by the author. The Review has not assured any editorial revision of it.

* Professor of Criminal Law, Universität Hamburg.The author wishes to gratefully acknowledge the support of Eva Bohle, LL.M. (UWC) and Sarah Imani, LL.M. (NYU) in the preparation of this paper.

For instance, a person who uploads data to the internet from outside Germany does, as a rule, not establish such a "Handlungsort" in Germany. In this case only the place in the country where the offender is physically present at the time of uploading the data defines the place where the offender acted ("Handlungsort"). This assumption holds true even for the scenario that the data is provided for cognition specifically on German territory and it holds true regardless whether the server to which the data is uploaded is located abroad or in Germany.

The question, whether and to what extent a place of result ("Erfolgsort") in the above-mentioned sense can be assumed for crimes committed in cyberspace has not yet been answered conclusively and hence remains contentious. There is agreement that result crimes ("Erfolgsdelikte") have a place of commission at the place where the result occurs; for instance, defamation ("Beleidigung") which is a crime under Section 185 StGB is committed wherever the victim perceives the defamatory information - regardless of whether the offender acts via the internet or via any other means of communication. According to the majority view, this rule is applicable also to crimes of concrete endangerment ("konkrete Gefährdungsdelikte"). Here, a place of result ("Erfolgsort") is established where the concrete endangerment of the legally protected interest ("Rechtsgut") is caused.

Whether this equally applies to offences of abstract endangerment ("abstraktes Gefährdungsdelikt"), is a matter of dispute; the German Federal Court of Justice (Bundesgerichtshof) left this point open (see below). The question is relevant in our context since a significant number of internet-specific crimes are construed as crimes of abstract endangerment. According to some authors, offences of abstract endangerment have a locus delicti at every place where the abstract endangerment potentially can transform into a real (concrete) danger. Other authors argue that offences of abstract endangerment have no place of result at all.

For another type of offences, which, in a way, are located between offences of abstract endangerment and offences of concrete endangerment, the so-called offences of "abstract-concrete endangerment", the German Federal Court of Justice (Bundesgerichtshof) held in a landmark decision of 12 December 2000 ("Toeben", BGHSt 46, 212), that the crime of "incitement to hatred" ("Volksverhetzung", Section 130) may be qualified as a territorial offence ("Inlandstat") even if the offender physically acted abroad only.

There is agreement in German scholarship that the general principles of jurisdiction need to be adjusted to the specific circumstances of cyberspace. It should be noted that, for instance, the application of the general provisions and principles concerning the establishment of the locus delicti may lead to a de facto universal reach of German criminal law under the principle of territoriality – universal jurisdiction in disguise. Considerations based on international law related and practical reasons as well as on principles of criminal law mandate a restrictive interpretation and application of the jurisdictional rules: according to what specific criteria, however, is a matter of dispute. Suggestions include technology-based criteria (e.g. push- vs. pull technologies), content-based criteria (such as the language of an information distributed via internet), perpetrator-based criteria (such as the mens rea), or the general requirement of an additional link of the crime to Germany.

(b) Does your national law consider it necessary and possible to locate the place where information and evidence is held? Where is the information that one can find on the web? Is it where the computer of the user is physically present? Is it there where the provider of the network has its (legal or factual) seat? Which provider? Or is it the place where the individual who made the data available? If these questions are not considered to be legally relevant, please state why.

With regard to the necessity to locate the place where information and evidence is held, two perspectives should be distinguished:

The first perspective concerns the question whether and in what regard the location of information and evidence is relevant from a jurisdictional point of view. From this perspective, as a rule, the location of information/evidence is not decisive. Whether the offence is covered by the ambit of German criminal law depends on where the offender acted or where the result, if any, occurred. If the offender physically acted on German territory, German criminal law applies regardless of the fact whether the information is located on a server in Germany or abroad.

The second perspective concerns the relevance of the location of information from a procedural/ evidentiary point of view. From this perspective, the location of information/ evidence is decisive. As will be explained in more detail below, German authorities are entitled to procedural measures only with regard to information/evidence which is located on German territory. For instance, a seizure or a data query concerning information located on a server outside Germany would be illegal since this would violate the sovereignty of the state where the server is located. A major practical problem concerns the fact that it is often difficult to determine *where* specific information is located.

(2) Can cyber crime do without determination of the locus delicti in your criminal justice system? Why (not)?

Generally, the determination of the locus delicti is indispensible for the determination of the applicability of German criminal law (see above) based on the principle of territoriality pursuant to Section 3 and 9 StGB. While German criminal law applies to all offences committed on German territory, it applies to extraterritorial offences only under specific circumstances set out, in particular, in Sections 4 to 7 of the German Criminal Code.

However, the precise determination of the place of commission is, from a practical point of view, not necessary in those cases where German criminal law is applicable also to extraterritorial behaviour anyway. If the other jurisdictional requirements (e.g. German nationality of the offender or victim, specific crimes listed in Sections 5 and 6) are met, then German criminal law applies regardless of the place of commission. It should be noted, however, that as a matter of procedural law, the determination of the place of

commission may still be relevant in those cases (see Section 153c of the Code of Criminal Procedure, providing for prosecutorial discretion in cases of extraterritorial jurisdiction).

(3) Which jurisdictional rules apply to cyber crime like hate speech via internet, hacking attacks on computer systems etc? If your state does not have jurisdiction over such offences, is that considered to be problematic?

There are no specific jurisdictional rules applicable to crimes of hate speech (sec. 130) or hacking attacks (secs. 202a, 202b, 202c, 303a, 303b); for the general rules, see above.

(4) Does your national law provide rules on the prevention or settlement of conflicts of jurisdiction? Is there any practice on it?

There are no specific rules in German law which deal with the prevention or settlement of conflicts of jurisdiction.

However, the *ne bis in idem* principle (which provides for a very rudimental mechanism of conflict resolution: first come first serve) applies with regard to prosecutions in other EU-Member States. Furthermore, on the level of procedural law, Section § 153c of the German Code of Criminal Procedure discharges mandatory prosecution with regard to crimes committed abroad. This allows for prosecutorial discretion also taking account of the fact that the same offence has been or is being prosecuted in another jurisdiction.

Beyond that, and while Germany is not a state party to the Council of Europe's Convention on the Transfer of Proceedings in Criminal Matters of 15 May 1972, a number of international instruments are applicable which implement consultation mechanisms with a view to the settlement of conflicts of jurisdiction (e.g. Article 21 UNTOC, Article 22(5) CCC).

(5) Can cyber crime do without jurisdictional principles in your criminal justice system, which would in essence mean that national criminal law is applicable universally? Should this be limited to certain crimes, or be conditional on the basis of a treaty?

According to the majority of writers in Germany, the unilateral extension of the applicability of domestic laws is possible, however, only within the boundaries of international law. Also the German Federal Court of Justice emphasized that the sovereignty of other states and the principle of non-intervention are to be respected. Most writers agree that, from the perspective of (customary) international law, true or so-called unconditional universal jurisdiction is warranted only with regard to genocide, crimes against humanity, and war crimes. While, theoretically, it would be an option to agree on a universal treaty providing for (universal) jurisdiction over cybercrime, there is agreement that, as things stand now, universal jurisdiction over cybercrime (which does not, say amount to a war crime at the same time) would not be in conformity with international law. Furthermore, the simple fact that it is difficult to determine the locus delicti of crimes committed in cyberspace is certainly no convincing argument to allow for universal jurisdiction. Also, according to many writers, a treaty-based exercise of jurisdiction (which can per definitionem apply only *inter partes*) is not (or only in the very rare cases of truly universal treaties) to be mixed up with universal, geographically unrestricted jurisdiction.

Thus, from the perspective of international law, universal jurisdiction extends to cybercrime only exceptionally, if at all (possibly regarding cyberwarfare/war crimes and incitement to genocide).

Given this, Section 6 No. 6 StGB (see above; which has been enacted in 1940 before the background of the 1910 Convention) has to be interpreted restrictively and in conformity with international law ("völkerrechtskonforme Reduktion").

(C) Substantive Criminal Law and Sanctions

There is a number of specific offences under German law which may be classified as "cyber crime"-offences. According to the protected legal interests these offences can be categorized as follows:[1]

- offences protecting the integrity of ICT-systems (e.g. §§ 202a, 202b, 205; 303a, 303b, 303c, 202c);
- offences protecting privacy (inter alia §§ 202, 203, 206);
- offences protecting property against attacks using false computer data ("Identitätsdiebstahl und –missbrauch"); §§ 263a, 265a, 269, 270, 274);
- offences protecting against illegal content (pornography, hate crimes, inter alia §§ 184 et seq.; 86 ff., 130, 284); and
- offences protecting intellectual property rights (§§ 106, 108a, 108b UrhG).

Which cyber crime offences under your national criminal justice system do you consider to have a transnational dimension? To what extent do definitions of cyber crime offences contain jurisdictional elements? To what extent do general part rules on commission, conspiracy or any other form of participation contain jurisdictional elements?

While, by their very character and given the global nature of cyberspace, cybercrimes certainly have a transnational dimension, under German law "cyber crime offences" (see above) do not expressly include a transnational element in the definition of the offence. Generally, the definitions of crimes in German law do contain jurisdictional elements only exceptionally (see for example Section 86(1): "disseminates within Germany"). As a rule, the jurisdictional reach of the offences under German law unfolds only if the definitions of crimes are read together with the general rules on jurisdiction (Sections 3 et seq.).

[1] Cf. *Sieber*, Gutachten (2012); *Vervaele*, Annex 1 (2012).

Do you consider cyber crime offences a matter that a state can regulate on its own? If so, please state how a state may do that. If not, please state why it cannot do that.

Every state is entitled to regulate cyber crime offences on its own. Of course, the general limitations on criminalizing human behaviour apply; in our context and in addition to limitations which derive from criminal law principles, principles of international law (see above) are of particular significance for the limitation of the authority to regulate. Ultimately, however, it is not so much a legal but a practical matter that international harmonisation and cooperation should be integral parts of a strategy to combat cybercrime.

Does your national criminal law provide for criminal responsibility for (international) corporations/providers? Does the attribution of responsibility have any jurisdictional implications?

German criminal law does not provide for the criminal responsibility of corporations (but see for "administrative responsibility", Section 130 of the Gesetz über Ordnungswidrigkeiten).

(Non-criminal) liability of providers is regulated in Sections 7 et seq of the Telemedia Act. According to Section 7 so-called content-providers shall be responsible for their own information which they keep ready for use. Sections 8 and 9 contain specific rules for so-called access-providers, hosting-providers, and caching and proxy-providers. Access-providers are not responsible for external content that they transmit/ communicate/ convey through an electronic communication network or to which they merely offer access provided they did not initiate the transmission or select the addressee of the transferred content and did not select or alter the transferred information.

Hosting providers are not responsible for external information that they host for users provided they do not have knowledge of illegal conduct or information and in case of claims for compensatory damages did not have knowledge of facts or circumstances that make the illegal act or information apparent, or [they are equally not responsible] provided they took action without any further hesitation in order to remove the information or close the access to this information as soon as they had knowledge.

Attention should also be paid to the provisions of the European Council's and Parliament's e-commerce directive 2000/31/ of 8 June 2000 ("Richtlinie über den elektronischen Geschäftsverkehr"); it entails grounds for exclusion of criminal responsibility that are relevant throughout the European Union including Germany, namely the exclusion of criminal responsibility for access providers and the limitation of liability for hosting-providers to cases of actual knowledge (Art. 14).

(D) Cooperation in Criminal Matters

In Germany, the law on mutual legal assistance is laid down in the Act on International Cooperation in Criminal Matters of 23 December 1982 (IRG).

According to its Section 1 (3), provisions of international treaties take precedence over the provisions of the IRG. Thus, in principle, the Act becomes relevant only where international agreements do not exist or are not directly applicable. International treaties within the meaning of Section 1 (3) IRG mean bilateral agreements, in particular with non-European states,[2] multilateral agreements on mutual legal assistance, in particular within the Council of Europe[3] and the European Union,[4] as well as conventions on specific

[2] E.g. Treaty of 19 July 1966 between the Federal Republic of Germany and the Republic of Tunisia concerning Extradition and Mutual Legal Assistance in Criminal Matters; Treaty between the Federal Republic of Germany and Canada concerning Extradition of 11 July 1977 as amended by the Supplementary Treaty of 13 May 2002; Treaty of 20 June 1978 between the United States of America and the Federal Republic of Germany as amended by the Supplementary Treaties of 21 October 1986 and 18 April 2006; Treaty of 14 April 1987 between Australia and the Federal Republic of Germany concerning Extradition; Treaty of 21 June 2001 between the Federal Republic of Germany and the Republic of India on Extradition; Treaty of 14 October 2003 between the Federal Republic of Germany and the United States of America on Mutual Legal Assistance in Criminal Matters as amended by the Supplementary Treaty of 18 April 2006; Treaty of 13 May 2002 between Canada and the Federal Republic of Germany on Mutual Assistance in Criminal Matters; Agreement between the European Union and Japan on Mutual Legal Assistance in Criminal Matters, 30 November 2009, OJ 2010 L 39/20; see *Hackner/Schierholt* Internationale Rechtshilfe in Strafsachen, 2. Auflage (2012), marg. no. 10.

