Project on Cybercrime
www.coe.int/cybercrime

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

First draft (1 June 2007)

Cybercrime legislation – country profile

Germany

This profile has been prepared within the framework of the Council of Europe's Project on Cybercrime in view of sharing information on cybercrime legislation and assessing the current state of implementation of the Convention on Cybercrime under national legislation. It does not necessarily reflect official positions of the country covered or of the Council of Europe.

Comments may be sent to:

Alexander Seger
Department of Technical Cooperation
Directorate General of Human Rights and Legal Affairs
Council of Europe, Strasbourg, France

Tel: +33-3-9021-4506
Fax: +33-3-9021-5650
Email: alexander.seger@coe.int
www.coe.int/cybercrime

Country:	**Germany**
Signature of Convention:	Yes: 23 November 2001
Ratification/accession:	No If not yet signed/acceded to: What measures are being undertaken in your country to become a Party? What specific obstacles (legislative or other) prevent ratification/accession? The necessary legislation for ratification is currently being prepared. However, before the Convention can be ratified, the process of implementation must be completed. In this respect, German law largely complies with the requirements of the Council of Europe Convention. However, a few amendments and changes to national law remain necessary. The implementation of the Convention will be effected through the following amendments to German law: • The Council of Europe's provisions regarding substantive criminal law – excluding the provision on content-related offences (Title 3 of the Council of Europe Convention) – is addressed by the German draft law against computer crime (BT-Drs. 16/3656) which was adopted by the Bundestag on 24 May 2007 (draft law regarding substantive criminal law). This law is also intended to cover the modifications introduced by the EU Framework Decision on attacks against information

	systems. • The Convention's provision on content-related offences (Title 3 of the Council of Europe Convention) is addressed by the German draft law to implement the EU Framework Decision on combating the sexual exploitation of children and child pornography (BT-Drs. 16/3439), which is currently under consideration in the Bundestag. • The Convention's provision regarding procedural law is addressed by the German draft law revising provisions on telecommunications surveillance and other covert investigative measures and implementing EU Directive 2006/24/EC (draft law regarding criminal procedural law). The draft law was adopted by the Federal Cabinet on 18 April 2007.
Provisions of the Convention	***Corrresponding provisions/solutions in national legislation*** *(pls quote or summarise briefly; pls attach relevant extracts as an appendix)*
Chapter I – Use of terms	
Article 1 – "Computer system", "computer data", "service provider", "traffic data"	Computer data are covered by section 202a (2) of the German Criminal Code (*Strafgesetzbuch*, StGB).
Chapter II – Measures to be taken at the national level *Section 1 – Substantive criminal law*	
Article 2 – Illegal access	Covered by section 202a (1) StGB.
Article 3 – Illegal interception	Currently covered in part by section 201 StGB as well as section 148 in connection with section 89 of the German Telecommunications Act (*Telekommunikationsgesetz*, TKG). Completely covered by the proposed section 202b of the draft law regarding substantive criminal law.
Article 4 – Data interference	Covered by section 303a StGB.
Article 5 – System interference	Covered in part by section 303b StGB. Amendment is necessary with regard to private computer systems and to the requirements of data input and transmission. This issue is addressed by the proposed amendment to section 303b in the draft law regarding substantive criminal law
Article 6 – Misuse of devices	Covered by the proposed section 202c in the draft law regarding substantive criminal law.
Article 7 – Computer-related forgery	Covered by section 269 StGB.
Article 8 – Computer-related fraud	Covered by section 263a StGB.
Article 9 – Offences related to child pornography	Covered in part by section 184b StGB. An amendment is necessary with respect to the age of the person involved (currently a person under the age of 14). This issue is addressed by the above-mentioned draft law to implement the EU Framework Decision on combating the

	sexual exploitation of children and child pornography.
Title 4 – Offences related to infringements of copyright and related rights	See below.
Article 10 – Offences related to infringements of copyright and related rights	Covered by sections 106 ff. of the German Copyright Act (*Urheberrechtsgesetz*, UrhG).
Article 11 – Attempt and aiding or abetting	Attempt is covered by sections 22-24 StGB. Aiding and abetting is covered by sections 26 and 27 StGB.
Article 12 – Corporate liability	Covered by sections 30 and 130 of the German Regulatory Offences Act (*Gesetz über Ordnungswidrigkeiten*, OWiG).
Article 13 – Sanctions and measures	Article 13 (1) is covered by the above-mentioned articles (sections 202a, 202b, 202c, 263a, 269, 303a, 303a StGB and section 106 UrhG). Article 13 (2) is covered by section 30 OWiG.
Section 2 – Procedural law	
Article 14 – Scope of procedural provisions	See below (Articles 16-21).
Article 15 – Conditions and safeguards	See below (Articles 16-21).
Article 16 – Expedited preservation of stored computer data	With respect to computer data, Article 16 is covered by sections 94, 95 and 98 of the German Code of Criminal Procedure (*Strafprozessordnung*, StPO). With respect to traffic data, Article 16 is covered in part by sections 100g and 100h StPO. The necessary amendment is addressed by the proposed amendment to section 100g in the draft law regarding criminal procedural law.
Article 17 – Expedited preservation and partial disclosure of traffic data	Covered in part by sections 100g and 100h StPO. The necessary amendments are addressed by the proposed amendment to section 100g in the draft law regarding criminal procedural law.
Article 18 – Production order	Article 18 (1) lit. a is covered by section 95 StPO. Article 18 (1) lit. b is covered by sections 112 and 113 TKG.
Article 19 – Search and seizure of stored computer data	Article 19 (1) and (3) are covered by sections 94, 95, 102, 103, 105, 161 and 163 StPO. Article 19 (2) is covered by the proposed amendment to section 110 (3) StPO in the draft law regarding criminal procedural law.
Article 20 – Real-time collection of traffic data	Covered in part by section 100g StPO. The necessary amendments are addressed by the proposed amendment to section 100g in the draft law regarding criminal procedural law.
Article 21 – Interception of content data	Covered by sections 100a and 100b StPO.
Section 3 – Jurisdiction	
Article 22 – Jurisdiction	Covered by sections 3-9 StGB.
Chapter III – International co-operation	
Article 24 – Extradition	Covered by sections 2 and 3 of the Act on International Legal Assistance in Criminal Matters (*Gesetz über die internationale Rechtshilfe in Strafsachen*, IRG) in the absence of applicable international agreements.

Article 25 – General principles relating to mutual assistance	Covered by provisions set forth in the IRG (e.g. sections 2 ff.: extradition; sections 59 ff.: other forms of mutual legal assistance).
Article 26 – Spontaneous information	Covered by sections 61a and 83j IRG in the absence of applicable international agreements.
Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements	Covered by sections 59 ff. IRG in the absence of applicable international agreements.
Article 28 – Confidentiality and limitation on use	Covered by sections 59 ff. IRG in the absence of applicable international agreements.
Article 29 – Expedited preservation of stored computer data	Covered by sections 66 f. IRG in the absence of applicable international agreements.
Article 30 – Expedited disclosure of preserved traffic data	Covered by sections 59 ff. IRG in the absence of applicable international agreements.
Article 31 – Mutual assistance regarding accessing of stored computer data	Covered by section 66 IRG in the absence of applicable international agreements.
Article 32 – Trans-border access to stored computer data with consent or where publicly available	Covered by section 94 StPO.
Article 33 – Mutual assistance in the real-time collection of traffic data	Covered by sections 59 ff. IRG in the absence of applicable international agreements.
Article 34 – Mutual assistance regarding the interception of content data	Covered by sections 59 ff. IRG in the absence of applicable international agreements.
Article 35 – 24/7 Network	Germany has established a 24/7 contact point within the Bundeskriminalamt. It is a member of the 24/7 Network of the "G8 High-Tech Crime Subgroup" and of the ICPO Interpol.
Article 42 – Reservations	

Appendix

A. German Criminal Code (*Strafgesetzbuch*, StGB):

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 that 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 defence:
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), number 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 that 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 proceedings 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), numbers 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 the purpose of sexual exploitation and for the purpose of the exploitation of workers and promotion of trafficking in human beings (sections 232 to 233a);
5. unauthorised distribution of narcotics;
6. dissemination of pornographic writings in cases under sections 184a and 184b subsections (1) to (3), also in conjunction with section 184c, first sentence;
7. counterfeiting of money and securities (sections 146, 151 and152), guaranteed 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 within a reasonable period of time is not made, is rejected, or the extradition is not practicable.

