Preparatory Colloquium
Verona (Italy), *28 – 30 November 2012*
Section I - Information Society and Penal Law

XIX. International Congress of AIDP
Section I – General Criminal Law
Cybercrime

Germany*

Marco GERCKE*

(B) Criminalisation

Please note that in this questionnaire only general characteristics of cyber crime offense definitions are of interest. Specific questions of individual crime definitions will be discussed in Section II of the Congress.

(1) Which specific legal interests are deemed to be in need of protection by criminal law (e.g., integrity of data processing systems, privacy of stored data)?

German criminal law currently contains a whole set of provisions that are applicable with regard to computer crime and cybercrime. Apart from specific computer crime and cybercrime provisions (such as for example Sec. 202a Penal Code) various provisions are either drafted technology neutral (such as for example Sec. 130 Penal Code) or have been amended to be applicable when committed through the use of ICT[1] (such as for example Sec. 86 Penal Code).[2]

The core group of computer and cybercrime related offences contains 19 provisions. Following the methodology of the Council of Europe Convention on Cybercrime[3] they can be associated to four different categories of crime – namely offences against the confidentiality, integrity and availability of computer data and computer systems, illegal content, computer related offences and copyright offences.

---

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

* Prof. Dr. Marco Gercke, Director, Cybercrime Research Institute, Cologne, Germany

[1] Information and Communication Technology.

[2] Sec. 86 was amended by Art. 4 Nr. 3 IuKDG. Regarding details see: *Gercke*, Rechtswidrige Inhalte im Internet, 2000, page 14.

[3] Council of Europe Convention on Cybercrime (CETS No. 185), available at: http://conventions.coe.int. For more details about the offences covered by the Convention, see below: § 6.2.; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; *Gercke*, The Slow Awake of a Global Approach Against Cybercrime, Computer Law Review International, 2006, 140 *et seq.*; *Gercke*, National, Regional and International Approaches in the Fight Against Cybercrime, Computer Law Review International 2008, page 7 *et seq.*; *Aldesco*, The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime, Entertainment Law Review, 2002, No. 1, available at: http://elr.lls.edu/issues/v23-issue1/aldesco.pdf; *Jones*, The Council of Europe Convention on Cybercrime, Themes and Critiques, 2005, available at: http://www.cistp.gatech.edu/snsp/cybersecurity/materials/callieCOEconvention.pdf; *Broadhurst*, Development in the global law enforcement of cyber-crime, in Policing: An International Journal of Police Strategies and Management, 29(2), 2006, page 408 *et seq.*; Adoption of Convention on Cybercrime, International Journal of International Law, Vol. 95, No. 4, 2001, page 889 *et seq.*

Preparatory Colloquium Verona (Italy), November 2012
Germany

While most computer crime and cybercrime offences can be divided into one of the four categories the range of protected legal interest is broader. The German law is based on a very complex system of protected legal interests.

	Title	Provision	Protected Legal Interest
Penal Code (Strafgesetzbuch)	Dissemination of propaganda material of unconstitutional organisations	Sec. 86	constitutional order[4]
	Using symbols of unconstitutional organisations	Sec. 86a	constitutional order[5]
	Incitement to hatred	Sec. 130	public peace[6], dignity of individuals[7]
	Distribution of Pornography	Sec. 184	Youth Protection[8], protection of anybody (including adults) against unwanted confrontation with pornographic writings[9]
	Distribution of pornography depicting violence or sodomy	Sec. 184a	Protection of victims[10]; Not limited to youth protection[11] Protection of victims[12]
	Distribution, acquisition and possession of child pornography	Sec, 184b	Protection of children that are abused to produce child pornography[13]; prevention of initiation effect[14]
	Distribution, acquisition and possession of juvenile pornography	Sec. 184c	Protection Juveniles (14-17 years of age)[15]
	Data espionage	Sec. 202a	Power of disposition of data holder[16]
	Data interception	Sec. 202b	Confidentiality of communication[17]
	Acts preparatory to data espionage and data interception	Sec. 202c	Various (reference to the protected legal interest of Sec 202a, Sec 202b, Sec 303a, Sec 303b)[18]
	Fraud	Sec. 263	Asset[19]
	Computer-related Fraud	Sec. 263a	Asset[20]