[3] E.g. European Convention on Extradition of 13 December 1957; European Convention on Mutual Assistance in Criminal Matters of 20 April 1959; Convention on the Transfer of Sentenced Persons of 21 March 1983; some of them supplemented by additional protocols and bilateral additional conventions.

[4] E.g. Council Act of 29 May 2000 establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union; Council Framework Decision of 13 June 2002 on the European Arrest Warrant and the Surrender Procedures between Member States; Council Framework Decision of 22 July 2003 on the execution in the European Union of orders of freezing property or evidence; Council Framework Decision of 24 February 2005 on the application of the principle of mutual recognition to financial penalties; Council Framework Decision of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union; Council Framework Decision of 18 December 2008 on the European evidence warrant for the purpose of obtaining objects, documents and data for use in proceedings in criminal matters; see also Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders of 19 June 1990 and the Convention on the stepping up of cross-border cooperation, particularly in combating terrorism, cross-border crime and illegal migration of 27 May 2005 (Prüm Convention) whose core elements were picked up by Council Decision of 23 June 2008 on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime; *Hackner/Schierholt* Internationale Rechtshilfe in Strafsachen, 2. Auflage (2012), marg. no. 10.

offences.[5] For cooperation in criminal proceedings involving a member state of the European Union the IRG applies; Section 1 (4) IRG. The rules of the IRG are further specified by the Government in (non-binding) guidelines concerning transnational cooperation in criminal matters ("Richtlinien für den Verkehr mit dem Ausland in strafrechtlichen Angelegenheiten" (RiVASt) as amended on 19 December 2012).

(1) To what extent do specificities of information technology change the nature of mutual assistance?

The proliferation and enhancement of information technologies affect the character of mutual legal assistance in two directions: On the one hand, information technology, in particular the World Wide Web, challenges traditional mutual legal assistance mechanisms by simply increasing opportunities to commit crimes with a transnational dimension. As a result and against the background that the competence of German authorities is generally confined to German territory, police and prosecutorial authorities have to rely to a growing extent on mutual legal assistance and transnational cooperation in criminal matters. Given the "volatility" of the data, the considerable length of time that such mutual assistance procedures can take is a problem. On the other hand, information technology provides for new means and mechanisms of (transnational) investigation and prosecution, such as the electronic transfer of documents, the electronic management of files and documents (Sections 77a, b IRG), and audio-visual interrogations (Section 61c IRG).

(2)

(a) Does your country provide for the interception of (wireless) telecommunication? Under which conditions?

(b) To what extent is it relevant that a provider or a satellite may be located outside the borders of the country?

The interception of telecommunications is provided for in section 100a of the German Code of Criminal Procedure (StPO). Accordingly, telecommunications may be intercepted and recorded without knowledge of the person(s) concerned if certain facts give rise to the suspicion that a person has committed a serious criminal offence (see Subs. 2), the offence is of particular gravity in the individual case, and other means of establishing the facts or determining the defendant's whereabouts would be much more difficult or offer no prospect of success. "Telecommunications" within the meaning of this provision include modern forms of communication such as text messages (SMS/MMS) and communication via the internet.

The surveillance of specific phases of email exchange (i.e. during a communication process still in action; "real time") is only permitted under the strict conditions of Section 100a (1). During other phases only a seizure pursuant to Section 94 et seq. StPO is admissible.[6] In this context, we also have to mention Section 110 (3) StPO. It regulates a search and seizure of storage media that are spatially separated (but located within German territory).

While Section 100a allows for the interception and recording of the content of telecommunications, the generation of call data ("Telekommunikationsverbindungsdaten") is regulated in Sections 100g and 100h of the Code of Criminal Procedure. The procedural conditions for an order pursuant to Section 100a StPO are laid down in Section 100b StPO.

Section 110 of the Telecommunications Act (TGK) together with the Telecommunications

Interception Ordinance (TKÜV) regulate if and to what extent telecommunication companies being under the obligation to cooperate have to take measures for the implementation of surveillance action or the issuance of information.

Section 4 TKÜV is to be taken into consideration regarding any communication containing

a foreign element: Where the telecommunications system recognizes as part of normal operational procedures that the terminal equipment using the identification to be intercepted is located abroad, the telecommunication shall not be covered, unless the telecommunication to be intercepted is diverted or forwarded to a telecommunications connection or a storage facility located in Germany. Pursuant to Section 4 (2) 1, however, the telecommunication shall be covered if it originates from a telecommunications connection that is not known to the authorized body and is destined for a foreign call number cited in the judicial order.

(c) Does your national law provide for mutual legal assistance concerning interception of telecommunication? Did your country conclude international conventions on it?

Generally, a German prosecutor/investigator must not access a server/provider/data

storage which is located outside German territory. In this case, a request for legal assistance is required. An exception from this rule is contained in Article 32 CCC regarding publicly available (open source) computer data.

Requests to intercept telecommunications can be dealt with according to section 59 IRG and according to specific provisions in a treaty. The details are spelled out in No. 77a of the (Government) guidelines concerning transnational cooperation in criminal matters ("Richtlinien für den Verkehr mit dem Ausland in strafrechtlichen Angelegenheiten").[7]

---

[5] E.g. European Convention on the Suppression of Terrorism of 27 January 1977; United Nations Convention of 20 December 1988 against Illicit Traffic in Narcotic Drugs and Psychotropic Substances; Convention of 26 July 1995 Drawn Up on the Basis of Article K.3 of the Treaty on European Union on the Protection of the European Communities' financial Interests; Convention on Cybercrime of 23 November 2001 and its Additional Protocol Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems of 28 January 2003.

[6] See BVerfGE 124, 43 = NJW 2009, 2431; BGH NJW 2010, 1297; dissenting opinion for cases where the email is still or again with the provider, BGH NJW 2009, 1828 (§§ 99, 100 StPO).

[7] No. 77a RiVaSt (Überwachung des Telekommunikationsverkehrs) reads:

In addition, the following treaty provisions, in particular, apply: Articles 17 to 20 of the EU Convention on Mutual Legal Assistance between Member States, which are further specified in a number of bilateral treaties, Article 34 CCC, and Article 12 of the bilateral treaty between the United States of American and Germany. In the context of seizures of emails, further international legal agreements may play into it: i.e. Art. 29, 31 and 32 CCC, which contain legal mutual assistance regulations for the securing and seizure of locked/ backed up computer data.

Furthermore, for the territory of the European Union, the Council's Framework decision 2003/577/JHA of 22 July 2003 on the execution in the European Union of orders freezing property or evidence which is implemented into German law in Sections 94, 97 IRG, as well as the Council Framework Decision 2008/978/JHA of 18 December 2008 on the European Evidence Warrant for the purpose of obtaining objects, documents and data for use in proceedings in criminal are to be mentioned.

(3) To what extent do general grounds for refusal apply concerning internet searches and other means to look into computers and networks located elsewhere?

There are no specific provisions regulating grounds for refusal with regard to internet searches etc. The general regulations on legal mutual assistance remain applicable. Therefore, in cases where a request for mutual assistance regarding a search (and seizure) of computers and/or networks that are located abroad is issued, conditions in accordance with German criminal procedural standards for permitting such a search have to be followed accordingly.

In this regard it is to be acknowledged that so-called covert online searches for criminal proceedings/prosecution, i.e. a single search of a computer while using the connected data line as well as a long-term surveillance of the computer's operation are illegal and inadmissible since there is no specific enabling legislation (different for online searches for preventive purposes, which is permissible under specific legislation, see e.g. Section 20k BKAG; Art. 34d BayPAG).

Section 100a StPO is not applicable, since an online search does not equal a surveillance of telecommunications; the same holds true for Section 102 StPO since an online search normally is covert, while Section 102 StPO does not fit for these kind of investigative methods (see BGHSt 51, 211 and BVerfG NJW 2008, 820).

Outgoing requests for search and seizure are measured against No. 114 RiVASt. Under certain conditions and within the territory of the EU, the prerequisite of dual criminality for incoming requests can be waived, see Section 94 IRG.

(4) Is in your national law the double criminality requirement for cooperation justified in situations in which the perpetrator caused effects from a state in which the conduct was allowed into a state where the conduct is criminalised?

According to the principle of double criminality, the act of the offender that constitutes the grounds for the request, must be subject to criminal liability in the requested state as well. Therefore what matters is the legal situation in the requesting as well as in the requested state. If neither the requested nor the requesting state is the state on which territory the offender acted, it is irrelevant from the perspective of double criminality whether the offender's behaviour was legal or not under the law of the state in which the offender acted.

"(1) Ersuchen, die auf die Durchführung einer Überwachung des Telekommunikationsverkehrs gerichtet sind, können sowohl vertraglos (§ 59 Absatz 1 IRG) als auch auf der Grundlage einer völkerrechtlichen Vereinbarung nach § 1 Absatz 3 IRG erledigt werden. Zulässig ist die Überwachung des Telekommunikationsverkehrs gemaß § 77 IRG nach Maßgabe der Bestimmungen der StPO (§§ 100a, 100b, 101).
Soweit sich aus einer Vereinbarung nicht etwas anderes ergibt oder die Stellung von Bedingungen bei Übermittlung von Erledigungsstücken nicht ausreicht, muss die ausländische Behörde zusichern, dass a) die Voraussetzungen der Telefonüberwachung vorlägen, wenn diese im ersuchenden Staat durchgeführt werden müsste, b) die gewonnenen Erkenntnisse nur zur Aufklärung der in dem Ersuchen genannten Straftat(en) verwendet werden und c) die Überwachungsprotokolle vernichtet werden, sobald sie zur Strafverfolgung nicht mehr erforderlich sind. Die Bewilligungsbehörde kann darüber hinaus die Zusicherung fordern, dass d) die Gegenseitigkeit verbürgt ist und e) der ersuchende Staat die Kosten der Maßnahme trägt. Der ersuchende Staat ist darauf hinzuweisen, dass die deutsche Staatsanwaltschaft gemäß § 101 StPO die Beteiligten von der Maßnahme zu unterrichten hat, sobald diese beendet ist und die Benachrichtigung ohne Gefährdung des Untersuchungszwecks, der öffentlichen Sicherheit und von Leib und Leben einer Person möglich ist. Der ersuchende Staat ist darauf hinzuweisen, dass nach Ablauf einer zu bestimmenden Frist davon ausgegangen wird, dass eine Benachrichtigung erfolgen kann, falls nicht entgegenstehende Tatsachen vor Fristablauf mitgeteilt werden.
(2) Über die Erkenntnisse aus einer in einem deutschen Ermittlungsverfahren durchgeführten Telekommunikationsüberwachung kann unter den Voraussetzungen des § 59 IRG zusammenfassend
Auskunft erteilt werden, wenn die Auskünfte wegen derselben Tat oder einer anderen, in § 100a StPO bezeichneten Straftat, erbeten werden (§§ 77 IRG, 477 Absatz 2 Satz 2 StPO). Kopien der Protokolle der Telekommunikationsüberwachung, umfassende Vermerke über den Gesprächsinhalt oder der Aufzeichnungsbänder dürfen entsprechend den Voraussetzungen des Absatzes 1 herausgegeben werden, wenn die Auskünfte wegen derselben Tat oder einer anderen, in § 100a StPO bezeichneten Straftat, erbeten werden (§§ 77 IRG, 477 Absatz 2 Satz 2 StPO).
(3) Auskünfte über Telekommunikationsverbindungen (§§ 100g, h StPO) können unter den Voraussetzungen des § 66 IRG herausgegeben werden. Im Hinblick auf die sich aus § 101 StPO ergebende Benachrichtigungspflicht gilt Absatz 1 entsprechend.
(4) Wird eine zuständige Behörde gemäß Artikel 20 Absatz 2 und 3 des Übereinkommens vom 29. Mai 2000 ü ber die Rechtshilfe in Strafsachen zwischen den Mitgliedstaaten der Europä ischen Union (EURhÜ bk 2000) darüber unterrichtet, dass der ersuchende Staat Telekommunikationsverkehr einer Zielperson im Hoheitsgebiet Deutschlands überwacht, so beantragt sie unverzü glich beim Gericht festzustellen, dass die Voraussetzungen für eine Überwachung der Telekommunikation nach den §§ 100a, 100b StPO vorliegen. Sollte über den Antrag nicht innerhalb der Frist von 96 Stunden entschieden werden, so verlangt sie eine Fristverlängerung gemäß Artikel 20 Absatz 4a iv EU-RhÜbk 2000."

(5) Does your national law allow for extraterritorial investigations? Under which conditions? Please answer both for the situation that your national law enforcement authorities need information as when foreign authorities need information available in your state.

(6) Is self service (obtaining evidence in another state without asking permission) permitted? What conditions should be fulfilled in order to allow self service? Please differentiate for public and protected information. What is the both (active and passive) practice in your country?

(7) If so, does this legislation also apply to searches to be performed on the publicly accessible web, or in computers located outside the country?