Section 8 Time of the Act
An act is committed at the time the perpetrator or the inciter or accessory acted, or in case of an omission, should have acted. The time when the result occurs is not determinative.

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 offence, 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 11 Terms Relating to Persons and Subject Matter

(1) Within the meaning of this law:

1. a relative is whoever belongs among the following persons:
a) relations by blood or marriage in direct line, the spouse, the same-sex partner, the fiancé, siblings, the spouses of siblings, siblings of spouses, even if the marriage or same-sex partnership upon which the relationship was based no longer exists, or when the relationship by blood or marriage has ceased to exist;
b) foster parents and foster children;
2. a public official is whoever, under German law:
a) is a civil servant or judge;
b) otherwise has an official relationship with public law functions; or
c) has been appointed to a public authority or other agency or has been commissioned to perform duties of public administration without prejudice to the organisational form chosen to fulfil such duties;
3. a judge is whoever under German law is a professional or honorary judge;
4. a person with special public service obligations is whoever, without being a public official, is employed by or is active for:
a) a public authority or other agency which performs duties of public administration; or
b) an association or other union, business or enterprise which carries out duties of public administration for a public authority or other agency,
and is formally obligated by law to fulfil duties in a conscientious manner;
5. an unlawful act is only one which fulfils all the elements of a penal norm;
6. the undertaking of an act is its attempt and completion;
7. a public authority is also a court;
8. a measure is every measure of reform and prevention, forfeiture, confiscation and rendering unusable;
9. compensation is every consideration consisting of a material benefit;

(2) An act is also intentional within the meaning of this law, if it fulfils the statutory elements of an offence which requires intent in relation to the conduct, even if only negligence is required as to the specific result caused thereby.

(3) Audio and visual recording media, data storage media, illustrations and other images shall be the equivalent of writings in those provisions which refer to this subsection.

Section 22 Definition of Terms

Whoever, in accordance with his understanding of the act, takes an immediate step towards the realisation of the elements of the offence, attempts to commit a crime.

Section 23 Punishability for an Attempt

(1) An attempt to commit a serious criminal offence is always punishable, while an attempt to commit a less serious criminal offence is only punishable if expressly provided by law.

(2) An attempt may be punished more leniently than the completed act (section 49a subsection (1)).

(3) If the perpetrator, due to a gross lack of understanding, fails to recognise that the attempt could not possibly lead to completion due to the nature of the object on which or the means with which it was to be committed, the court may withhold punishment or in its own discretion mitigate the punishment (section 49 subsection(2)).

Section 24 Abandonment

(1) Whoever voluntarily renounces further execution of the act or prevents its completion shall not be punished for an attempt. If the act is not completed due in no part to the contribution of the abandoning party, he shall not be punished if he makes voluntary and earnest efforts to prevent its completion.

(2) If more than one person participate in the act, whoever voluntarily prevents its completion will not be punished for an attempt. However his voluntary and earnest efforts to prevent the completion of the act shall suffice for exemption from punishment if the act is not completed due in no part to his contribution or is committed independently of his earlier contribution to the act.

Section 26 Incitement

Whoever intentionally induces another to intentionally commit an unlawful act shall, as an inciter, be punished the same as a perpetrator.

Section 27 Accessoryship

(1) Whoever intentionally renders aid to another in that person's intentional commission of an unlawful act shall be punished as an accessory.

(2) The punishment for the accessory corresponds to the punishment threatened for the perpetrator. It shall be mitigated pursuant to section 49 subsection (1).

Section 149 Preparation of the Counterfeiting of Money and Stamps

(1) Whoever prepares a counterfeiting of money or stamps by producing, procuring for himself or another, offering for sale, storing or giving to another:
1. plates, frames, type, blocks, negatives, stencils, computer programs or similar equipment which by its nature is suited to the commission of the act;
2. paper which is identical or confusingly similar to the type of paper which is designated for the production of money or official stamps and specially protected against imitation, or
3. holograms or other elements serving to afford protection against counterfeiting
shall be punished with imprisonment for not more than five years or a fine if he prepared the counterfeiting of money, otherwise with imprisonment for not more than two years or a fine.

(2) Whoever voluntarily:
1. renounces the execution of the prepared act and averts a danger caused by him that others continue to prepare the act or execute it, or prevents the completion of the act; and
2. destroys or renders useless the means for counterfeiting, to the extent they still exist and are useful for counterfeiting, or reports their existence to a public authority or surrenders them there,
shall not be punished under subsection (1).

(3) If the danger that others continue to prepare or execute the act is averted, or the completion of the act is prevented due in no part to the contribution of the perpetrator, then the voluntary and earnest efforts of the perpetrator to attain this goal shall suffice in lieu of the prerequisites of subsection (2), no 1.

Section 184b Dissemination, Purchase, and Possession of Pornographic Writings Involving Children

(1) Whoever, in relation to pornographic writings (section 11 subsection (3)) that have as their object the sexual abuse of children (sections 176 to 176b) (pornographic writings involving children):
1. disseminates them;
2. publicly displays, posts, presents or otherwise makes them accessible; or
3. produces, obtains, supplies, stocks, offers, announces, commends or undertakes to import or export them, in order to use them or copies made from them within the meaning of numbers 1 or 2 or makes such use possible by another,
shall be punished with imprisonment for three months to five years.

(2) Whoever undertakes to obtain possession for another of pornographic writings involving children that reproduce an actual or true to life event, shall be similarly punished.

(3) In cases under subsection (1) or subsection (2), imprisonment for six months to ten years shall be imposed if the perpetrator acts on a commercial basis or as a member of a gang that has combined for the continued commission of such acts and the pornographic writings involving children reproduce an actual or true to life event.

(4) Whoever undertakes to obtain possession of pornographic writings involving children that reproduce an actual or true to life event shall be punished with imprisonment for up to two years or a fine. Whoever possesses the writings set forth in sentence 1 shall be similarly punished.

(5) Subsections (2) and (4) shall not apply to acts that exclusively serve the fulfilment of legal, official, or professional duties.

(6) In cases under subsection (3), section 73d shall be applicable. Objects to which a crime under subsection (2) or (4) relates shall be confiscated. Section 74a shall be applicable.

Section 201 Violation of the Confidentiality of the Spoken Word

(1) Whoever, without authorisation:
1. makes an audio recording of the privately spoken words of another; or
2. uses or makes a recording thus produced accessible to a third party,
shall be punished with imprisonment for not more than three years or a fine.

(2) Whoever, without authorisation:
1. listens with an eavesdropping device to privately spoken words not intended to come to his attention; or
2. publicly communicates, verbatim, or the essential content of the privately spoken words of another recorded pursuant to subsection (1), number 1, or listened to pursuant to subsection (2), number 1,
shall be similarly punished. The act under sentence 1, number 2, shall only be punishable if the public communication is capable of interfering with the legitimate interests of another. It is not unlawful if the public communication was made for the purpose of safeguarding pre-eminent public interests.

(3) Whoever, as a public official or a person with special public service obligations, violates the confidentiality of the spoken word (subsections (1) and (2)) shall be punished with imprisonment for not more than five years or a fine.

(4) An attempt shall be punishable.

(5) The audio recording media and eavesdropping devices which the perpetrator or the inciter or accessory used may be confiscated. Section 74a shall be applicable.

Section 202a Data Espionage

(1) Whoever, without authorisation, obtains data for himself or another, which were not intended for him and were specially protected against unauthorised access, shall be punished with imprisonment for not more than three years or a fine.

(2) Within the meaning of subsection (1), data shall be only those which are stored or transmitted electronically or magnetically or otherwise in a not immediately perceivable manner.

Section 202a Data Espionage (draft law)

(1) Whoever, without authorisation and by means of violating access security mechanisms, obtains for himself or another party access to data that are not intended for him and that are specially protected against unauthorised access, shall be punished with imprisonment for not more than three years or a fine.