[4] *Steinmetz* in MüKo-StGB § 86, No. 1; *Sternberg-Lieben* in Sch/Sch § 86, No. 1*; Gercke* in Gercke/Brunst, Praxishandbuch Internetstrafrecht, page 160.
[5] *Steinmetz* in MüKo-StGB § 86a, No. 1.
[6] OLG Celle JR 1998, 79.; *Rudolphi* in SK-StGB § 130, No.1a.
[7] *Lackner/Kühl,* § 130 StGB, no. 1; *Lenckner* in Sch/Sch § 130, No. 1a.
[8] *Hörnle* in MüKo-StGB § 184, Rn. 2; *Scholz/Liesching*, Jugendschutz, III StGB, § 184, No. 1.
[9] *Gercke* in Gercke/Brunst, Praxishandbuch Internetstrafrecht, page 131.
[10] *Schreibauer,* Das Pornographieverbot des § 184 StGB, 1999, page. 80; H*örnle* in MüKo-StGB, § 184a, Rn. 2.
[11] *Lenckner/Perron/Eisele* in Sch/Sch, § 184a, No. 1.
[12] *Schreibauer,* Das Pornographieverbot des § 184 StGB, 1999, page. 80; H*örnle* in MüKo-StGB, § 184a, Rn. 2.
[13] BT-Drs. 12/3001 S. 4, 12/4883 S. 8, BGHSt 45, 45, LG Stuttgart NStZ 2003, 36, *Harms*, NStZ 2003, 646, *Wolters/Horn* in SK-StGB, § 184a Rn.1; *Lenckner/Perron,* in Sch/Sch, § 184b, Rn.1.
[14] *Hörnle* in MüKo-StGB, § 184b, Rn. 1.
[15] *Gercke* in Gercke/Brunst, Praxishandbuch Internetstrafrecht, page 153.
[16] *Schreibauer/Hessel*, KR 2007, 616; *Fischer*, Strafgesetzbuch, § 202a, Rn. 2; *Tag* in Nomos Komentar Gesamtes Strafrecht, § 202a, Rn. 3; *Schumann*, NStZ 2007. 676; Kritisch zum Rechtsgut: *Vassilaki,* CR 2008, 131.
[17] *Gercke* in Gercke/Brunst, Praxishandbuch Internetstrafrecht, page 71.
[18] *Gercke* in Gercke/Brunst, Praxishandbuch Internetstrafrecht, page 153.
[19] RGSt 74 168; BGHSt 3, 99; BGHSt 16, 325; SK-StGB/Hoyer, § 263 Rn. 7; LK/Tiedemann, § 263 Rn. 18, 24 f. vor § 263, Fischer, § 263, Rn. 3
[20] BGH, NJW 1995, 669; Bühler, MDR 1987, 449; MüKo-StGB/Hefendehl/Wohlers, § 263 a Rn. 1; SK-StGB/ Günther, § 263 a Rn. 4

	Forgery of data intended to serve as evidence	Sec. 269	Security and Reliability of legal relations and procedures related to evidence[21]
	Data manipulation	Sec. 303a	Integrity of computer data[22]
	System manipulation	Sec. 303b	Integrity of computer systems[23]
Copyrigh t Act (Urheber gesetz)	Unlawful exploitation of copyrighted works	Sec. 106	Utilization of copyright protected work[24]
	Infringement of related rights	Sec. 108	Utilization of related rights[25]
	Infringement of technological measures and rights-management information	Sec. 108b	Effective technical measures[26]
Interstate Agreement on Protection of Minors in relation to Media (Jugendmedienschutz-Staatsvertrag)	Criminal Sanctions	Sec. 23	Youth Protection[27]

(2) Please give typical examples of criminal laws concerning

(a) attacks against IT systems

A typical example of a criminal law provision concerning attacks against IT systems is Sec. 303b Penal Code.