Extraterritorial investigation by (criminal) law enforcement agencies is only admissible if and to the extent that the state on whose territory these measures are to be carried out, permits them explicitly or at least condones them. This holds true regardless of whether it is about a constellation where German officials investigate on foreign territory or whether foreign officials act on German territory. Regarding the territory of other EU Member States, Art. 89 of the Treaty on the Functioning of the European Union stipulates that the Council, acting in accordance with a special legislative procedure, shall lay down the conditions and limitations under which the competent authorities of the Member States referred to in Articles 82 and 87 may operate in the territory of another Member State in liaison and in agreement with the authorities of that State.

Art. 32 CCC includes relevant regulations for the permission of extraterritorial investigation in the area of cyber crime crimes committed on the Internet. Thereafter a contracting party may, without the authorisation of another Party: a) access publicly available (open source) stored computer data, regardless of where the data is located geographically; or b) access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system. Some argue that at least for the first two exceptions, these shall be applicable not only between the contracting parties but also deemed valid in terms of customary international law.

In addition it is to be emphasized again that covert online searches continue to be inadmissible due to a lack of enabling legislation in German law (see above). Hence it cannot be requested in the framework of legal mutual assistance.

(8) Is your country a party to Passenger Name Record (PNR) (financial transaction, DNA-exchange, visa matters or similar) agreements? Please specify and state how the exchange of data is implemented into national law.

Does your country have an on-call unit that is staffed on a 24/7 basis to exchange data? Limit yourself to the issues relevant for the use of information for criminal investigation.

(9) To what extent will data referred to in your answer to the previous question be exchanged for criminal investigation and on which legal basis?

To what extent does the person involved have the possibility to prevent/ correct/delete information? To what extent can this information be used as evidence? Does the law of your country allow for a Notice and Takedown of website containing illegal information? Is there a practice? Does the seat of the provider, owner of the site or any other foreign element play a role?

Regarding these issues, German law is sigificantly determined by European law.

Between the EU and the USA as well as Australia Passenger Name Records Agreements were concluded that henceforth provide the legal grounds for data transfer by airline companies to the respective domestic/ foreign authorities. Regarding Germany, the agreement of 26 July 2007 between the European Union and the USA on the processing of flight passenger data and the transfer of such data by the airlines to the United States Department of Homeland Security (DHS), has been approved through a respective Act.[8] The specific modalities governing the transfer of passenger name records do not stem directly from the agreement itself but from a US attached communication addressed to the EU. Neither the PNR agreement between Germany and the USA nor the PNR agreement between the EU and Australia provide for subjective rights of the concerned persons; those can be found, however, in European law.[9]

An agreement that contains regulations on the exchange of all relevant data such as DNA-profiles, fingerprints and car license data for the purpose of criminal investigations and prosecution is the so-called Prüm treaty enacted on 26 November 2006.[10]

---

[8] BGBl. II 2007 S. 1978; BT-Drs. 826/07 vom 14.11.2007, S. 3; for the legal opinion of the federal government pertaining to the question, whether these treaties required ratification by all member states of the EU, see BT-Drucks. 17/7312 of 14 October 2011, pp. 21. BGBl. II 2007 S. 1978; BT-Drs. 826/07 vom 14 November 2007, S. 3.

[9] Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters [in Germany not yet implemented]; Art 8 ECHR; Art 16 of the Treaty on the Functioning of the European Union; Art 8 Charter of Fundamental Rights of the European Union.
These PNR-agreements are particularly criticized for reasons related to data protection.

[10] Treaty of 27 May 2005 between the Kingdom of Belgium, the Federal Republic of Germany, the Kingdom of Spain, the French Republic, the Grand Duchy of Luxemburg, the Kingdom of the Netherlands and the Republic of Austria on the stepping up of cross-border cooperation,

The essential regulations of this treaty were transferred into the legal framework of the EU by Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime.[11] The Prüm Treaty as well as the Council's decision 2008/615/JHA of 23 June 2008 arrange for the establishment of national data storage, that then could be accessed by all contracting parties and member states respectively within a so-called hit/no-hit procedure.

There is a close connection to Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between the law enforcement authorities of the Member States of the European Union, which by now is implemented into German law, Sections 92 et seqq. IRG.

Following the model of the Prüm treaty, the agreement of 1 October 2008 between the government of the Federal Republic of Germany and the United States of America on enhancing cooperation in preventing and combating serious crime was concluded.[12] This agreement stipulates the automatic comparison of pseudonomized DNA reference data with DNA-profiles and fingerprints. Individual rights of the persons involved pertaining to the rectification, erasure, or blocking of data that is either inaccurate or incomplete are not included in the agreement; only the contracting parties have such rights pursuant to Art. 14.

With the agreement of 28 June 2010 between the European Union and the USA on the processing and transfer of Financial Messaging Data for the purpose of a terrorist finance tracking program there is an international treaty that concerns the exchange of data related to financial transactions (also known as the SWIFT agreement). Art. 16 of the agreement provides for the right of the concerned person to seek the rectification, erasure, or blocking of his or her personal data processed by the U.S. Treasury Department pursuant to this Agreement, where the data are inaccurate or the processing contravenes this agreement.

In Art. 4 of the agreement of 25 June 2003 between the EU and the USA on mutual legal assistance, another provision on the identification of bank information can be found. Moreover, similar provisions can be found in Art. 18 of the agreement of 11 October 2010 between the EU and Japan on mutual legal assistance in criminal matters (only in regard to bank accounts) and Art 9bis of the agreement of 14 October 2003 between Germany and the USA on mutual legal assistance in criminal matters (determination of bank information).

There exists a 24/7 contact point in Germany. The contact point is located at the Federal

Criminal Police Office ("Bundeskriminalamt").

(10) Do you think an international enforcement system to implement decisions (e.g. internet banning orders or disqualifications) in the area of cyber crime is possible? Why (not)?

(11) Does your country allow for direct consultation of national or international databases containing information relevant for criminal investigations (without a request)?

Generally, information exchange and data requests on a transnational level are only possible within the legal framework of mutual legal assistance. However, there are certain international agreements that provide for direct access to certain data storages without further reference to mutual legal assistance. In that context, we have for instance the above-mentioned Prüm treaty, the respective Council Decision 2008/615/JI of 23 June 2008, and the data exchange agreement between Germany and the USA [establishment of national data storage with DNA-profiles, fingerprints et cetera and the request according to the hit/no-hit procedure, yet in cases of a (anonymous) hit then on the basis of mutual legal assistance].

Other important information systems include the Schengen information system (police information and query system for tracing persons and property, certain national offices have access to the data), the VISA information system (between others, an instrument for fighting fraud, visa issuance authorities and certain national offices as well as Europol shall have access), Eurodac (central data storage within the framework of the asylum system, amelioration of inter-operationality with SIS and VIS are intended, access by criminal law enforcement agencies and Europol shall be provided), the Europol Information system [securing of personal (dactyloscopic data and DNA-profiles) e.g. as well as offence-relevant data, inputting and access by the respective national office (in Germany the BKA - Federal Criminal Police Office) and liaison officer, analysis system] and the customs information system (central data storage, in which under specific/ certain conditions personal data could be secured; access in particular to customs, but also other national offices).

Moreover, based on the Framework Decision on the organisation and content of the exchange of information extracted from criminal records between Member States and Council Decision 2009/316/JI on the establishment of the European Criminal Records Information System (ECRIS), which are both implemented in German law with the law of 15 December 2011, with effect from 27 April 2012 (BGBl. 2011 I S. 2714, an integration of criminal records within the EU took place (at present no online-access as yet to the records of other national states is possible; system of mutual electronic information and requests).

---

particularly in combating terrorism, cross-border crime and illegal migration: also known as "Schengen III"; see for domestic implementation in Germany BGBl. 2006 II S. 626; 2007 II S. 626, 857, 1420; 2010 II S. 870; 2006 I S. 1458.

[11] See also BGBl. 2009 I S. 2507.

[12] Treaty Law of 1 September 2009, BGBl. 2009 II S. 1010; Implementation Act of 11 September 2009, BGBl. 2009 I S. 2998.

(12) Does your state participate in Interpol/Europol/Eurojust or any other supranational office dealing with the exchange of information? Under which conditions?

Germany as a member of the EU partakes in Europol as well as Eurojust.[13]

The national contact point for the European police office "Europol" is at the Federal Criminal Police Office (BKA), which also serves as the central office for Interpol, to which Germany also belongs. Pursuant to Section 74 (3) IRG, Sections 14 (1) 1 No. 2 and 15 (1)-(3) provides the the BKA with authority for data transfer, public announcement and identification (see also Nos. 123 and 125 RiVASt).

(E) Human Rights Concerns

Which human rights or constitutional norms are applicable in the context of criminal investigations using information technology? Is it for the determination of the applicable human rights rules relevant where the investigations are considered to have been conducted? How is the responsibility or accountability of your state involved in international cooperation regulated? Is your state for instance accountable for the use of information collected by another state in violation of international human rights standards?

German law enforcement agencies, generally but also when taking action that involve modern information and electronic investigation technologies are legally bound by (national) constitutional (Grundgesetz – GG) as well as international human rights instruments, regardless of whether the respective measures are taken on German soil or (exceptionally) outside German territory.

The application of information technologies is an area of high human rights sensibility, in particular regarding the privacy of correspondence, posts and telecommunications provided for in Art 10 GG, the right to the inviolability of the home, Art. 13 GG and the right to confidentiality and integrity of IT systems pursuant to Art. 2 (1) in connection with Art. 1 (1) GG (see also Art 16 of the Treaty on the Functioning of the European Union, Art 8 ECHR, Art 8 Charta of Fundamental Rights of the European Union). In 2008 in a seminal decision, the Federal Constitutional Court presented a kind of new basic right, i.e. the right of integrity and confidentiality of computer systems ("Grundrecht der Integrität und Vertraulichkeit von Computersystemen", (BVerfGE 120, 274). As a consequence of the general guarantee of human dignity, so the German Federal Constitutional Court argues, the core area of private life must not to be investigated, especially not by electronic investigation methods.[14]

Another question, however, is the responsibility for human rights violations by foreign authorities in the context of mutual legal assistance.

Furthermore, it is questionable if information that is retrieved by foreign authorities while committing human rights violations can be presented in criminal proceedings in Germany. Concerning interrogations, it should be noted that addressees of Section 136a StPO are German authorities responsible for criminal prosecution; however, evidence that is retrieved by private persons (and foreign interrogation officers respectively) under circumstances that constitute a flagrant violation of human dignity (such as torture) cannot be used (OLG Hamburg NJW 2005, 2326. 2329). The threshold for a prohibition against the use of the retrieved information is apparently relatively high.

(F) Future Developments

Modern telecommunication creates the possibility of contacting accused, victims and witnesses directly over the border. Should this be allowed, and if so, under which conditions? If not, should the classical rules on mutual assistance be applied (request and answer) and why?

The immediate communication with persons residing in another country is regulated by No. 121 RiVASt. Accordingly, German enforcement agencies in criminal matters are allowed to communicate with persons residing in a foreign state – regardless of whether that person is German or of another nationality – in writing or by phone, only when the foreign state in question does not deem such an act as interference with its sovereign rights.

Is there any legal impediment under the law of your country to court hearings via the screen (skype or other means) in transnational cases? If so which? If not, is there any practice?

Generally, regarding the interrogation of a witness during the trial period, an interrogation "via the screen" would be in conflict with the fundamental principle of presentation of evidence before the deciding judges ("Unmittelbarkeitsprinzip"). A notable exception hereto can be found in Section 247a StPO, which stipulates an audiovisual interrogation of a witness. For cases with a nexus to another state, Section 247a (1) together with Section 251 (2) No. 2 StPO are relevant.

According to these provisions, an audiovisual interrogation is admissible when witnesses or expert witnesses cannot be expected to attend trial due to the long distance under equal consideration of the value of his or her testimony.

---

[13] In this matter see in particular the Implementation Act on the Council decision 2009/ 371/JI of 6 April 2009 establishing the European Police Office (Europol-Gesetz of 16 December 1997 and the Implementation Act on the Council decision (2002/187/JHA) of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crimes of 12 May 200; not yet implemented: the Council decision of 16 December 2008 on the strengthening of Eurojust and amending draft of the implementation act BT-Drucks. 17/8728.

[14] *Vogel* ZIS 2012, 480, 482 with further references, in particular BVerfGE 109, 279; 113, 348; BVerfGE 129, 208.

The obligation to be present at all times during the trial, Section 231 StPO, prohibits an interrogation of the accused via the screen. Exceptions can be made only in proceedings with minor charges. Moreover, there are certain scenarios where for a certain period of time the proceedings can continue without the accused being present. However, an audiovisual interrogation is not envisaged in these cases. Section 247a StPO is applicable exclusively for witnesses, not for the accused.

Art. 10 (9) of the European agreement on mutual legal assistance offers the possibility to interrogate the accused via video conference.

Generally a rather careful/ sensible usage of these new technologies is warranted. Advantages may be the acceleration of proceedings, e.g. the higher quality of evidence in contrast to the reading of interrogation protocols and the possibility for the accused to claim his or her right to confrontation. However, there are substantial downsides to this: what is lost is the possibility of getting a close impression of the person which would otherwise (i.e. when the person is present) be attainable.