(2) Within the meaning of subsection (1), data shall be only those which are stored or transmitted electronically or magnetically or otherwise in a not immediately perceivable manner.

Section 202b Data Interception (draft law)

Whoever, without authorisation and through the use of technological means, obtains for himself or another party access to data not intended for him (section 202a subsection (2)) from non-public transmissions of data or from electromagnetic emissions of data processing equipment, shall be punished with imprisonment for no more than two years or a fine, provided that the offence is not subject to a more severe penalty under other provisions.

Section 202c Preparation of Data Espionage or Data Interception (draft law)

(1) Whoever prepares a criminal offence pursuant to section 202a or 202b by creating, procuring for himself or another party, selling, giving over to another party, disseminating or otherwise providing access to

1. passwords or other security codes that enable access to data (section 202a subsection (2)), or
2. computer programmes whose purpose is to commit such an act,

shall be punished with imprisonment for no more than one year or a fine.

(2) Section 149 subsections 2 and 3 shall apply accordingly.

Section 263 Fraud

(1) Whoever, with the intent of obtaining an unlawful material benefit for himself or a third person, damages the assets of another by provoking or affirming a mistake by pretending that false facts exist or by distorting or suppressing true facts, shall be punished with imprisonment for not more than five years or a fine.

(2) An attempt shall be punishable.

(3) In especially serious cases the punishment shall be imprisonment for six months to ten years. An especially serious case exists, as a rule, if the perpetrator:

1. acts on a commercial basis or as a member of a gang which has combined for the continued commission of falsification of documents or fraud;
2. causes an asset loss of great magnitude or by the continued commission of fraud acts with the intent of placing a large number of human beings in danger of loss of assets;
3. places another person in financial need;
4. abuses his powers or his position as a public official; or
5. feigns an insured event after he or another have, to this end, set fire to a thing of significant value or destroyed it, in whole or in part, through the setting of a fire or caused the sinking or wrecking of a ship.

(4) Section 243 subsection (2) as well as sections 247 and 248a shall apply accordingly.

(5) Whoever on a commercial basis commits fraud as a member of a gang which has combined for the continued commission of crimes under sections 263 to264 or 267 to 269, shall be punished with imprisonment for one year to ten years, in less serious cases with imprisonment for six months to five years.

(6) The court may order supervision of conduct (section 68 subsection (1)).

(7) Sections 43a, 73d shall be applicable if the perpetrator acted as a member of a gang which has combined for the continued commission of crimes under sections 263 to 264 or 267 to 269. Section 73d shall also be applicable if the perpetrator acted on a commercial basis.

Section 263a Computer Fraud

(1) Whoever, with the intent of obtaining an unlawful material benefit for himself or a third person, damages the assets 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 order of events, shall be punished with imprisonment for not more than five years or a fine.

(2) Section 263 subsections (2) to (7) shall apply accordingly.

(3) Whoever prepares a criminal offence under subsection (1) by manufacturing computer programs, the purpose of which is to commit such an act, or for himself or another, obtains offers for sale, holds, or gives to another, shall be punished with imprisonment for not more than three years or a fine.

(4) in cases under subsection (3), section 149 subsections (2) and (3) shall apply accordingly.

Section 267 Falsification of Documents

(1) Whoever, for the purpose of deception in legal relations, produces a counterfeit document, falsifies a genuine document or uses a counterfeit or a falsified document shall be punished with imprisonment for not more than five years or a fine.

(2) An attempt shall be punishable.

(3) In especially serious cases the punishment shall be imprisonment for six months to ten years. An especially serious case exists, as a rule, if the perpetrator:

1. acts on a commercial basis or as a member of a gang which has combined for the continued commission of fraud or falsification of documents;
2. causes an asset loss of great magnitude;
3. substantially endangers the security of legal relations through a large number of counterfeit or falsified documents; or
4. abuses his powers or his position as a public official.

(4) Whoever commits the falsification of documents on a commercial basis as a member of a gang which has combined for the continued commission of crimes under sections 263 to 264 or 267 to 269 shall be punished with imprisonment for one year to ten years, in less serious cases with imprisonment for six months to five years.

Section 269 Falsification of Legally Relevant Data

(1) Whoever, for purposes of deception in legal relations, stores or modifies legally relevant data in such a way that a counterfeit or falsified document would exist upon its retrieval, or uses data stored or modified in such a manner, shall be punished with imprisonment for not more than five years or a fine.

(2) An attempt shall be punishable.

(3) Section 267 subsections (3) and (4), shall apply accordingly.

Section 303a Alteration of Data (draft law concerning subsection 3 only)

(1) Whoever unlawfully deletes, suppresses, renders unusable or alters data (section 202a subsection (2)) shall be punished with imprisonment for not more than two years or a fine.

(2) An attempt shall be punishable.

(3) Section 202c shall apply accordingly with respect to the preparation of a criminal offence under subsection (1).

Section 303b Computer Sabotage

(1) Whoever interferes with data processing which is of substantial significance to the business or enterprise of another party or a public authority by:

1. committing an act under section 303a subsection (1); or
2. destroying, damaging, rendering unusable, removing or altering a data processing system or a data carrier,

shall be punished with imprisonment for not more than five years or a fine.

(2) An attempt shall be punishable.

Section 303b Computer Sabotage (draft law)

(1) Whoever seriously interferes with data processing which is of substantial significance to another party by

1. committing an act under section 303a subsection (1),
2. enters or transmits data (section 202a subsection (2)) with the intention of causing harm to another party or
3. Destroying, damaging, rendering unusable, removing or altering a data processing system or a data carrier,

shall be punished with imprisonment of no more than three years or a fine.

(2) If such interference involves data processing that is of substantial significance to the business or enterprise of another party or to a public authority, the penalty shall consist of imprisonment of no more than five years or a fine.

(3) An attempt shall be punishable.

(4) In particularly serious cases under subsection (2), the punishment shall consist of imprisonment from six months to ten years. As a rule, a case is to be considered particularly serious when the perpetrator

1. causes a loss of assets of great magnitude,
2. acts on a commercial basis or as a member of a gang established to commit recurrent acts of computer sabotage,
3. interferes with the provision of goods or services vital to the population or compromises the security of the Federal Republic of Germany

(5) Section 202c shall apply accordingly with respect to the preparation of a criminal offence under subsection (1).

B. Copyright Act (*Gesetz über Urheberrecht und verwandte Schutzrechte Urheberrechtsgesetz*, UrhG)

Section 106 Unauthorised Exploitation of Copyrighted Works

(1) Whoever reproduces, distributes or publicly communicates a work or an adaptation or transformation of a work, other than in a manner allowed by law and without the right holder's consent, shall be punished with imprisonment for up to three years or a fine.

(2) An attempt shall be punishable.

Section 107 Unlawful Affixing of Designation of Author

(1) Whoever

1. without the author's consent, affixes a designation of author (section 10 subsection (1)) to the original of a work of fine art or distributes an original bearing such designation,
2. affixes a designation of author (section 10 subsection (1)) on a copy, adaptation or transformation of a work of fine art in such manner as to give to the copy, adaptation or transformation the appearance of an original or distributes a copy, adaptation or transformation bearing such designation,

shall be punished with imprisonment for up to three years or a fine provided the offence is not subject to a more severe penalty under other provisions.

(2) An attempt shall be punishable.

Section 108 Infringement of Neighbouring Rights

(1) Whoever, other than in a manner allowed by law and without the right holder's consent:

1. reproduces, distributes or publicly communicates a scientific edition (section 70) or an adaptation or transformation of such edition;
2. exploits a posthumous work or an adaptation or transformation of such work contrary to section 71;
3. reproduces, distributes or publicly communicates a photograph (section 72) or an adaptation or transformation of a photograph;
4. exploits a performance contrary to section 77 subsection (1) or (2) or section 78 subsection (1);
5. exploits an audio recording contrary to section 85;
6. exploits a broadcast contrary to section 87;
7. exploits a video or video and audio recording contrary to section 94 or section 95 in conjunction with section 94;
8. uses a database contrary to section 87b (1),

shall be punished with imprisonment for up to three years or a fine.

(2) An attempt shall be punishable.