Appendix 1: Statutes

Criminal Code (Strafgesetzbuch – StGB)

Full citation: Criminal Code in the version promulgated on 13 November 1998, Federal Law Gazette [Bundesgesetzblatt] I p. 3322, last amended by Article 8 of the Law of 8 April 2013, Federal Law Gazette I p. 734

Section 3
Applicability to Domestic Acts.
German criminal law shall apply to acts, which were committed domestically.

Section 4
Applicability to Acts on German Ships and Aircraft.
German criminal law shall apply, regardless of the law of the place where the act was committed, to acts which are committed on a ship or in an aircraft, which is entitled to fly the federal flag or the national insignia of the Federal Republic of Germany.

Section 5
Acts Abroad Against Domestic Legal Interests.
German criminal law shall apply, regardless of the law of the place the act was committed, to the following acts committed abroad:

1. preparation of a war of aggression (Section 80);
2. high treason (Sections 81 to 83);
3. endangering the democratic rule of law:
   (a) in cases under Sections 89 and 90a subsection (1), and Section 90b, if the perpetrator is a German and has his livelihood in the territorial area of applicability of this law; and
   (b) in cases under Sections 90 and 90a subsection (2);
4. treason and endangering external security (Sections 94 to 100a);
5. crimes against the national defense:
   (a) in cases under Sections 109 and 109e to109g; and
   (b) in cases under Sections 109a, 109d and 109h, if the perpetrator is a German and

has his livelihood in the territorial area of applicability of this law;

6. abduction and casting political suspicion on another (Sections 234a, 241a), if the act is directed against a person who has his domicile or usual residence in Germany;

6a. child stealing in cases under Section 235 subsection (2), no. 2, if the act is directed against a person who has his domicile or usual residence in Germany;

7. violation of business or trade secrets of a business located within the territorial area of applicability of this law, an enterprise, which has its registered place of business there, or an enterprise with its registered place of business abroad, which is dependent on an enterprise with its registered place of business within the territorial area of applicability of this law and constitutes with it a group;
8. crimes against sexual self-determination:
   (a) in cases under Section 174 subsections (1) and (3), if the perpetrator and the person, against whom the act was committed are Germans at the time of the act and have their livelihoods in Germany; and
   (b) in cases under Sections 176 to 176b and 182, if the perpetrator is a German;
9. termination of pregnancy (Section 218), if the perpetrator at the time of the act is a German and has his livelihood in the territorial area of applicability of this law;
10. false unsworn testimony, perjury and false affirmations in lieu of an oath (Sections 153 to 156) in a proceeding pending before a court or other German agency within the territorial area of applicability of this law, which is competent to administer oaths or affirmations in lieu of an oath;
11. crimes against the environment in cases under Sections 324, 326, 330 and 330a, which were committed in the area of Germany's exclusive economic zone, to the extent that international conventions on the protection of the sea permit their prosecution as crimes;

11a. crimes under Section 328 subsection (2), nos. 3 and 4 subsections (4) and (5), also in conjunction with Section 330, if the perpetrator is a German at the time of the act;

12. acts, which a German public official or a person with special public service obligations commits during his official stay or in connection with his duties;
13. acts committed by a foreigner as a public official or as a person with special public service obligations;
14. acts which someone commits against a public official, a person with special public service obligations, or a soldier in the Federal Armed Forces during the discharge of his duties or in connection with his duties;

14a. bribery of a member of parliament (Section 108e) if the perpetrator is a German at the time of the act or the act was committed in relation to a German;
15. trafficking in organs (section 18 of the Transplantation Law), if the perpetrator is a German at the time of the act.

Section 6
Acts Abroad Against Internationally Protected Legal Interests.
German criminal law shall further apply, regardless of the law of the place of their commission, to the following acts committed abroad:

1. (deleted)
2. serious criminal offences involving nuclear energy, explosives and radiation in cases under Sections 307 and 308 subsections (1) to (4),Section 309 subsection (2) and Section 310;
3. assaults against air and sea traffic (Section 316c);
4. trafficking in human beings for sexual exploitation and for exploitation of workforce, as well as promotion of human trafficking (Sections 232 to 233a);
5. unauthorized distribution of narcotics;
6. dissemination of pornographic writings in cases under Sections 184a and 184b subsections (1) to (3), also in connection with Section 184c sentence 1;
7. counterfeiting of money and securities (Sections 146, 151 and 152), payment cards and blank Eurochecks (Section 152b subsections (1) to (4), as well as their preparation (Sections 149, 151, 152 and 152b subsection (5);
8. subsidy fraud (Section 264);
9. acts which, on the basis of an international agreement binding on the Federal Republic of Germany, shall also be prosecuted if they are committed abroad.

Section 7 Applicability to Acts Abroad in Other Cases.
(1) German criminal law shall apply to acts, which were committed abroad against a German, if the act is punishable at the place of its commission or the place of its commission is subject to no criminal law enforcement.
(2) German criminal law shall apply to other acts, which were committed abroad if the act is punishable at the place of its commission or the place of its commission is subject to no criminal law enforcement and if the perpetrator:

1. was a German at the time of the act or became one after the act; or
2. was a foreigner at the time of the act, was found to be in Germany and, although the Extradition Act would permit extradition for such an act, is not extradited, because a request for extradition is not made, is rejected, or the extradition is not practicable.

Section 9 Place of the Act.
(1) An act is committed at every place the perpetrator acted or, in case of an omission, should have acted, or at which the result, which is an element of the offense, occurs or should occur according to the understanding of the perpetrator.
(2) Incitement or accessoryship is committed not only at the place where the act was committed, but also at every place where the inciter or accessory acted or, in case of an omission, should have acted or where, according to his understanding, the act should have been committed. If the inciter or accessory in an act abroad acted domestically, then German criminal law shall apply to the incitement or accessoryship, even if the act is not punishable according to the law of the place of its commission.

Section 86
Dissemination of propaganda material of unconstitutional organisations
(1) Whosoever within Germany disseminates or produces, stocks, imports or exports or makes publicly accessible through data storage media for dissemination within Germany or abroad, propaganda material

1. of a political party which has been declared unconstitutional by the Federal Constitutional Court or a political party or organisation which has been held by final decision to be a surrogate organisation of such a party;
2. of an organisation which has been banned by final decision because it is directed against the constitutional order or against the idea of the comity of nations or which has been held by final decision to be a surrogate organisation of such a banned organisation;
3. of a government, organisation or institution outside the Federal Republic of Germany active in pursuing the objectives of one of the parties or organisations indicated in Nos 1 and 2 above; or
4. propaganda materials the contents of which are intended to further the aims of a former National Socialist organisation, shall be liable to imprisonment not exceeding three years or a fine.

(2) Propaganda materials within the meaning of subsection (1) above shall only be written materials (section 11(3)) the content of which is directed against the free, democratic constitutional order or the idea of the comity of nations.
(3) Subsection (1) above shall not apply if the propaganda materials or the act is meant to serve civil education, to avert unconstitutional movements, to promote art or science, research or teaching, the reporting about current or historical events or similar purposes.

(4) If the guilt is of a minor nature, the court may order a discharge under this provision.

Section 86a
Using symbols of unconstitutional organisations
(1) Whosoever
1. domestically distributes or publicly uses, in a meeting or in writtenmaterials (section 11(3)) disseminated by him, symbols of one of the parties or organisations indicated in section 86(1) Nos 1, 2 and 4; or
2. produces, stocks, imports or exports objects which depict or contain such symbols for distribution or use in Germany or abroad in a manner indicated in No 1,

shall be liable to imprisonment not exceeding three years or a fine.
(2) Symbols within the meaning of subsection (1) above shall be in particular flags,insignia, uniforms and their parts, slogans and forms of greeting. Symbols which are so similar as to be mistaken for those named in the 1st sentence shall be equivalent to them.
(3) Section 86(3) and (4) shall apply mutatis mutandis.

Section 91
Encouraging the commission of a serious violent offence endangering the state
(1) Whosoever
1. displays or supplies to another written material (section 11(3)) which by its content is capable of serving as an instruction to the commission of a serious violent offence endangering the state (section 89a(1)), if the circumstances of its dissemination are conducive to awakening or encouraging the preparedness of others to commit a serious violent offence endangering the state,
2. obtains written material within the meaning of No. 1 above for the purpose of committing a serious violent offence endangering the state

shall be liable to imprisonment not exceeding three years or a fine.
(2) Subsection (1) No. 1 above shall not apply if
1. the act serves the purpose of citizenship education, the defence against anti-constitutional movements, arts and sciences, research or teaching, reporting about current or historical events or similar purposes or
2. if the act exclusively serves the fulfilment of lawful professional or official duties.

(3) If the degree of guilt is of a minor nature, the court may order a discharge for the offence under this provision.

Section 111
Public incitement to crime
(1) Whosoever publicly, in a meeting or through the dissemination of written materials (section 11(3)) incites the commission of an unlawful act, shall be held liable as an abettor (section 26).
(2) If the incitement is unsuccessful the penalty shall be imprisonment not exceeding five years or a fine. The penalty must not be more severe than if the incitement had been successful (subsection (1) above); section 49(1) No 2 shall apply.

Section 130
Incitement to hatred
(1) Whosoever, in a manner capable of disturbing the public peace
1. incites hatred against segments of the population or calls for violent or arbitrary measures against them; or
2. assaults the human dignity of others by insulting, maliciously maligning, or defaming segments of the population,

shall be liable to imprisonment from three months to five years.
(2) Whosoever
1. with respect to written materials (section 11(3)) which incite hatred against segments of the population or a national, racial or religious group, or one characterised by its ethnic customs, which call for violent or arbitrary measures against them, or which assault the human dignity of others by insulting, maliciously maligning or defaming segments of the population or a previously indicated group
   (a) disseminates such written materials;
   (b) publicly displays, posts, presents, or otherwise makes them accessible;
   (c) offers, supplies or makes them accessible to a person under eighteen years; or
   (d) produces, obtains, supplies, stocks, offers, announces, commends, undertakes to import or export them, in order to use them or copies obtained from them within the meaning of Nos (a) to (c) or facilitate such use by another; or
2. disseminates a presentation of the content indicated in No 1 above by radio, media services, or telecommunication services
1. shall be liable to imprisonment not exceeding three years or a fine.

(3) Whosoever publicly or in a meeting approves of, denies or downplays an act committed under the rule of National Socialism of the kind indicated in section 6 (1) of the Code of International Criminal Law, in a manner capable of disturbing the public peace shall be liable to imprisonment not exceeding five years or a fine.
(4) Whosoever publicly or in a meeting disturbs the public peace in a manner that violates the dignity of the victims by approving of, glorifying, or justifying National Socialist rule of arbitrary force shall be liable to imprisonment not exceeding three years or a fine.
(5) Subsection (2) above shall also apply to written materials (section 11(3)) of a content such as is indicated in subsections (3) and (4) above.
(6) In cases under subsection (2) above, also in conjunction with subsection (5) above, and in cases of subsections (3) and (4) above, section 86(3) shall apply mutatis mutandis.

Section 130a
Attempting to cause the commission of offences by means of publication
(1) Whosoever disseminates, publicly displays, posts, presents, or otherwise makes accessible written material (section 11(3)) capable of serving as an instruction for an unlawful act named in section 126(1) and intended by its content to encourage or cause others to commit such an act, shall be liable to imprisonment not exceeding three years or a fine.
(2) Whosoever

1. disseminates, publicly displays, posts, presents, or otherwise makes accessible written material (section 11(3)) capable of serving as an instruction for an unlawful act named in section 126(1); or
2. gives instructions for an unlawful act named in section 126(1) publicly or in a meeting,

in order to encourage or cause others to commit such an act, shall incur the same penalty.
(3) Section 86(3) shall apply mutatis mutandis.

Section 131
Dissemination of depictions of violence
(1) Whosoever

1. disseminates written materials (section 11(3)), which describe cruel or otherwise inhuman acts of violence against humans or humanoid beings in a manner expressing glorification or which downplays such acts of violence or which represents the cruel or inhuman aspects of the event in a manner which violates human dignity;
2. publicly displays, posts, presents, or otherwise makes them accessible;
3. offers, supplies or makes them accessible to a person under eighteen years; or
4. produces, obtains, supplies, stocks, offers, announces, commends, undertakes to import or export them, in order to use them or copies obtained from them within the meaning of numbers 1 to 3 above or facilitate such use by another,

shall be liable to imprisonment not exceeding one year or a fine.
(2) Whosoever disseminates a presentation with a content indicated in subsection (1) above by radio, media services, or telecommunication services shall incur the same penalty.
(3) Subsections (1) and (2) above shall not apply in cases of reporting about current or historical events.
(4) Subsection (1) No 3 above shall not apply if the person authorised to care for another person acts; this shall not apply if that person grossly neglects his duty of education by offering, giving, or making them accessible.

Section 176
Child abuse
(1) Whosoever engages in sexual activity with a person under fourteen years of age (child) or allows the child to engage in sexual activity with himself shall be liable to imprisonment from six months to ten years.
(2) Whosoever induces a child to engage in sexual activity with a third person or to allow third persons to engage in sexual activity with the child shall incur the same penalty.
(3) In especially serious cases the penalty shall be imprisonment of not less than one year.
(4) Whosoever

1. engages in sexual activity in the presence of a child;
2. induces the child to engage in sexual activity, unless the act is punishable under subsection (1) or subsection (2) above;
3. presents a child with written materials (section 11(3)) to induce him to engage in sexual activity with or in the presence of the offender or a third person or allow the offender or a third person to engage in sexual activity with him; or
4. presents a child with pornographic illustrations or images, audio recording media with pornographic content or pornographic speech,

shall be liable to imprisonment from three months to five years.
(5) Whosoever supplies or promises to supply a child for an offence under subsections (1) to (4) above or who agrees with another to commit such an offence shall be liable to imprisonment from three months to five years.
(6) The attempt shall be punishable; this shall not apply to offences under subsection (4) Nos 3 and 4 and subsection (5) above.

Section 184
Distribution of pornography
(1) Whosoever with regard to pornographic written materials (section 11(3))

1. offers, gives or makes them accessible to a person under eighteen years of age;
2. displays, presents or otherwise makes them accessible at a place accessible to persons under eighteen years of age, or which can be viewed by them;
3. offers or gives them to another in retail trade outside the business premises, in kiosks or other sales areas which the customer usually does not enter, through a mail-order business or in commercial lending libraries or reading circles;
1. 3a. offers or gives them to another by means of commercial rental or comparable commercial supply for use, except for shops which are not accessible to persons under eighteen years of age and which cannot be viewed by them;
4. undertakes to import them by means of a mail-order business;
5. publicly offers, announces, or commends them at a place accessible to persons under eighteen years of age or which can be viewed by them, or through dissemination of written materials outside business transactions through the usual trade outlets;
6. allows another to obtain them without having been requested to do so;
7. shows them at a public film showing for an entry fee intended entirely or predominantly for this showing;
8. produces, obtains, supplies, stocks, or undertakes to import them in order to use them or copies made from them within the meaning of Nos 1 to 7 above or to facilitate such use by another; or
9. undertakes to export them in order to disseminate them or copies made from them abroad in violation of foreign penal provisions or to make them publicly accessible or to facilitate such use,

shall be liable to imprisonment not exceeding one year or a fine.
(2) Subsection (1) No 1 above shall not apply if the offender is the person in charge of the care of the person, unless that person grossly violates his duty of education by offering, giving, or making them available. Subsection (1) No 3a above shall not apply if the act takes place in business transactions with commercial borrowers.

Section 184a
Distribution of pornography depicting violence or sodomy
Whosoever

1. disseminates;
2. publicly displays, presents, or otherwise makes accessible; or
3. produces, obtains, supplies, stocks, offers, announces, commends, or undertakes to import or export, in order to use them or copies made from them within the meaning of Nos 1 or 2 above or facilitates such use by another, pornographic written materials (section 11(3)) that have as their object acts of violence or sexual acts of persons with animals

shall be liable to imprisonment not exceeding three years or a fine.

Section 184b
Distribution, acquisition and possession of child pornography
(1) Whosoever

1. disseminates;
2. publicly displays, presents, or otherwise makes accessible; or
3. produces, obtains, supplies, stocks, offers, announces, commends, or undertakes to import or export in order to use them or copies made from them within the meaning of Nos 1 or 2 above or facilitates such use by another pornographic written materials (section 11 (3)) related to sexual activities performed by, on or in the presence of children (section 176 (1)) (child pornography)

shall be liable to imprisonment from three months to five years.
(2) Whosoever undertakes to obtain possession for another of child pornography reproducing an actual or realistic activity shall incur the same penalty.
(3) In cases under subsection (1) or subsection (2) above the penalty shall be imprisonment of six months to ten years if the offender acts on a commercial basis or as a member of a gang whose purpose is the continued commission of such offences and the child pornography reproduces an actual or realistic activity.
(4) Whosoever undertakes to obtain possession of child pornography reproducing an actual or realistic activity shall be liable to imprisonment not exceeding two years or a fine. Whosoever possesses the written materials set forth in the 1st sentence shall incur the same penalty.
(5) Subsections (2) and (4) above shall not apply to acts that exclusively serve the fulfilment of lawful official or professional duties.
(6) In cases under subsection (3) above section 73d shall apply. Objects to which an offence under subsection (2) or (4) above relates shall be subject to a depriation order. Section 74a shall apply.

Section 184c
Distribution, acquisition and possession of juvenile pornography
(1) Whosoever
1. disseminates;
2. publicly displays, presents, or otherwise makes accessible; or
3. produces, obtains, supplies, stocks, offers, announces, commends, or undertakes to import or export in order to use them or copies made from them within the meaning of Nos 1 or 2 above or facilitates such use by another pornographic written materials (section 11 (3)) related to sexual activities performed by, on or in the presence of persons between the ages of fourteen to eighteen years (juvenile pornography)

shall be liable to imprisonment not exceeding three years or a fine.
(2) Whosoever undertakes to obtain possession for another of juvernile pornography reproducing an actual or realistic activity shall incur the same penalty.
(3) In cases under subsection (1) or subsection (2) above the penalty shall be imprisonment of three months to five years if the offender acts on a commercial basis or as a member of a gang whose purpose is the continued commission of such offences and the juvenile pornography reproduces an actual or realistic activity.
(4) Whosoever undertakes to obtain possession of child pornography reproducing an actual or realistic activity shall be liable to imprisonment not exceeding one year or a fine. The 1st sentence shall not apply to acts of persons related to juvenile pornography produced by them while under eighteen years of age and with the consent of the persons therein depicted.
(5) Section 184b (5) and (6) shall apply mutatis mutandis.

Section 184d
Distribution of pornographic performances by broadcasting, media services or telecommunications services
Whosoever disseminates pornographic performances via broadcast, media services, or telecommunications services shall be liable pursuant to sections 184 to 184c. In cases under section 184 (1) the 1st sentence above shall not apply to dissemination via media services or telecommunications services if it is ensured by technical or other measures that the pornographic performance is not accessible to persons under eighteen years of age.

Section 202a
Data espionage
(1) Whosoever unlawfully obtains data for himself or another that were not intended for him and were especially protected against unauthorised access, if he has circumvented the protection, shall be liable to imprisonment not exceeding three years or a fine.
(2) Within the meaning of subsection (1) above data shall only be those stored or transmitted electronically or magnetically or otherwise in a manner not immediately perceivable.

Section 202b
Phishing
Whosoever unlawfully intercepts data (section 202a(2)) not intended for him, for himself or another by technical means from a non-public data processing facility or from the electromagnetic broadcast of a data processing facility, shall be liable to imprisonment not exceeding two years or a fine, unless the offence incurs a more severe penalty under other provisions.

Section 202c
Acts preparatory to data espionage and phishing
(1) Whosoever prepares the commission of an offence under section 202a or section 202b by producing, acquiring for himself or another, selling, supplying to another, disseminating or making otherwise accessible
1. passwords or other security codes enabling access to data (section 202a(2)), or
2. software for the purpose of the commission of such an offence,

shall be liable to imprisonment not exceeding one year or a fine.
(2) Section 149(2) and (3) shall apply mutatis mutandis.

Section 206
Violation of the postal and telecommunications secret
(1) Whosoever unlawfully discloses to another person facts which are subject to the postal or telecommunications secret and which became known to him as the owner or employee of an enterprise in the business of providing postal or telecommunications services, shall be liable to imprisonment not exceeding five years or a fine.
(2) Whosoever, as an owner or employee of an enterprise indicated in subsection (1) above unlawfully
1. opens a piece of sealed mail which has been entrusted to such an enterprise for delivery or gains knowledge of its content without breaking the seal by using technical means;
2. suppresses a piece of mail entrusted to such an enterprise for delivery; or
3. permits or encourages one of the offences indicated in subsection (1) or in Nos 1 or 2 above,

shall incur the same penalty.
(3) Subsections (1) and (2) above shall apply to persons who
1. perform tasks of supervision over an enterprise indicated in subsection (1) above;
2. are entrusted by such an enterprise or with its authorisation, to provide postal or telecommunications services; or
3. are entrusted with the establishment of facilities serving the operation of such an enterprise or with performing work thereon.

(4) Whosoever unlawfully discloses to another person facts which became known to him as a public official outside the postal or telecommunications service on the basis of an authorised or unauthorised infringement of the postal or telecommunications secret shall be liable to imprisonment not exceeding two years or a fine.
(5) The immediate circumstances of the postal operations of particular persons as well as the content of pieces of mail are subject to the postal secret. The content of telecommunications and their immediate circumstances, especially the fact whether someone has participated in or is participating in a telecommunications event, are subject to the telecommunications secret. The telecommunications secret also extends to the immediate circumstances of unsuccessful attempts to make a connection.

Section 263a
Computer fraud
(1) Whosoever with the intent of obtaining for himself or a third person an unlawful material benefit damages the property of another by influencing the result of a data processing operation through incorrect configuration of a program, use of incorrect or incomplete data, unauthorised use of data or other unauthorised influence on the course of the processing shall be liable to imprisonment not exceeding five years or a fine.
(2) Section 263(2) to (7) shall apply mutatis mutandis.
(3) Whosoever prepares an offence under subsection (1) above by writing computer programs the purpose of which is to commit such an act, or procures them for himself or another, offers them for sale, or holds or supplies them to another shall be liable to imprisonment not exceeding three years or a fine.
(4) In cases under subsection (3) above section 149(2) and (3) shall apply mutatis mutandis.

Section 265a
Obtaining services by deception
(1) Whosoever obtains the service of a machine or a telecommunications network serving public purposes or uses a means of transportation or obtains entrance to an event or institution by deception with the intent of not paying for them shall be liable to imprisonment not exceeding one year or a fine unless the act is punishable under other provisions with a more severe penalty.
(2) The attempt shall be punishable.
(3) Section 247 and section 248a shall apply mutatis mutandis.

Section 268
Forgery of technical records
(1) Whosoever for the purpose of deception in legal commerce
1. produces a counterfeit technical record or falsifies a technical record or
2. uses a counterfeit or falsified technical record

shall be liable to imprisonment not exceeding five years or a fine.
(2) A technical record shall mean a presentation of data, measurements or calculations, conditions or sequences of events, which, in whole or in part, is produced automatically by a technical device, allows the object of the record to be recognised either generally or by informed persons and is intended as proof of a legally relevant fact, regardless of whether this was already the purpose of the presentation when it was produced or only later.
(3) It shall be equivalent to the production of a counterfeit technical record if the offender influences the result of the record by interfering with the recording process.
(4) The attempt shall be punishable.
(5) Section 267(3) and (4) shall apply mutatis mutandis.

Section 269
Forgery of data intended to provide proof
(1) Whosoever for the purposes of deception in legal commerce stores or modifies data intended to provide proof in such a way that a counterfeit or falsified document would be created upon their retrieval, or uses data stored or modified in such a manner, shall be liable to imprisonment not exceeding five years or a fine.
(2) The attempt shall be punishable.
(3) Section 267(3) and (4) shall apply mutatis mutandis.

Section 274
Suppression of documents; changing a border mark
(1) Whosoever
1. destroys, damages or suppresses a document or a technical record which does not belong to him or not exclusively to him with the intent of causing damage to another;
2. deletes, suppresses, renders unusable or alters legally relevant data (section 202a(2)), which are not or not exclusively at his disposal, with the intent of causing damage to another; or
3. takes away, destroys, renders unrecognisable, moves or falsely places a border stone or another sign intended as a designation of a border or water level with the intent of causing damage to another,

shall be liable to imprisonment not exceeding five years or a fine.
(2) The attempt shall be punishable.

Section 284
Organising unlawful gaming
(1) Whosoever without the permission of a public authority publicly organises or operates a game of chance or makes equipment for it available shall be liable to imprisonment not exceeding two years or a fine.
(2) Games of chance in clubs or private societies in which games of chance are regularly organised shall be deemed to be publicly organised.
(3) Whosoever in cases under subsection (1) above acts
1. on a commercial basis; or
2. as a member of a gang whose purpose is the continued commission of such offences,

shall be liable to imprisonment from three months to five years.
(4) Whosoever advertises a public game of chance (subsections (1) and (2) above), shall be liable to imprisonment not exceeding one year or a fine.

Section 285
Participation in unlawful gaming
Whosoever participates in a public game of chance (section 284) shall be liable to imprisonment not exceeding six months or a fine not exceeding one hundred and eighty daily units.

Section 303a
Data tampering
(1) Whosoever unlawfully deletes, suppresses, renders unusable or alters data (section 202a (2)) shall be liable to imprisonment not exceeding two years or a fine.
(2) The attempt shall be punishable.

Section 303b
Computer sabotage
(1) Whosoever interferes with data processing operations which are of substantial importance to another by
1. committing an offence under section303a(1); or
2. entering or transmitting data (section 202a(2)) with the intention of causing damage to another; or
3. destroying, damaging, rendering unusable, removing or altering a data processing system or a data carrier,

shall be liable to imprisonment not exceeding three years or a fine.
(2) If the data processing operation is of substantial importance for another's business, enterprise or a public authority, the penalty shall be imprisonment not exceeding five years or a fine.
(3) The attempt shall be punishable.
(4) In especially serious cases under subsection (2) above the penalty shall be imprisonment from six months to ten years. An especially serious case typically occurs if the offender
1. causes major financial loss,
2. acts on a commercial basis or as a member of a gang whose purpose is the continued commission of computer sabotage, or
3. through the offence jeopardises the population's supply with vital goods or services or the national security of the Federal Republic of Germany.