Section 108a Unlawful Exploitation on a Commercial Basis

(1) Where the person committing the acts referred to in sections 106 to 108 does so on a commercial basis, the penalty shall be imprisonment for up to five years or a fine.

(2) An attempt shall be punishable.

Section 108b Unauthorised interference with technical protection measures and information necessary for rights management

(1) Any person who,
1. with the intention of enabling access to or use of a work protected under this Act or other subject matter protected under this Act, circumvents an effective technical measure without the consent of the right holder, or
2. knowingly without authorisation
a) removes or alters rights management information originating from right holders, if any such information is affixed to a reproduction of a work or other protected subject matter or is published in connection with the public communication of such a work or other protected subject matter, or
(b) disseminates, prepares for dissemination, broadcasts, publicly communicates or makes available to the public a work or other protected subject matter where rights management information has been removed or altered without authorisation
and in so doing has at least recklessly induced, enabled, facilitated or concealed the infringement of copyright or related rights
shall, if the offence was not committed for the exclusive private use of the perpetrator or persons personally associated with the perpetrator or is not related to such use, be punished with imprisonment for no more than one year or a fine.

(2) Punishment shall also be imposed upon any person who, in violation of section 95a subsection (3), produces, imports, disseminates, sells or rents a device, product or component for commercial purposes.

(3) Where the person committing the acts referred to in subsection (1) does so on a commercial basis, the penalty shall be imprisonment for no more than three years or a fine.

C. Regulatory Offences Act (*Gesetz über Ordnungswidrigkeiten*, OWiG)

Section 30 Regulatory Fine Imposed on Legal Persons and on Associations of Persons

(1) Where a person acting
1. as an entity authorised to represent a legal person or as a member of such an entity,
2. as chairman of the executive committee of an association without legal capacity or as a member of such committee,
3. as a partner authorised to represent a partnership with legal capacity, or
4. as the authorised representative with full power of attorney or in a managerial position as procura holder or the authorised representative with a commercial power of attorney of a legal person or of an association of persons referred to in numbers 2 or 3,
5. as another person responsible on behalf of the management of the operation or enterprise forming part of a legal person, or of an association of persons referred to in numbers 2 or 3, also covering supervision of the conduct of business or other exercise of controlling powers in a managerial position,
has committed a criminal offence or a regulatory offence as a result of which duties incumbent on the legal person or on the association of persons have been violated, or where the legal person or the association of persons has been enriched or was intended to be enriched, a regulatory fine may be imposed on such person or association.

(2)The regulatory fine shall amount
1. in the case of a criminal offence committed with intent, to not more than one million Euros,
2. in the case of a criminal offence committed negligently, to not more than five hundred thousand Euros.
Where a regulatory offence has been committed, the maximum regulatory fine that can be imposed shall be determined by the maximum regulatory fine imposable for the regulatory offence at issue. The second sentence shall also apply where an act simultaneously constituting a criminal offence and a regulatory offence has been committed, provided that

the maximum regulatory fine imposable for the regulatory offence exceeds the maximum pursuant to the first sentence.

(3) Section 17 subsection 4 and section 18 shall apply *mutatis mutandis*.

(4) If criminal proceedings or proceedings to impose a regulatory fine are not instituted in respect of the criminal offence or the regulatory offence, or if such proceedings are discontinued, or if imposition of a criminal penalty is dispensed with, the regulatory fine may be assessed independently. Statutory provision may be made to the effect that a regulatory fine may be imposed in its own right in further cases as well. However, independent assessment of a regulatory fine against the legal person or association of persons shall be precluded where the criminal offence or the regulatory offence cannot be prosecuted for legal reasons; section 33 subsection 1, second sentence, shall remain unaffected.

(5) Assessment of a regulatory fine incurred by the legal person or association of persons shall, in respect of one and the same offence, preclude a forfeiture order, pursuant to sections 73 or 73a of the Criminal Code or pursuant to section 29a, against such person or association of persons.

Section 130

(1) Whoever, as the owner of an operation or undertaking, intentionally or negligently omits to take the supervisory measures required to prevent contraventions, within the operation or undertaking, of duties incumbent on the owner as such and the violation of which carries a criminal penalty or a regulatory fine, shall be deemed to have committed a regulatory offence in a case where such contravention has been committed as would have been prevented, or made much more difficult, if there had been proper supervision. The required supervisory measures shall also comprise appointment, careful selection and surveillance of supervisory personnel.

(2) An operation or undertaking within the meaning of subsection 1 shall include a public enterprise.

(3) Where the breach of duty carries a criminal penalty, the regulatory offence may carry a regulatory fine not exceeding one million Euros. Where the breach of duty carries a regulatory fine, the maximum regulatory fine for breach of the duty of supervision shall be determined by the maximum regulatory fine imposable for the breach of duty. The second sentence shall also apply in the case of a breach of duty carrying simultaneously a criminal penalty and a regulatory fine, provided that the maximum regulatory fine imposable for the breach of duty exceeds the maximum pursuant to the first sentence.

D. German Code of Criminal Procedure (*Strafprozessordnung*, StPO)

Section 94 Objects Which May Be Seized

(1) Objects which may have importance as evidence for the investigation shall be impounded or be secured in another manner.

(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 licenses 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 and to deliver it upon request.

(2) In the case of non-compliance, the coercive measures provided under section 70 may be used against such person. This shall not apply to persons entitled to refuse to testify.

Section 98 Order of Seizure

(1) Seizures shall be ordered only by the judge and, in exigent circumstances, by the public prosecution office and 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 judge.

(2) An official who seized an object without judicial order shall within three days apply for judicial approval if neither the person concerned nor an adult relative was present at the seizure, or if the person concerned and, if he was absent, an adult relative of that person raised express objection to the seizure. The person concerned may at any time apply for a judicial decision. To the extent that public charges are not preferred, the decision shall be made by the Local Court in whose district the seizure took place. If a seizure, seizure of mail or a search has already been made in another district, the Local Court in the district in which the public prosecution office conducting the preliminary proceedings has its seat shall issue a decision. In this case, the person concerned may also submit the application to the Local Court in whose district the seizure took place. If this Local Court is not competent pursuant to the fourth sentence, the judge shall forward the application to the competent Local Court. The person concerned shall be informed of his rights.

(3) The judge shall be notified of the seizure within three days if the seizure was made by the public prosecution office or by one of the officials assisting it after the public charges were preferred; the objects seized shall be put at his disposal.

(4) If it is necessary to make a seizure in an official building or an installation of the Federal Armed Forces which is not open to the general public, the superior authority of the Federal Armed Forces shall be requested to carry out such seizure. The requesting agency 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 100a Conditions Regarding Interception of Telecommunications

Interception and recording of telecommunications may be ordered if certain facts substantiate the suspicion that a person was the perpetrator or inciter of, or accessory to

1. a) criminal offences against peace, of high treason, of endangering the democratic state based on the rule of law, or of treason and of endangering external security (sections 80 to 82, 84 to 86, 87 to 89, 94 to 100a of the Criminal Code, section 20 subsection (1), numbers 1 to 4 of the Associations Act);

   b) criminal offences against national defence (sections 109d to 109h of the Criminal Code);

   c) criminal offences against public order (sections 129 to 130 of the Criminal Code, section 92 subsection (1), number 7 of the Residence Act),

   d) incitement or accessoryship to desertion or incitement to disobedience (sections 16, 19 in conjunction with section 1 subsection (3) of the Military Criminal Code) without being a member of the Federal Armed Forces;

   e) criminal offences against the security of the troops of the non-German contracting parties to the North Atlantic Treaty stationed in the Federal Republic of Germany or of the troops of one of the Three Powers present in *Land* Berlin (sections 89, 94 to 97, 98 to 100, 109d to 109g of the Criminal Code, sections 16 and 19 of the Military Criminal Code in conjunction with Article 7 of the Fourth Criminal Law Amendment Act);