(5) Section 202c shall apply mutatis mutandis to acts preparatory to an offence under subsection (1) above.

Section 317
Disruption of telecommunications facilities
(1) Whosoever prevents or endangers the operation of a telecommunications facility which serves public purposes by destroying, damaging, removing, altering or rendering unusable an object which serves its operation, or taps electrical power intended for its operation shall be liable to imprisonment not exceeding five years or a fine.
(2) The attempt shall be punishable.
(3) Whosoever commits the offence negligently shall be liable to imprisonment not exceeding one year or a fine.

Act on Copyright and Related Rights (Copyright Act; Urheberrechtsgesetz - UrhG)

Full citation: Copyright Act of 9 September 1965 (Federal Law Gazette Part I, p. 1273), as last amended by Article 1 of the Act of 14 December 2012 (Federal Law Gazette Part I, p. 2579)

Article 106
Unlawful exploitation of copyrighted works
(1) Anyone who without the consent of the rightholder reproduces, distributes or communicates to the public a work or an adaptation or transformation of a work in manners other than those permitted by law shall be liable to imprisonment of not more than 3 years or a fine.
(2) Any attempt shall be punishable.

Article 107
Unlawful affixing of designation of author
(1) Any person who
1. without the consent of the author affixes to the original of an artistic work the designation of author (Article 10 (1)) or distributes an original bearing such designation,
2. affixes to a copy, an adaptation or transformation of an artistic work the designation of author (Article 10 (1)) in a manner which gives the copy, adaptation or transformation the appearance of an original, or distributes a copy, such an adaptation or transformation bearing such designation,

shall be liable to imprisonment of not more than three years or a fine, unless other provisions impose a more serious sentence.
(2) Any attempt shall be punishable.

Article 108
Infringement of related rights
(1) Any person who without the consent of the rightholder
1. reproduces, distributes or communicates to the public a scientific edition (Article 70) or an adaptation or transformation of such an edition,
2. exploits a posthumous work or an adaptation or transformation of such a work contrary to Article 71,
3. reproduces, distributes or communicates to the public a photograph (Article 72) or an adaptation or transformation of a photograph,
4. exploits a performance by a performer contrary to Article 77 (1) or (2), first sentence, Article 78 (1),
5. exploits an audio recording contrary to Article 85,
6. exploits a broadcast contrary to Article 87,
7. exploits a video recording or a video and audio recording contrary to Articles 94 or 95 read in conjunction with Article 94,
8. exploits a database contrary to Article 87b (1),

in manners other than those permitted by law shall be liable to imprisonment of not more than three years or a fine.
(2) Any attempt shall be punishable.

Article 108a
Unlawful exploitation on a commercial scale
(1) Where the offender in the cases referred to in Articles 106 to 108 acts on a commercial basis, the penalty shall be imprisonment of not more than five years or a fine.
(2) Any attempt shall be punishable.

Article 108b
Infringement of technological measures and rights-management information
(1) Any person who,
1. with the intention of enabling for himself or a third party access to a work which is protected under this Act or to other subject-matter protected under this Act or its exploitation, circumvents an effective technological measure without the consent of the rightholder, or
2. knowingly without authorisation
a) removes or alters rights-management information provided by rightholders, if any of the information concerned is affixed to a copy of a work or of other protected subject-matter, or is released in the context of the communication to the public of such a work or protected subject-matter, or
b) distributes, imports for distribution, broadcasts, communicates to the public or makes available to the public a work or other protected subject-matter where rights-management information was removed or altered without authorisation
by doing so, has at least carelessly induced, enabled, facilitated or concealed an infringement of copyright or related rights,
if the offence was not committed exclusively for the personal private use of the offender or of persons personally associated with the offender or does not relate to such use, shall be liable to imprisonment of not more than one year or a fine.
(2) Punishment shall also be imposed on any person who in violation of Article 95a (3) produces, imports, distributes, sells or rents a device, a product or component for commercial purposes.
(3) If in cases under paragraph (1) the offender acts on a commercial scale, the penalty shall be imprisonment of not more than three years or a fine.

Code of Criminal Procedure (Strafprozessordnung – StPO)

Full citation: Code of Criminal Procedure in the version published on 7 April 1987 (Federal Law Gazette [Bundesgesetzblatt] Part I p. 1074, 1319), as most recently amended by Article 1 of the Act of 21 January 2013 (Federal Law Gazette [Bundesgesetzblatt] Part I p. 89)

Section 94
[Objects Which May Be Seized]
(1) Objects which may be of importance as evidence for the investigation shall be impounded or otherwise secured.
(2) Such objects shall be seized if in the custody of a person and not surrendered voluntarily.
(3) Subsections (1) and (2) shall also apply to driver's licences which are subject to confiscation.

Section 95
[Obligation to Surrender]
(1) A person who has an object of the above-mentioned kind in his custody shall be obliged to produce it and to surrender it upon request.
(2) In the case of non-compliance, the regulatory and coercive measures set out in Section 70 may be used against such person. This shall not apply to persons who are entitled to refuse to testify.

Section 96
[Official Documents]
Submission or surrender of files or other documents officially impounded by authorities or public officials may not be requested if their highest superior authority declares that publication of the content of these files or documents would be detrimental to the welfare of the Federation or of a German *Land*. The first sentence shall apply *mutatis mutandis* to files and other documents held in the custody of a Member of the Federal Parliament or of a *Land* parliament or of an employee of a Federal or *Land* parliamentary group where the agency responsible for authorizing testimony has made a corresponding declaration.

Section 97
[Objects Not Subject to Seizure]
(1) The following objects shall not be subject to seizure:
1. written correspondence between the accused and the persons who, according to Section 52 or Section 53 subsection (1), first sentence, numbers 1 to 3b, may refuse to testify;
2. notes made by the persons specified in Section 53 subsection (1), first sentence, numbers 1 to 3b, concerning confidential information entrusted to them by the accused or concerning other circumstances covered by the right of refusal to testify;

3. other objects, including the findings of medical examinations, which are covered by the right of the persons mentioned in Section 53 subsection (1), first sentence, numbers 1 to 3b, to refuse to testify.
(2) These restrictions shall apply only if these objects are in the custody of a person entitled to refuse to testify unless the object concerned is an electronic health card as defined in section 291a of Part Five of the Social Code. Objects covered by the right of physicians, dentists, psychological psychotherapists, psychotherapists specializing in the treatment of children and juveniles, pharmacists and midwives to refuse to testify shall not be subject to seizure either if they are in the custody of a hospital or a service provider which collects, processes or uses personal data for the persons listed, nor shall objects to which the right of the persons mentioned in Section 53 subsection (1), first sentence, numbers 3a and 3b, to refuse to testify extends, be subject to seizure if they are in the custody of the counselling agency referred to in that provision. The restrictions on seizure shall not apply if certain facts substantiate the suspicion that the person entitled to refuse to testify participated in the criminal offence, or in accessoryship after the fact, obstruction of justice or handling stolen goods, or where the objects concerned have been obtained by means of a criminal offence or have been used or are intended for use in perpetrating a criminal offence, or where they emanate from a criminal offence.
(3) Insofar as the assistants (Section 53a) of the persons mentioned in Section 53a subsection (1), first sentence, numbers 1 to 3b, have a right to refuse to testify, subsections (1) and (2) shall apply *mutatis mutandis*.
(4) The seizure of objects shall be inadmissible insofar as they are covered by the right of the persons mentioned in Section 53 subsection (1), first sentence, number 4, to refuse to testify. This protection from seizure shall also extend to objects which the persons mentioned in Section 53 subsection (1), first sentence, number 4, have entrusted to their assistants (Section 53a). The first sentence shall apply *mutatis mutandis* insofar as the assistants (Section 53a) of the persons mentioned in Section 53 subsection (1), first sentence, number 4, have a right to refuse to testify.
(5) The seizure of documents, sound, image and data media, illustrations and other images in the custody of persons referred to in Section 53 subsection (1), first sentence, number 5, or of the editorial office, the publishing house, the printing works or the broadcasting company, shall be inadmissible insofar as they are covered by the right of such persons to refuse to testify. Subsection (2), third sentence, and Section 160a subsection (4), second sentence, shall apply *mutatis mutandis*; in these cases, too, seizure shall only be admissible, however, where it is not disproportionate to the importance of the case having regard to the basic rights arising out of Article 5 paragraph (1), second sentence, of the Basic Law, and the investigation of the factual circumstances or the establishment of the whereabouts of the perpetrator would otherwise offer no prospect of success or be much more difficult.

Section 98
[Order of Seizure]
(1) Seizure may be ordered only by the court and, in exigent circumstances, by the public prosecution office and the officials assisting it (section 152 of the Courts Constitution Act). Seizure pursuant to Section 97 subsection (5), second sentence, in the premises of an editorial office, publishing house, printing works or broadcasting company may be ordered only by the court.
(2) An official who has seized an object without a court order shall apply for court confirmation within three days if neither the person concerned nor an adult relative was present at the time of seizure, or if the person concerned and, if he was absent, an adult relative of that person expressly objected to the seizure. The person concerned may at any time apply for a court decision. The competence of the court shall be determined by Section 162. The person concerned may also submit the application to the Local Court in whose district the seizure took place, which shall then forward the application to the competent court. The person concerned shall be instructed as to his rights.
(3) Where after public charges have been preferred, the public prosecution office or one of the officials assisting has effected seizure, the court shall be notified of the seizure within three days; the objects seized shall be put at its disposal.
(4) If it is necessary to effect seizure in an official building or an installation of the Federal Armed Forces which is not open to the general public, the superior official agency of the Federal Armed Forces shall be requested to carry out such seizure. The agency making the request shall be entitled to participate. No such request shall be necessary if the seizure is to be made in places which are inhabited exclusively by persons other than members of the Federal Armed Forces.

Section 98a
[Automated Comparison and Transmission of Personal Data]
(1) Notwithstanding Sections 94, 110 and 161, where there are sufficient factual indications to show that a criminal offence of substantial significance has been committed
1. relating to the illegal trade in narcotics or weapons or the counterfeiting of money or official stamps,
2. relating to national security (sections 74a, 120 of the Courts Constitution Act),
3. relating to offences which pose a danger to the general public,
4. relating to endangerment of life and limb, sexual self-determination or personal liberty,
5. on a commercial or habitual basis, or
6. by a member of a gang or in some other organized way,

personal data relating to individuals who manifest certain significant features which may be presumed to apply to the perpetrator may be 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 determining the perpetrator's whereabouts would offer much less prospect of success or be much more difficult.
(2) For the purposes of subsection (1), the storing agency shall extract from the database the data required for matching purposes and transmit it to the criminal prosecuting authorities.
(3) Insofar as isolating the data for transmission from other data requires disproportionate effort, the other data shall, upon order, also be transmitted. Their use shall not be admissible.
(4) Upon request by the public prosecution office, the storing agency shall assist the agency effecting the comparison.
(5) Section 95 subsection (2) shall apply *mutatis mutandis*.

Section 98b
[Competence; Return and Deletion of Data]
(1) 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. The order shall be made in writing. It shall name the person obliged to transmit the data and shall be limited to the data and comparison characteristics required for the particular case. The transmission of data may not be ordered where special rules on use, being provisions under Federal law or under the corresponding *Land* law, present an obstacle to their use. Sections 96 and 97, and Section 98 subsection (1), second sentence, shall apply *mutatis mutandis*.
(2) Regulatory and coercive measures (Section 95 subsection (2)) may be ordered only by the court and, in exigent circumstances, also by the public prosecution office; the imposition of detention shall be reserved to the court.
(3) 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.
(4) Upon completion of a measure pursuant to Section 98a, the agency responsible for monitoring compliance with data protection rules by public bodies shall be notified.

Section 98c
[Comparison of Data to Clear Up a Criminal Offence]
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. Special rules on use presenting an obstacle thereto, being provisions under Federal law or under the corresponding *Land* law, shall remain unaffected.

Section 99
[Seizure of Postal Items]
Seizure of postal items and telegrams addressed to the accused which are held in the custody of persons or enterprises providing, or collaborating in the provision of, postal or telecommunications services on a commercial basis shall be admissible. Seizure of postal items and telegrams shall also be admissible where known facts support the conclusion that they originate from the accused or are intended for him and that their content is of relevance to the investigation.

Section 100
[Jurisdiction]
(1) Only the court and, in exigent circumstances the public prosecution office, shall be authorized to implement seizure (Section 99).
(2) A seizure ordered by the public prosecution office, even if it has not yet resulted in a delivery, shall become ineffective if it is not confirmed by the court within three working days.
(3) The court shall have the authority to open the delivered post. The court may transfer this authority to the public prosecution office insofar as this is necessary so as not to endanger the success of the investigation by delay. The transfer shall not be contestable; it may be revoked at any time. So long as no order has been made pursuant to the second sentence, the public prosecution office shall immediately forward the delivered postal items to the court, leaving any unopened postal items sealed.
(4) The court competent pursuant to Section 98 shall decide on a seizure ordered by the public prosecution office. The court which ordered or confirmed the seizure shall decide whether to open an item that has been delivered.
(5) Postal items in respect of which no order to open them has been made are to be forwarded to the intended recipient without delay. The same shall apply insofar as there is no necessity to retain the postal items once opened.
(6) Such part of a retained postal item as does not appear expedient to withhold for the purposes of the investigation is to be transmitted to the intended recipient in the form of a copy.

Section 100a
[Conditions Regarding Interception of Telecommunications]
(1) Telecommunications may be intercepted and recorded also without the knowledge of the persons concerned if

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

(2) Serious criminal offences for the purposes of subsection (1), number 1, shall be:
1. pursuant to the Criminal Code:
a) crimes against peace, high treason, endangering the democratic state based on the rule of law, treason and endangering external security pursuant to sections 80 to 82, 84 to 86, 87 to 89a and 94 to 100a;
b) bribery of a member of parliament pursuant to section 108e;
c) crimes against the national defence pursuant to sections 109d to 109h;
d) crimes against public order pursuant to sections 129 to 130;
e) counterfeiting money and official stamps pursuant to sections 146 and 151, in each case also in conjunction with section 152, as well as section 152a subsection (3) and section 152b subsections (1) to (4);
f) crimes against sexual self-determination in the cases referred to in sections 176a, 176b, 177 subsection (2), number 2, and section 179 subsection (5), number 2;
g) dissemination, purchase and possession of pornographic writings involving children and involving juveniles, pursuant to section 184b subsections (1) to (3), section 184c subsection (3);
h) murder and manslaughter pursuant to sections 211 and 212;
i) crimes against personal liberty pursuant to sections 232 to 233a, 234, 234a, 239a and 239b;
j) gang theft pursuant to section 244 subsection (1), number 2, and aggravated gang theft pursuant to section 244a;
k) crimes of robbery or extortion pursuant to sections 249 to 255;
l) commercial handling of stolen goods, gang handling of stolen goods and commercial gang handling of stolen goods pursuant to sections 260 and 260a;
m) money laundering or concealment of unlawfully acquired assets pursuant to section 261 subsections (1), (2) and (4);
n) fraud and computer fraud subject to the conditions set out in section 263 subsection (3), second sentence, and in the case of section 263 subsection (5), each also in conjunction with section 263a subsection (2);
o) subsidy fraud subject to the conditions set out in section 264 subsection (2), second sentence, and in the case of section 264 subsection (3), in conjunction with section 263 subsection (5);
p) criminal offences involving falsification of documents under the conditions set out in section 267 subsection (3), second sentence, and in the case of section 267 subsection (4), in each case also in conjunction with section 268 subsection (5) or section 269 subsection (3), as well as pursuant to sections 275 subsection (2) and section 276 subsection (2);
q) bankruptcy subject to the conditions set out in section 283a, second sentence;
r) crimes against competition pursuant to section 298 and, subject to the conditions set out in section 300, second sentence, pursuant to section 299;
s) crimes endangering public safety in the cases referred to in sections 306 to 306c, section 307 subsections (1) to (3), section 308 subsections (1) to (3), section 309 subsections (1) to (4), section 310 subsection (1), sections 313, 314, 315 subsection (3), section 315b subsection (3), as well as sections 361a and 361c;
t) taking and offering a bribe pursuant to sections 332 and 334;
2. pursuant to the Fiscal Code:
a) tax evasion under the conditions set out in section 370 subsection (3), second sentence, number 5;
b) commercial, violent and gang smuggling pursuant to section 373;
c) handling tax-evaded property as defined in section 374 subsection (2);
3. pursuant to the Pharmaceutical Products Act:
criminal offences pursuant to section 95 subsection (1), number 2a, subject to the conditions set out in section 95 subsection (3), second sentence, number 2, letter b;
4. pursuant to the Asylum Procedure Act:
a) inducing an abusive application for asylum pursuant to section 84 subsection (3);
b) commercial and gang inducement to make an abusive application for asylum pursuant to section 84a;
5. pursuant to the Residence Act:
a) smuggling of aliens pursuant to section 96 subsection (2);
b) smuggling resulting in death and commercial and gang smuggling pursuant to section 97;
6. pursuant to the Foreign Trade and Payments Act:
criminal offences pursuant to section 34 subsections (1) to (6);
7. pursuant to the Narcotics Act:
a) criminal offences pursuant to one of the provisions referred to in section 29 subsection (3), second sentence, number 1, subject to the conditions set out therein;
b) criminal offences pursuant to section 29a, section 30 subsection (1), numbers 1, 2 and 4, as well as sections 30a and 30b;

8. pursuant to the Precursors Control Act:
criminal offences pursuant to section 19 subsection (1), subject to the conditions set out in section 19 subsection (3), second sentence;
9. pursuant to the War Weapons Control Act:
a) criminal offences pursuant to section 19 subsections (1) to (3) and section 20 subsections (1) and (2), as well as section 20a subsections (1) to (3), each also in conjunction with section 21;
b) criminal offences pursuant to section 22a subsections (1) to (3);
10. pursuant to the Code of Crimes against International Law:
a) genocide pursuant to section 6;
b) crimes against humanity pursuant to section 7;
c) war crimes pursuant to sections 8 to 12;
11. pursuant to the Weapons Act:
a) criminal offences pursuant to section 51 subsections (1) to (3);
b) criminal offences pursuant to section 52 subsection (1), number 1 and number 2, letters c and d, as well as section 52 subsections (5) and (6).
(3) Such order may be made only against the accused or against persons in respect of whom it may be assumed, on the basis of certain facts, that they are receiving or transmitting messages intended for, or transmitted by, the accused, or that the accused is using their telephone connection.
(4) 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.

Section 100b
[Order to Intercept Telecommunications]
(1) Measures pursuant to Section 100a may be ordered by the court only upon application by the public prosecution office. 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. 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.
(2) The order shall be given in writing. The operative part of the order shall indicate
1. where known, the name and address of the person against whom the measure is directed;
2. the telephone number or other code of the telephone connection or terminal equipment to be intercepted, insofar as there are no particular facts indicating that they are not at the same time assigned to another piece of terminal equipment;
3. the type, extent and duration of the measure specifying the time at which it will be concluded.
(3) On the basis of this order all persons providing, or contributing to the provision of, telecommunications services on a commercial basis shall enable the court, the public prosecution office and officials working in the police force to assist it (section 152 of the Courts Constitution Act), to implement measures pursuant to Section 100a and shall provide the required information without delay. Whether and to what extent measures are to be taken in this respect shall follow from the Telecommunications Act and from the Telecommunications Interception Ordinance issued thereunder. Section 95 subsection (2) shall apply *mutatis mutandis*.
(4) If the conditions for making the order no longer prevail, the measures implemented on the basis of the order shall be terminated without delay. Upon termination of the measure, the court which issued the order shall be notified of the results thereof.
(5) The *Länder* and the Federal Public Prosecutor General shall submit a report to the Federal Office of Justice every calendar year by the 30th June of the year following the reporting year, concerning measures ordered pursuant to Section 100a within their area of competence. The Federal Office of Justice shall produce a summary of the measures ordered nationwide during the reporting year and shall publish it on the Internet.
(6) The reports pursuant to subsection (5) shall indicate:
1. the number of proceedings in which measures were ordered pursuant to Section 100a subsection (1);
2. the number of orders to intercept telecommunications pursuant to Section 100a subsection (1), distinguishing between
a) initial and follow-up orders, as well as
b) fixed, mobile and Internet telecommunication;
3. in each case the underlying criminal offence by reference to the categories listed in Section 100a subsection (2).

Section 102
[Search in Respect of the Suspect]
A body search, a search of the property and of the private and other premises of a person who, as a perpetrator or as an inciter or accessory before the fact, is suspected of committing a criminal offence, or is suspected of accessoryship after the fact or of obstruction of justice or of handling stolen goods, may be made for the purpose of his apprehension, as well as in cases where it may be presumed that the search will lead to the discovery of evidence.

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*.

Section 247a
[Witness Examination in Another Place]
If there is an imminent risk of serious detriment to the well-being of the witness were he to be examined in the presence of those attending the main hearing, the court may order that the witness remain in another place during the examination; such an order shall also be admissible under the conditions set out in Section 251 subsection (2), insofar as this is necessary to establish the truth. The decision shall be incontestable. A simultaneous audio-visual transmission of the testimony shall be provided in the courtroom. The testimony shall be recorded if there is a concern that the witness will not be available for examination at a future main hearing and the recording is necessary for establishing the truth. Section 58a subsection (2) shall apply *mutatis mutandis*.

Section 251
[Reading Out Records]
(1) Examination of a witness, expert or co-accused may be replaced by reading out a record of another examination or a certificate containing a written statement originating from him
1. if the defendant has defence counsel, and the public prosecutor, defence counsel and defendant agree;
2. if the witness, expert or co-accused has died or cannot be examined by the court for another reason within a foreseeable period of time;
3. insofar as the written record or certificate concerns the presence or the level of asset loss.
(2) Examination of a witness, expert, or co-accused may also be replaced by reading out the written record of his previous examination by a judge if
1. illness, infirmity, or other insurmountable impediments prevent the witness, expert or co-accused from appearing at the main hearing for a long or indefinite period;
2. the witness or expert cannot reasonably be expected to appear at the main hearing given the great distance involved, having regard to the importance of his statement;
3. the public prosecutor, defence counsel and the accused agree to the reading out.
(3) Where the reading is to serve purposes other than specifically reaching a judgment, particularly the purpose of preparing the decision as to whether an individual is to be summoned and examined, records of examinations, certificates and other documents serving as evidence may otherwise be read out too.
(4) In the cases referred to in subsections (1) and (2), the court shall decide whether reading out shall be ordered. The reason for reading out shall be indicated. If the written record of a judicial examination is read out, it shall be stated whether the person concerned was examined under oath. If not, an oath shall be administered retrospectively where the court deems this necessary and an oath can still be administered.

Act on International Cooperation in Criminal Matters (Gesetz über die internationale Zusammenarbeit in Strafsachen – IRG)

Act on International Cooperation in Criminal Matters of 23 December 1982 (Federal Law Gazette I page 2071), as last amended by Article 1 of the Act of 21 July 2012, Federal Law Gazette I, 1566).

Section 1
Scope of Application
(1) This Act shall govern the relations with foreign States regarding legal assistance in criminal matters.
(2) Criminal matters under this Act shall include proceedings resulting from an offence which under German law would constitute a regulatory offence sanctionable by a fine or which pursuant to foreign law is subject to a similar penalty, provided that a court of criminal jurisdiction determines the sentence.

(3) Provisions of international treaties shall take precedence before the provisions of this law to the extent that they have become directly applicable national law.
(4) This Act shall govern the support in criminal proceedings involving a Member State of the European Union.

Section 59
Admissibility of Assistance
(1) At the request of a competent authority of a foreign State, other legal assistance in a criminal matter may be provided.
(2) Legal assistance within the meaning of subsection (1) above shall be any kind of support given for foreign criminal proceedings regardless of whether the foreign proceedings are conducted by a court or by an executive authority and whether the legal assistance is to be provided by a court or by an executive authority.
(3) Legal assistance may be provided only in those cases in which German courts and executive authorities could render mutual legal assistance to each other.

Section 60
Rendering Assistance
If the executive authority responsible for granting legal assistance determines that the requirements for rendering legal assistance have been fulfilled, the executive authority responsible for rendering the legal assistance shall be bound by such determination, without prejudice to s. 61.
Section 61 a
Transmission of Personal Data Without Request
(1) Courts and the public prosecution service may transmit personal data from criminal proceedings to the public authorities of another State as well as to Inter-State and supranational authorities without request by the latter if
1. transmission without request to a German court or to a German public prosecution service were admissible,
2. facts exist which warrant the expectation that the transmission is necessary
a) in order to prepare a request by the receiving State for assistance for the purpose of prosecution or enforcement of a sentence for an offence which would be punishable by a maximum term of more than five years' imprisonment under German law, and the conditions for granting assistance on request would be fulfilled if such a request was made or
b) in the individual case to avert a danger to the existence or security of the State, or to the life, limb or freedom of a person, or to property of significant value, protection of which is in the public interest, or to prevent a crime as described under a) above, and
3. the public authority to which the data are transmitted is competent to implement the appropriate measures under no. 2 above.
If an adequate level of data protection is ensured in the receiving State, the 1st sentence no. 2 a) above shall apply with the proviso that an offence punishable under German law by a maximum term of more than five years' imprisonment shall be substituted by an offence of significant gravity.
(2) The transmission shall occur under the condition that
1. time limits pursuant to German law for data deletion and for review of data deletion will be observed,
2. transmitted data will only be used for the purposes for which they were transmitted and
3. transmitted data will be deleted or corrected immediately upon information in accordance with subsection (4) below.
(3) Transmission shall be precluded if it is evident to the court or the public prosecution service that – taking into consideration the special public interest in the transmission – the protected interests of the person demand the preclusion of the transmission in the individual case; the protected interests of the person concerned include the existence of an adequate level of data protection in the receiving State.
(4) The receiving authority shall be notified without undue delay upon discovery that the transmission of data was inadmissible or that the transmitted data were incorrect.