2. counterfeiting money or shares or bonds (sections 146, 151, 152 of the Criminal Code),

   aggravated trafficking in human beings pursuant to section 181, numbers 2 and 3 of the Criminal Code,

   murder, manslaughter or genocide (sections 211, 212, 220a of the Criminal Code),

   a criminal offence against personal liberty (sections 234, 234a, 239a, 239b of the Criminal Code),

   gang theft (section 244 subsection (1), number 2 of the Criminal Code) or aggravated gang theft (section 244a of the Criminal Code),

robbery or extortion resembling robbery (sections 249 to 251, 255 of the Criminal Code),

extortion (section 253 of the Criminal Code),

commercial handling of stolen goods or gang handling of stolen goods (section 260 of the Criminal Code) or commercial gang handling (section 260a of the Criminal Code),

money laundering or concealment of unlawfully obtained assets pursuant to section 261 subsection (1), (2) or (4) of the Criminal Code,

a criminal offence endangering the general public in the cases of sections 306 to 306c, or section 307 subsection (1) to (3), section 308 subsections (1) to (3), section 309 subsections (1) to (4), section 310 subsection (1), sections 313, 314 or section 315 subsection (3), section 315b subsection (3) or sections 316a or 316c of the Criminal Code,

3. a criminal offence pursuant to section 52a subsections (1) to (3), section 53 subsection (1), first sentence, numbers 1, 2, second sentence of the Weapons Act, section 34 subsections (1) to (6) of the Foreign Trade and Payments Act or pursuant to section 19 subsections (1) to (3), section 20 subsection (1) or (2), each also in conjunction with section 21 or section 22a subsections (1) to (3) of the War Weapons Control Act,
4. a criminal offence pursuant to one of the provisions referred to in section 29 subsection (3), second sentence, number 1, of the Narcotics Act under the conditions set forth therein or a criminal offence pursuant to sections 29a, 30 subsection (1), numbers 1, 2, 4, section 30a or section 30b of the Narcotics Act, or
5. a criminal offence pursuant to section 92a subsection (2) or section 92b of the Residence Act or pursuant to section 84 subsection (3) or section 84a of the Asylum Procedure Act

or, in cases in which the attempt is punishable, has attempted to perpetrate or participate in such offences or has prepared such offences by committing a criminal offence and if other means of establishing the facts or determining the accused's whereabouts offer no prospect of success or are considerably more difficult. The order may be made only against the accused or against persons in respect of whom it can be assumed, on the basis of particular facts, that they are receiving messages intended for the accused or receiving or transmitting messages from the accused or that the accused is using their connection.

Section 100b Order to Intercept Telecommunications

(1) The interception and recording of telecommunications (section 100a) may be ordered only by a judge. In exigent circumstances, the order may also be given by the public prosecution office. The order of the public prosecution office shall become ineffective if it is not confirmed by the judge within three days.

(2) The order shall be given in writing. It must indicate the name and address of the person against whom it is directed as well as the telephone number or other identification of the person's telecommunications access line. The type, extent and time of the measures shall be specified in the order. The order shall be limited to a maximum duration of three months. An extension of not more than three months shall be admissible if the prerequisites designated under section 100a continue to exist.

(3) On the basis of this order all persons providing, or collaborating in the provision of, telecommunications services on a commercial basis shall enable the judge, the public prosecution office and officials assisting it working in the police force (section 152 of the Courts Constitution Act) to intercept and record telephone calls. Whether and to what extent measures are to be taken in this respect shall follow from section 88 of the Telecommunications Act and from the Ordinance issued thereunder for the technical and organisational implementation of interception measures. Section 95 subsection (2) shall apply *mutatis mutandis*.

(4) If the prerequisites provided under section 100a no longer prevail, the measures resulting from the order shall be terminated without delay. The judge and the person bound by subsection (3) shall be informed of the termination.

(5) The personal information obtained by the measure may be used as evidence in other criminal proceedings only insofar as during its evaluation information was obtained which is required to clear up one of the criminal offences listed in Section 100a.

(6) If the records obtained by the measures are no longer required for criminal prosecution purposes, they shall be destroyed without delay under the control of the public prosecution office. The destruction shall be recorded in writing.

Section 100g

(1) If certain facts substantiate the suspicion that a person, as a perpetrator, inciter or accessory, or using terminal equipment (section 3, number 3, of the Telecommunications Act), has committed a criminal offence of substantial significance, particularly one of the offences referred to in section 100a, first sentence, or, in cases where an attempt is punishable, has attempted to perpetrate or participate in such offences or has prepared such offences by committing a criminal offence, an order may be made to the effect that commercial providers of telecommunications services or those who are involved in the provision of such services shall, without delay, give information on the telecommunications traffic data referred to in subsection (3) to the extent that the information is necessary for the investigation. This shall only apply insofar as such traffic data concern the accused or the other persons referred to in Section 100a, second sentence. The order may also be made in respect of information concerning future telecommunications traffic.

(2) An order may only be made for the provision of information on whether telecommunications traffic has been established from a telecommunications access line to the persons referred to in subsection (1), second sentence, if other means of establishing the facts or determining the accused's whereabouts offer no prospect of success or are considerably more difficult.

(3) Telecommunications traffic data shall be:

1. *in the case of a connection, authorisation codes, personal access numbers, identifications of position as well as the subscriber number or the identification of the calling and called access line or the terminal equipment,*
2. *the beginning and the end of the connection according to the date and the time of day,*
3. *telecommunication services used by the customer,*
4. *termination points of non-switched connections, their beginning and their end according to the date and the time of day.*

Section 100g (draft law)

(1) If certain facts substantiate the suspicion that a person, as a perpetrator, inciter or accessory

1. has committed, even in a single case, a criminal offence of substantial significance, particularly one of the offences specified in section 100a subsection (2), has attempted to commit a criminal offence in cases where an attempt is punishable, or has prepared a criminal offence by committing a criminal offence or
2. has committed a criminal offence through the use of telecommunications,

traffic data (section 96 subsection (1), section 113a of the Telecommunications Act) may be collected without the knowledge of the person concerned, to the extent that this is necessary for ascertaining the facts or for determining the whereabouts of the accused. In cases under the first sentence number 2, the measure shall be admissible only where other means of ascertaining the facts or determining the whereabouts of the accused offer no prospect of success and where the collection of such data is proportionate to the significance of the case. The collection of location data in real time is permitted only in cases where the first sentence number 1 applies.

(2) Section 100a subsection (3) and section 100b subsections (1) to (4), first sentence, shall apply accordingly. In derogation of section 100b subsection (2), second sentence number 2, in the case of a criminal offence of substantial significance, a sufficiently precise

designation of the locality and time of the telecommunication shall suffice if other means of ascertaining the facts would offer no prospect of success or be considerably more difficult.

(3) If the traffic data are not collected from a telecommunications service provider, such collection shall, following the conclusion of the communication activity, be determined pursuant to general provisions.

(4) In accordance with section 100b subsection (5), an annual overview of measures conducted pursuant to subsection (1) shall be compiled which contains the following information:

1. the number of cases in which measures were conducted pursuant to subsection (1);
2. the number of orders to conduct measures pursuant to subsection (1), differentiated according to initial orders and extension orders;
3. the criminal offence that occasioned the respective order, differentiated according to subsection (1), first sentence, numbers 1 and 2;
4. the number of past months for which traffic data were retrieved pursuant to subsection (1), starting from the time the order was issued;
5. the number of measures that produced no results because the requested data were not available either in whole or in part.

Section 100h

(1) The order must contain the name and the address of the person against whom the order is directed, as well as the subscriber number or other identification of his telecommunications access line. In the case of a criminal offence of substantial significance it shall be sufficient if there is adequate designation of the locality and time of the telecommunication, in regard to which the information is to be provided, if other means of establishing the facts would offer no prospect of success or be much more difficult. Section 100b subsection (1) and subsection (2), first and third sentences, subsection (6) and section 95 subsection (2) shall apply mutatis mutandis*; section 100b subsection (2), fourth and fifth sentences, and subsection (4) shall also apply* mutatis mutandis *in the case of an order for information on future telecommunications traffic.*

(2) Where the right of refusal to testify applies in the cases referred to under section 53 subsection (1), numbers 1, 2 and 4, a request for information on telecommunications traffic established by or with the person entitled to refuse to testify shall be inadmissible; any information acquired nonetheless shall not be used. This shall not apply if the person entitled to refuse to testify is suspected of incitement, accessoryship, obstruction of justice or handling stolen goods.