Section 61 c
Audiovisual Examination
A witness or an expert who fails to appear for examination by a foreign legal authority by use of a video conference although properly summoned shall neither be charged with the costs arising from his failure to appear nor have any penalty for contempt imposed upon him.
Section 67
Search and Seizure
(1) Objects that may be considered for handing over to a foreign State may be seized or otherwise secured even prior to the receipt of the request for surrender. To this end, a search may be conducted.
(2) If the conditions specified in s. 66(1) no. 1 and (2) no. 1 apply, objects may also be seized or otherwise secured if necessary for the enforcement of a request which is not directed at the handing over of the objects. Subsection (1) 2nd sentence above shall apply mutatis mutandis.
(3) The Amtsgericht in whose district they are to be performed shall have jurisdiction to order the search and seizure. S. 61(2) 2nd sentence shall apply mutatis mutandis.

(4) If cases of emergency the public prosecution service or its agents (s. 152 of the Gerichtsverfassungsgesetz) may order the search and seizure.

Section 74
Federal Jurisdiction
(1) The Bundesministerium der Justiz with the consent of the Auswärtiges Amt and other federal ministries whose portfolio would be affected by the legal assistance shall decide on foreign requests for legal assistance and on requests to foreign States for legal assistance. If an authority responsible for rendering legal assistance falls within the portfolio of another federal ministry, that ministry shall take the place of the Bundesministerium der Justiz. The federal ministries responsible pursuant to the 1st and 2nd sentences above may delegate the exercise of their powers to federal authorities subordinate to them. The Bundesamt für Justiz shall decide on requests under subparagraphs 2 and 3 of Paragraph 2 of Part IX of this Act.
(2) The Bundesregierung may delegate the exercise of the power to decide on foreign requests for legal assistance and to request foreign States for legal assistance by way of an agreement to the Landesregierungen. The Landesregierungen shall have the right to delegate their powers further.
(3) The powers of the Bundeskriminalamt to transmit data, to place a person or an object on a „wanted"-list and to establish a person's identity at the request of a foreign State shall be governed by s. 14(1) 1st sentence no. 2 and 15(1) to (3) of the Bundeskriminalamtgesetz.

Section 77 a
Electronic Communication and Dossier
(1) If under this Act the provision of legal assistance requires the submission of written documentation including originals or certified copies, the submission of electronic documents shall suffice if so provided for by secondary legislation under s. 77 b. The electronic documents shall contain a qualified electronic signature under the Signaturgesetz and must be fit for use by an authority or court. The same shall apply to declarations, applications or justifications which under this Act are explicitly required to be in writing or signed.
(2) The qualified electronic signature may be substituted by another secure procedure which ensures the authenticity and integrity of the transmitted electronic documents.
(3) An electronic document shall be deemed to have been received as soon as the receiving facility of the authority or court has recorded it. If a transmitted document is not fit for use the sender shall be informed of this without undue delay together with instructions about the valid technical parameters. Unless the use of an electronic dossier has been approved under subsection (4) below, a hard copy of the electronic document shall be made without undue delay.
(4) An electronic dossier may be kept if this has been approved by secondary legislation under s. 77 b. Documents and objects for inspection (originals) handed in to the electronic dossier and fit for transposing shall be transposed into an electronic document in order to replace the original unless the secondary legislation under s. 77 b provides otherwise. The electronic document must contain a notice about when and by whom the original was transposed. The originals shall be stored until the end of the proceedings so that they may be produced upon request within a week.
(5) An electronic document created under subsection (4) 2nd and 3rd sentences above shall be used for the purpose of the proceedings unless there is cause to doubt that it is identical to the original.
(6) If the electronic document created under subsection (1) above in addition to the notice under subsection (4) 3rd sentence above contains a notice bearing a qualified electronic signature
1. to the effect that the onscreen display is in content and appearance identical to the original and
2. as to whether the original or a certified copy of it had been present for the transposal, the original may be destroyed before the end of the proceedings. Under the conditions of the 1st sentence above declarations of the person concerned and of third parties internal to the proceedings and any attached simple copies may be destroyed.
(7) Ss. 110 c to 110 e of the Ordnungswidrigkeitengesetz shall apply mutatis mutandis.

Section 77 b
Authorisation to Pass Secondary Legislation
The Bundesministerium der Justiz and the Landesregierungen shall determine within their remit of competence through secondary legislation
1. the date and time after which electronic documents may be submitted under s. 77 a(1),
2. the signature requirements for the transmission of the electronic documents under s. 77 a(2) and the required form,
3. the date and time after which dossiers are to be or may be kept electronically under s. 77 a(4),
4. the organisational-technical parameters for the creation, maintenance and storage of the electronic dossiers including the exceptions from the replacement of the original under s. 77 a(4),
5. the originals which in variance from s. 77 a(6) shall continue to be stored.

The Landesregierungen may delegate the authorisation by secondary legislation to the authorities in charge of the State administration of justice. Electronic transmission under s. 77 a(1) may be restricted to individual courts and authorities as well as

proceedings. The use of an electronic dossier under s. 77 a(4) may be restricted to proceedings before individual authorities or to different stages of proceedings.

Section 92

Data Transmission Without Request

(1) To the extent that an international agreement so provides public authorities may transmit without request personal data that give rise to the suspicion that an offence has been committed, to public authorities of another Member State of the European Union as well as organs and institutions of the European Communities, if

1. a transmission without request to a German court or prosecution service were permissible and
2. the transmission is useful in
a) initiating criminal proceedings in another Member State or
b) assisting criminal proceedings already pending there and
3. the authority to whom the data are transmitted has jurisdiction for the measures under no.2 above.

(2) S. 61 a(2) to (4) shall apply mutatis mutandis.

[nicht aktuell §§ 92 – 92c IRG]

Section 94

Requests for Freezing, Seizure and Search

(1) Ss. 58(3) and 67 shall apply to requests pursuant to Council Framework Decision 2003/577/JHA of 22 July 2003 on the execution in the European Union of orders freezing property or evidence (OJ L 196/45) with the proviso

1. that double criminality shall not need to be established if the offence on which the request is based is under the law of the requesting State punishable by a custodial sanction with a maximum term of no less than three years and is listed in one of the categories of offences listed in article 3(2) of the Council Framework Decision 2003/577/JHA,
2. that a request in tax, duties, customs and currency matters shall also be admissible if the German law does not provide for equivalent taxes or duties or does not contain similar tax, duties, customs or currency provisions as the law of the requesting Member State.

(2) The granting of requests under subsection (1) above shall be inadmissible if

1. a ban on seizure exists pursuant to s. 77(1) in conjunction with s. 97 of the Strafprozessordnung or
2. the convicted person has already been finally tried for the same offence on which the request is based by another State than the requesting Member State provided that the sanction has already been enforced, is currently being enforced or can no longer be enforced under the law of the convicting State.

This shall not apply if the request serves the preparation of an order for confiscation or deprivation and if deprivation or confiscation could have been ordered separately under s. 76 a of the Strafgesetzbuch.

(3) The granting of requests for measures under s. 58(3) and s. 67 may be stayed as long as

1. it could jeopardise ongoing criminal investigations and
2. the objects to which the request attaches have been seized or otherwise secured for other criminal proceedings.

Section 97

Requests for Pieces of Evidence

S. 94(1) shall apply mutatis mutandis to requests by Member States for the handing over of objects which may serve as evidence in proceedings in the requesting Member State and which may be seized or otherwise secured pursuant to Council Framework Decision 2003/577/JHA of 22 July 2003 on the execution in the European Union of orders freezing property or evidence.

Telemedia Act (Telemediengesetz)

Full citation: The Act was adopted by the Bundestag as Article 1 of the Act of 26 February 2007 I 179. It entered into force on 1 March 2007 pursuant to Article 5 sentence 1 of this Act in conjunction with the Notification of 1 March 2007 I 251 (Federal Gazette I, p. 179)

Section 7 General principles

(1) Service providers shall be responsible for their own information which they keep ready for use, in accordance with general legislation.

.. .

(2) Service providers within the meaning of Sections 8 to 10 are not required to monitor the information transmitted or stored by them or to search for circumstances indicating an illegal activity. This shall be without prejudice to obligations to remove or disable access to information under general legislation, even where the service provider does not bear responsibility pursuant to Sections 8 to 10. Privacy of telecommunications pursuant to Section 88 of the Telecommunications Act must be maintained.

Section 8 Acting as a conduit of information
(1) Service providers shall not be responsible for the information of third parties which they transmit in a communication network or to which they give access, as long as they
1. have not initiated the transmission,
2. have not selected the addressee of the transmitted information, and
3. have not selected or modified the transmitted information.
Sentence 1 shall not apply when the service provider deliberately works together with a recipient of his service to commit illegal acts.
(2) The transmission of information pursuant to Sub-section 1 and the provision of access to it includes the automatic, intermediate and transient storage of this information, in so far as this takes place for the sole purpose of carrying out the transmission in the communication network and the information is not stored for any period longer than is reasonably necessary for the transmission.

Section 9 Temporary storage for the accelerated transmission of information
Service providers shall not be responsible for automatic, intermediate and temporary storage which serves the sole purpose of making more efficient the information's onward transmission to other recipients on their request, as long as they
do not modify the information,
comply with conditions on access to the information,
comply with rules regarding the updating of the information, specified in a manner
widely recognised and used by industry,
do not interfere with the lawful use of technology, stipulated in widely recognised and
used industrial standards, to obtain data on the use of the information, and
act expeditiously to remove or to disable access to the information they have stored
within the meaning of this provision upon obtaining knowledge of the fact that the information at the initial source of the transmission has been removed from the network
.. .
or that access to it has been disabled, or that a court or administrative authority has
ordered such removal or disablement. Section 8 (1) sentence 2 applies mutatis mutandis.

Section 10 Storing of information
Service providers shall not be responsible for the information of third parties which they store for a recipient of a service, as long as they have no knowledge of the illegal activity or the information and, as regards claims for damages, are not aware of any facts or circumstances from which the illegal activity or the information is apparent, or upon obtaining such knowledge, have acted expeditiously to remove the information or to disable access to it. Sentence 1 shall not apply when the recipient of the service is acting under the authority or control of the service provider.

Appendix 2: Select Bibliography

Ambos §§ 3 et seq. in Münchener Kommentar zum Strafgesetzbuch, 2nd ed. (2011)

Bär Transnationaler Zugriff auf Computerdaten, Zeitschrift für Internationale Strafrechtsdogmatik 2011, 53

Bär Handbuch zur EDV-Beweissicherung (2007)

Brodowski/Freiling Cyberkriminalität, Computerstrafrecht und die digitale Schattenwirtschaft (2011)

Gercke Straftaten und Strafverfolgung im Internet, Goltdammer's Archiv für Strafrecht 2012, 474

Gercke Die Entwicklung des Internetstrafrechts 2010/2011, Zeitschrift für Urheber- und Medienrecht 2011, 609

Gercke Zur Zulässigkeit sog. Transborder Searches – Der strafprozessuale Zugriff auf im Ausland gespeicherte Daten, Strafverteidiger-Forum 2009, 271

Gercke/Brunst Praxishandbuch Internetstrafrecht (2009)

Graf Strafprozessordnung. Kommentar, 2nd ed. (2012)

Hackner/Schierholt Internationale Rechtshilfe in Strafsachen. Ein Leitfaden für die Praxis, 2nd ed. (2012)

Hilgendorf/Frank/Valerius Computer- und Internetstrafrecht (2005)

Hilgendorf Überlegungen zur strafrechtlichen Interpretation des Ubiquitätsprinzips im Zeitalter des Internets, Neue Juristisch Wochenschrift 1997, 1873

Malek Strafsachen im Internet (2005)

Meyer-Goßner Strafprozessordnung. Mit GVG und Nebengesetzen, 53rd ed. (2010)

Park Handbuch Durchsuchung und Beschlagnahme, 2nd Ed. 2009

Paul Primärrechtliche Regelungen zur Verantwortlichkeit von Internetprovidern aus strafrechtlicher Sicht (2005)

Roxin/Schünemann Strafverfahrensrecht, 27th ed. (2012)

Schomburg/Lagodny/Gleß/Hackner (Hrsg.), Internationale Rechtshilfe. Kommentar, 5th ed. (2012)

Sieber Gutachten C zum 69. Juristentag. Straftaten und Strafverfolgung im Internet (2012)

Sieber Straftaten und Strafverfolgung im Internet, NJW-Beilage 2012, 86

Sieber/Brüner/Satzger/v. Heintschel-Heinegg (eds.) Europäisches Strafrecht (2011)

Sieber/Nolde Sperrverfügungen im Internet (2008)

Vogel Informationstechnologische Herausforderungen an das Strafprozessrecht, ZIS 2012, 480

Werle/Jeßberger §§ 3 et seq., in Leipziger Kommentar zum Strafgesetzbuch, 12th ed., 2009.

Wörner Einseitiges Strafanwendungsrecht und entgrenztes Internet?, Zeitschrift für Internationale Strafrechtsdogmatik 2012, 458

Wolter (ed.) Systematischer Kommentar zur Strafprozessordnung. Mit GVG und EMRK, Band V §§ 246a – 295 StPO, 4th ed. (2012)