(3) The personal data obtained from the information provided may be used for the purposes of evidence in other criminal proceedings only insofar as during their evaluation information emerges which is required to clear up a criminal offence referred to in section 100g subsection (1), first sentence, or if the accused gives his consent thereto.

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 and in cases where it may be presumed that the search will lead to the discovery of evidence.

Section 103 Searches in Respect of Other Persons

(1) Searches in respect of other persons shall be admissible only for the purpose of apprehending the accused or to pursue the traces of a criminal offence or to seize certain objects, and only if facts are present which support the conclusion that the person, trace, or object looked for is in the premises which are to be searched. For the purpose of apprehending an accused who is strongly suspected of having committed an offence pursuant to section 129a of the Criminal Code, or one of the offences designated in this

provision, a search of private and other premises shall also be admissible if they are in a building where, on the basis of certain facts, the accused is presumed to be.

(2) The restrictions of subsection 1, first sentence, do not apply to premises where the accused was apprehended or which he entered during the pursuit.

Section 105 Search Order; Execution

(1) Searches shall be ordered by the judge only and, in exigent circumstances, also by the public prosecution office and officials assisting it (section 152, Courts Constitution Act). Searches pursuant to Section 103 subsection 1, second sentence, shall be ordered by the judge; the public prosecution office shall be authorised to order searches in exigent circumstances.

(2) A municipal official or two members of the community in the district where the search is made shall be called in, if possible, to assist, if private premises, business premises, or fenced-in property are to be searched without the judge or the public prosecutor being present. The persons called in as members of the community shall not be police officers or officials assisting the public prosecution office.

(3) If it is necessary to make a search in an official building or in an installation or establishment of the Federal Armed Forces which is not open to the general public, the superior authority of the Federal Armed Forces shall be requested to carry out such search. The requesting authority shall be entitled to participate. No such request shall be necessary if the search is to be made in places which are inhabited exclusively by persons other than members of the Federal Armed Forces.

Section 110 Examination of Papers (draft law)

(1) The public prosecution office shall have the authority to examine the papers of the person with respect to whom the search was conducted (section 152 of the Courts Constitution Act).

(2) Otherwise, officials shall be authorised to examine found papers only if the holder approves 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 that shall be sealed with the official seal in the presence of the holder.

(3) The examination of electronic storage media may be extended to storage media in separate locations, to which storage media the person with respect to whom the search was conducted is authorised to provide access. Data that could be of significance for the investigation may be stored if there is concern that such data may be lost prior to the securing of the data carrier; such data shall be deleted as soon as they are no longer required for criminal prosecution purposes.

Section 161 Information and Investigations

(1) For the purpose indicated in section 160 subsections (1) to (3), the public prosecution office shall be entitled to request information from all authorities and to make investigations of any kind, either itself or through the authorities and officials in the police force, provided there are no other statutory provisions specifically regulating their powers. The authorities and officials in the police force shall be obliged to comply with the request or order of the public prosecution office, and they shall be entitled in this case to request information from all authorities.

(2) Where personal information has been obtained as a result of a measure taken under police law, corresponding to the measure pursuant to section 98a, it may be used as evidence only insofar as during its evaluation information was obtained which is required to clear up one of the criminal offences listed in Section 98a subsection (1). The first sentence shall apply *mutatis mutandis* so far as measures taken under police law correspond to the measures referred to in section 100c subsection (1), number 2, and in section 110a.

(3) Personal information obtained in or from private premises by technical means for the purpose of personal protection in a clandestine investigation based on police law may be used as evidence where the offence concerned is murder or manslaughter (sections 211 and 212 of the Criminal Code), kidnapping for extortion or hostage taking (sections 239a and

239b of the Criminal Code), an assault on air and sea traffic (section 316c of the Criminal Code), or one of the offences pursuant to the Narcotics Act and referred to in section 100a, first sentence, number 4. Such use shall only be admissible after determination of its lawfulness by the presiding judge of a penal chamber of the Regional Court in whose district the authority making the order is located.

Section 163 Duties of the Police

(1) The authorities and officials in the police force shall investigate criminal offences and shall take all measures where there should be no delay, in order to prevent concealment of facts. To this end they shall be entitled to request all authorities for information, and in exigent circumstances to demand such information, and they shall be entitled to conduct investigations of any kind unless there are other statutory provisions specifically regulating their powers.

(2) The authorities and officials in the police force shall transmit, without delay, their records to the public prosecution office. Direct transmission to the Local Court shall be possible if it appears that a judicial investigation needs to be performed promptly.

E. Telecommunications Act (*Telekommunikationsgesetz*, TKG)

Section 89 Prohibition to Intercept, Obligation on Receiving Equipment Operators to Maintain Privacy

Interception by means of radio equipment shall be permitted only for communications intended for the radio equipment operator, radio amateurs within the meaning of the Amateur Radio Act of 23 June 1997 (Federal Law Gazette Part I page 1494), the general public or a non-defined group of persons. The content of communications other than those referred to in sentence 1 and the fact of their reception, even where reception has been unintentional, may not, even by persons not already committed to privacy under section 88, be imparted to others. Section 88 subsection (4) applies accordingly. The interception and forwarding of communications on the basis of special legal authorisation remain unaffected.

Section 112 Automated Information Procedure

(1) Any person providing publicly available telecommunications services shall store, without undue delay, data collected under section 111 subsection (1), first and third sentences, and subsection (2) in customer data files in which the telephone numbers and quotas of telephone numbers allocated to other telecommunications service providers for further marketing or other use and, with regard to ported numbers, the current carrier portability codes, are also to be included. Section 111 subsection (1), third and fourth sentences, apply accordingly with regard to the correction of customer data files. In the case of ported numbers the telephone number and associated carrier portability code are not to be erased before expiry of the year following the date on which the telephone number was returned to the network operator to whom it had originally been allocated. The person with obligations shall ensure that

1. the Federal Network Agency can, at all times, retrieve from customer data files data for information requests from the authorities referred to in subsection (2) by means of automated procedures in the Federal Republic of Germany;
2. data can be retrieved using incomplete search data or searches made by means of a similarity function.

The requesting authority is to consider, without undue delay, the extent to which it needs the data provided and erase, without undue delay, any data not needed. The person with obligations is to ensure by technical and organisational measures that no retrievals can come to his notice.

(2) Information from the customer data files pursuant to subsection (1) shall be provided to

1. the courts and criminal prosecution authorities;
2. federal and state police enforcement authorities for purposes of averting danger;

3. the Customs Criminological Office and customs investigation offices for criminal proceedings and the Customs Criminological Office for the preparation and execution of measures under section 39 of the Foreign Trade and Payments Act;
4. federal and state authorities for the protection of the Constitution, the Military Counterintelligence Service and the Federal Intelligence Service;
5. the emergency service centres pursuant to section 108 and the service centre for the maritime mobile emergency number 124124;
6. the Federal Financial Supervisory Authority; and
7. the Customs Administration authorities for the purposes set forth in section 2 subsection (1) of the Undeclared Work Act

via central inquiry offices, as stipulated in subsection (4), at all times, insofar as such information is needed to discharge their legal functions and the requests are submitted to the Federal Network Agency by means of automated procedures.

(3) The Federal Ministry of Economics and Technology shall be empowered to issue, in agreement with the Federal Chancellery, the Federal Ministry of the Interior, the Federal Ministry of Justice, the Federal Ministry of Finance and the Federal Ministry of Defence, and with the consent of the German Bundesrat, a statutory order in which the following matters are regulated

1. the essential requirements in respect of the technical procedures for
   a) the transmission of requests to the Federal Network Agency;
   b) the retrieval of data by the Federal Network Agency from persons with obligations, including the data types to be used for the queries; and
   c) transmission by the Federal Network Agency to the requesting authorities of the data retrieved;
2. the security requirements to be observed; and
3. in respect of retrievals using incomplete search data and searches made by means of similarity functions for which specifications on the character sequences to be included in the search are provided by the Ministries contributing to the statutory order,
   a) the minimum requirements in respect of the scope of the data to be entered in order to identify, as precisely as possible, the person to whom the search relates;
   b) the permitted number of hits to be transmitted to the requesting authority; and
   c) the requirements in respect of the erasure of data not needed.

In other respects, the statutory order may also restrict the query facility for the authorities referred to in subsection (2) numbers 5 to 7 to the extent that is required for such authorities. The Federal Network Agency shall determine the technical details of the automated retrieval procedure in a technical directive to be drawn up with the participation of the associations concerned and the authorised bodies and to be brought into line with the state of the art, where required, and published by the Federal Network Agency in its Official Gazette. The person with obligations according to subsection (1) and the authorised bodies are to meet the requirements of the technical directive not later than one year following its publication. In the event of an amendment to the directive, defect-free technical facilities configured to the directive shall meet the modified requirements not later than three years following its taking effect.

(4) At the request of the authorities referred to in subsection (2), the Federal Network Agency shall retrieve and transmit to the requesting authority the relevant data sets from the customer data files pursuant to subsection (1). It shall examine the admissibility of the transmission only where there is special reason to do so. Responsibility for such admissibility lies with the authorities referred to in subsection (2). For purposes of data protection control by the competent body, the Federal Network Agency shall record, for each retrieval, the time, the data used in the process of retrieval, the data retrieved, the person retrieving the data, the requesting authority and the reference number of the requesting authority. Use for any other purposes of data recorded is not permitted. Data recorded are to be erased after a period of one year.

(5) The person with obligations according to subsection (1) shall make all such technical arrangements in his area of responsibility as are required for the provision of

information under this provision, at his expense. This also includes procurement of the equipment required to secure confidentiality and protection against unauthorised access, installation of a suitable telecommunications connection, participation in the closed user system and the continued provision of all such arrangements as are required under the statutory order and the technical directive pursuant to subsection (3). Compensation for information provided by means of automated procedures is not paid to persons with obligations.

Section 113 Manual Information Procedure

(1) Any person commercially providing or assisting in providing telecommunications services shall, in a given instance, provide the competent authorities, at their request, without undue delay, with information on data collected under sections 95 and 111 to the extent required for the prosecution of criminal or regulatory offences, for averting danger to public safety or order and for the discharge of the legal functions of the federal and state authorities for the protection of the Constitution, the Federal Intelligence Service and the Military Counterintelligence Service. The person with obligations pursuant to sentence 1 shall provide information on data by means of which access to terminal equipment or to storage devices or units installed in such equipment or in the network is protected, notably personal identification numbers (PINs) or personal unlocking keys (PUKs), by virtue of an information request pursuant to section 161 subsection (1), first sentence, or section 163 subsection (1) of the Code of Criminal Procedure, data collection provisions in federal or state police legislation for averting danger to public safety or order, section 8 subsection (1) of the Federal Act on the Protection of the Constitution, the corresponding provisions of legislation to protect the constitutions of the *Länder*, section 2 subsection (1) of the Federal Intelligence Service Act or section 4 subsection (1) of the Military Counterintelligence Service Act; such data shall not be transmitted to any other public or private bodies. Access to data which are subject to telecommunications privacy shall be permitted only under the conditions of the relevant legislation. The person with obligations shall maintain silence vis-à-vis his customers and third parties about the provision of information.

(2) The person with obligations according to subsection (1) is to make such arrangements as are required in his area of responsibility for the provision of information, at his expense. In respect of information provided, the person with obligations is granted compensation by the requesting authority, the level of which, in derogation of section 23 of the Court Remuneration and Compensation Act, is determined by the statutory order referred to in section 110 subsection (9). Sentence 2 also applies in those cases in which, under the manual information procedure, merely data are requested which the person with obligations also keeps available for retrieval under the automated information procedure under section 112. Sentence 2 does not apply in those cases in which the information was not provided completely or correctly under the automated information procedure under section 112.

Section 148 Penal Provisions

(1) Any person who,

1. in violation of section 89, first or second sentence, intercepts a communication or imparts to others the content of a communication or the fact of its reception; or
2. in violation of section 90 subsection (1), first sentence,

a) owns, or

b) manufactures, markets, imports or otherwise introduces in the area of application of this Act

transmitting equipment as referred to there,

shall be punished with imprisonment for not more than two years or a fine.

(2) Where action in the cases of subsection (1) number 2 letter b arises through negligence, the offender shall be punished with imprisonment for not more than one year or a fine.

F. Act on International Legal Assistance in Criminal Matters (*Gesetz über die internationale Rechtshilfe in Strafsachen*, IRG)

Section 2 Principle

(1) A foreign national who is being prosecuted or who has been sentenced in a foreign country because of an act punishable there may be extradited to such foreign country at the request of the competent authorities for the purpose of prosecution or execution of a sentence given because of that act or because of the imposition of another penalty.

(2) A foreign national who has been sentenced in a foreign country because of an act punishable there may be extradited to another foreign country, which has taken over enforcement, at the request of the competent authorities of that country, for the purpose of executing the sentence imposed because of the act, or for the imposition of another penalty.

(3) Foreign nationals pursuant to this law shall be persons who are not German nationals pursuant to Article 116 (1) of the Basic Law.

Section 3 Extradition for the Purpose of Prosecution or Execution

(1) Extradition shall be admissible only if the act contains the elements of a criminal offence under German law or if, after analogous conversion of the facts, the act would under German law constitute an offence.

(2) Extradition for the purpose of prosecution shall be admissible only if the act is punishable under German law by a maximum of at least one year of imprisonment or if, after analogous conversion of the facts, the act would, under German law, be punishable by such a penalty.

(3) Extradition for the purpose of execution shall be admissible only if extradition for the purpose of prosecution because of the act would have been allowed and if a penalty involving imprisonment is to be executed. It shall further be granted on condition if it is to be expected that the period of imprisonment to be served, or the sum of the periods of imprisonment still to be served, is at least four months.

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) shall be every type of aid given to foreign criminal proceedings regardless of whether the foreign proceedings are conducted by a court or by a governmental authority and whether the legal assistance is to be provided by a court or by a governmental authority.

(3) Legal assistance may be provided only under circumstances under which German courts and governmental authorities could render legal assistance to each other.

Section 60 Rendering Assistance

If the governmental authority responsible for authorising legal assistance determines that the requirements for rendering legal assistance have been met, the governmental authority responsible for rendering the legal assistance shall be bound by such determination. Section 61 shall remain unaffected.

Section 61 Court Decision

(1) If a court decision that is responsible for rendering legal assistance considers that the requirements for rendering legal assistance have not been met, it shall give reasons for ist opinion and shall request a ruling by the Higher Regional Court. The Higher Regional Court shall also rule upon application of the public prosecution office at the Higher Regional Court, or in the case of section 66, upon application of a person claiming that his rights would be violated if assistance were rendered, whether the requirements for rendering legal assistance have been met. For such proceedings before the Higher Regional Court, sections 30 and 31 subsections (1), (2) and (4), sections 32 and 33 subsections (1), (2) and (4),

section 38 subsection (4), second sentence, and section 40 subsection (1), as well as the provisions of Chapter 11, Vol. 1 of the Code of Criminal Procedure, with the exception of sections 140-143, shall apply accordingly. For any subsequent proceedings, section 42 shall apply accordingly.

(2) Jurisdiction ratione loci shall lie with the Higher Regional Court and the public prosecution office at the Higher Regional Court in whose district the legal assistance is to be or has been rendered. If acts of legal assistance are to be or have been carried out in the districts of different Higher Regional Courts, jurisdiction shall depend on which Higher Regional Court or, where no Higher Regional Court is yet involved in the case, which public prosecution office at a Higher Regional Court was first to deal with the case.

(3) The decision of the Higher Regional Court shall be binding on those courts and authorities which are responsible for rendering the legal assistance.

(4) Legal assistance may not be granted if the court has ruled that the requirements for rendering legal assistance have not been met.

Section 61a Transmission of Personal Data without Request

(1) Courts and public prosecution offices may transmit personal data from criminal proceedings to the public authorities of another state as well as to interstate and supranational authorities without request by the latter if

1. transmission without request to a German court or to a German public prosecution office would have been admissible,
2. there are facts which warrant the expectation that the transmission is necessary
a) in order to prepare a request by the receiving state for legal assistance for the purpose of prosecution or execution of a sentence for a crime that is punishable by a maximum of more than five years of imprisonment in the area of application of this law, and the conditions for granting assistance upon request would be met if such request were 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, maintenance of which is demanded by the public interest, or to prevent a crime as described under letter a), and
3. the public authority to which the data are transmitted is competent to implement appropriate measures pursuant to number 2.

If adequate data protection is ensured in the receiving state, number 2 letter a), first sentence, applies with the provision that a crime which is punishable by a maximum of more than five years of imprisonment at a place within the scope of application of this law is substituted by a crime of significant gravity.

(2) Transmission is to be conducted under the condition that

1. time limits pursuant to German law for deletion and for review of deletion of transmitted data will be observed,
2. transmitted data will be used only for the purposes for which they were transferred, and
3. transmitted data will be deleted or corrected immediately upon information in accordance with subsection 4.

Section 62 Temporary Transfer to a Foreign Country for Foreign Proceedings

(1) A person who is held in pre-trial detention or in prison or who is subject to a rehabilitative and preventive measure involving deprivation of his liberty within the territory to which this Act applies, may, on request by the competent authority of a foreign country, be temporarily transferred to that country to attend proceedings pending there to be examined as a witness, for the purpose of confrontation or for inspection by the court, if

1. after having been advised, he states that he consents and this is recorded by a judge,
2. it is not to be anticipated that the duration of deprivation of liberty will be extended or the purpose of the criminal proceedings will be prejudiced as a result of the transfer,
3. an assurance is given that during the period of his transfer, the person concerned will not be subjected to a penalty or other sanction or proceeded against by virtue of measures which could not also have been taken during his absence and that in the event of his release he may leave the requesting State, and

4. an assurance is given that the person concerned will be returned without delay following the taking of evidence unless this has been waived.

The consent (first sentence no. 1) cannot be revoked.

(2) The public prosecution office at the Higher Regional Court shall prepare and carry out the transfer. The public prosecution office at the Higher Regional Court in whose region the deprivation of liberty is being enforced shall have local jurisdiction.

(3) The period of deprivation of liberty served in the requesting State shall be deducted from the period of deprivation of liberty to be enforced within the territory to which this Act applies. Section 37 subsection (4) shall apply accordingly.

Section 63 Temporary Transfer from a Foreign Country for Foreign Proceedings

(1) A person who is held in a foreign country in pre-trial detention or in prison or who is subject to a rehabilitative and preventive measure involving deprivation of his liberty may, on request by the competent authority of that country, be temporarily transferred to the territory within which this law applies to give evidence for proceedings pending in that country and, after the evidence has been taken, be returned. The person concerned shall be kept in detention to ensure his return.

(2) Detention shall be ordered by means of a written arrest warrant. The arrest warrant shall contain the following information:

1. the person concerned,
2. the request for the taking of evidence in the presence of the person concerned and
3. the reason for detention.

(3) The decision concerning detention shall be taken by the judge responsible for rendering legal assistance or by the judge at the Local Court in whose district the authority responsible for rendering legal assistance is located. This decision is not open to appeal.

(4) Sections 27, 45 subsection (4) and 62 subsection (2), first sentence, shall apply accordingly.

Section 64 Transit of Witnesses

(1) A foreign national who is held in a foreign country in pre-trial detention or in prison or who is subject to a rehabilitative and preventive measure involving deprivation of his liberty may, on request by a competent authority, be transported to a third state through the territory to which this law applies as a witness for examination, confrontation or inspection and be returned after the taking of evidence.

(2) The person concerned will be kept in detention to ensure secure transit.

Sections 27, 30 subsection (1), 42, 44, 45 subsections (3) and (4), 47, 63 subsection (2) shall apply accordingly.

Section 65 Transit for Enforcement Purposes

The transit of a foreign national, for purposes of enforcing a sentence or other sanction, from the state in which he was sentenced through the territory to which this law applies to a foreign country that has taken over such enforcement, shall be governed by sections 43 subsections (2) to (4) and sections 44, 45 and 47 as appropriate, provided that the request may also be submitted by a competent authority of the state in which the judgment was issued.

Section 66. Surrender of objects

(1) Upon request by the competent authority of a foreign country, objects may be surrendered

1. which may serve as evidence for foreign proceedings or
2. which the person concerned or a participant acquired as a result of the offence on which the request is based or as consideration for such objects.

(2) Surrender shall be admissible only if

1. the act giving rise to the request constitutes an unlawful act also under German law which fulfils the elements of an offence contained in a penal act or an act which permits punishment

by non-criminal fine, or if it would constitute such an act also under German law if the facts were transposed to an analogous context,
2. a seizure order issued by a competent authority of the requesting state has been submitted or such an authority has made a declaration stating that the requirements for seizure would be fulfilled if the objects were located in the requesting state, and
3. an assurance is given that the rights of third parties will remain unaffected and that objects surrendered subject to reservation will be returned immediately upon request.

(3) The public prosecution office at the Regional Court shall prepare the decision on surrender and carry out surrender once it has been authorised. The public prosecution office at the Regional Court in whose region the objects are located shall have local jurisdiction. Section 61 subsection (2), second sentence, shall apply accordingly.

Section 67 Search and seizure

(1) Objects that may become the subject of surrender to a foreign state may be seized or otherwise secured even prior to the receipt of the request for surrender. A search may also be conducted for this purpose.

(2) Subject to the conditions set forth in section 66 subsection (1) number 1 and subsection (2) number 1, objects may also be seized or otherwise secured if necessary for the execution of a request which is not directed toward the surrender of the objects. Subsection (1), second sentence, shall apply accordingly.

(3) The search and seizure shall be ordered by the Local Court in whose district the actions are to be conducted. Section 61 subsection (2), second sentence, shall apply accordingly.

(4) In case of imminent danger, the public prosecution office and its investigative personnel (section 152 of the Courts Constitution Act) shall be authorised to order the search and seizure.

Section 68 Return

(1) A person sought who, on request and subject to his subsequent return, has been temporarily extradited to face criminal proceedings brought against him within the territory to which this law applies, shall be returned to the requested state at the agreed time unless that state waives his return. The public prosecution office involved in the criminal proceedings referred to in the first sentence shall be responsible for ordering and effecting the return of the person sought.

(2) If the return of the person sought would not otherwise be guaranteed, his detention may be ordered by means of a written arrest warrant. The arrest warrant shall contain the following information:
1. the person sought,
2. the state to which the person sought is to be returned, and
3. the reasons justifying the order for detention.

(3) The decision concerning detention shall be taken by the respective court competent for ordering measures involving deprivation of liberty in the criminal proceedings referred to in subsection (1), first sentence. The decision shall not be open to appeal.

(4) Sections 18, 19, 24, 25, 27 and 45 subsection (4) shall apply accordingly.

Section 69 Temporary Transfer from a Foreign Country for German Proceedings

(1) A person who is held in a foreign country in pre-trial detention or in prison or who is subject to a rehabilitative and preventive measure involving deprivation of his liberty and who, on request, has been temporarily transferred to a German court or German authority for examination, confrontation or inspection shall, during his stay in the territory to which this law applies, be held in detention in order to ensure his return to that country.

(2) The decision concerning detention shall be taken by the court seised with the case and, in respect of preparatory proceedings, by the judge at the Local Court in whose district the public prosecution office conducting the proceedings is located. The decision is not open to appeal.

(3) Sections 27 and 45 subsection (4), section 62 subsection (2), first sentence and section 63 subsection (2) shall apply accordingly.

Section 83j Transmission of Data without Request

(1) To the extent provided by an international agreement, personal data that substantiate the suspicion that a criminal offence has been committed may be transmitted by public authorities to the public authorities of another European Union Member State as well as to organs and institutions of the European Communities, without request, provided that
1. a transmission, without request, to a German court or German public prosecution office would also be admissible and
2. the transmission is suited for
a) the institution of criminal proceedings in that other Member State or
b) the furthering of criminal proceedings already instituted in that Member State, and
3. the authority to which the data are transmitted is competent to undertake the measures under number 2.

(2) section 61a subsections (2) to (4) shall apply accordingly.