Section 303b Computer sabotage
(1) Whosoever interferes with data processing operations which are of substantial importance to another by
1. committing an offence under section303a(1); or
2. entering or transmitting data (section 202a(2)) with the intention of causing damage to another; or
3. destroying, damaging, rendering unusable, removing or altering a data processing system or a data carrier,
shall be liable to imprisonment not exceeding three years or a fine.
(2) If the data processing operation is of substantial importance for another's business, enterprise or a public authority, the penalty shall be imprisonment not exceeding five years or a fine.
(3) The attempt shall be punishable.

[21] *Bühler*, MDR 1987, 453; Sch/Sch*/Cramer* § 269 Rn.3 m.w.N; A.A. SK-StGB*/Hoyer*, § 269 Rn. 1; *Lenckner/Winkelbauer* CR 1986, 824, die die Auffassung vertreten, die Norm sichere die Dispositionsfreiheit derjenigen Teilnehmer am Rechtsverkehr, die durch unechte Beweismittel zu sonst nicht getätigtem rechtserheblichen Verhalten veranlasst werden könnten. Zum Rechtsgut vgl. auch *Möhrenschlager*, wistra 1986, 134.
[22] *Hilgendorf/Frank/Valerius,* Rn. 193; SK-StGB*/Hoyer*, § 303a, Rn. 2; LK/*Tolksdorf*, § 303a, Rn. 2; Sch/Sch/*Stree*, § 303a, Rn. 1
[23] BT-Drs. 10/5058, S. 34; *Fischer,* § 303b, Rn. 1
[24] Erbs/Hohlhaas*/Kaiser, U* 180, § 106, Rn. 5
[25] Wandtke/Bullinger*/Hildebrandt, §* 108, Rn. 2
[26] Erbs/Hohlhaas*/Kaiser, U* 180, § 108b, Rn. 3
[27] Erbs/Kohlhaas, Strafrechtliche Nebengesetze, JMStV, § 23 Rn. 5

(4) In especially serious cases under subsection (2) above the penalty shall be imprisonment from six months to ten years. An especially serious case typically occurs if the offender
1. causes major financial loss,
2. acts on a commercial basis or as a member of a gang whose purpose is the continued commission of computer sabotage, or
3. through the offence jeopardises the population's supply with vital goods or services or the national security of the Federal Republic of Germany.
(5) Section 202c shall apply mutatis mutandis to acts preparatory to an offence under subsection (1) above.

Sec. 303b protects the integrity of computer systems.[28]

Actus Reus:

The provision requires that the offender interferes with a data processing operation. Data processing includes results of electronic[29] processes as well as the processing of data.[30] In this regard the provision covers input[31] as well as storage processes.[32] An interference requires that an intended process was manipulated or modified.[33] This is not the case if a manipulation has no recognizable consequences.[34] The criminalization further requires that the data processing operation is of substantial importance to another. This is the case if the operation of the authorized person is in danger.[35] Details of the interpretation of the term are controversially discussed.[36] Even computer systems from private users are covered.[37] However, based upon the explanatory note to the draft law that amended Sec. 303b in 2007 the application with regard to private people requires that the system is of essential relevance to them.[38] The offence can either be committed by committing an act covered by Sec. 303a, by input of computer data (that especially covers denial of service attacks[39]) or interference with the system or data storage devices.

Mens rea:

Sec. 303 requires that the offender acts intentionally.[40]

(b) Violation of IT privacy

One example for a provision protecting privacy is Sec. 202b Penal Code

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

---

[28] BT-Drs. 10/5058, S. 34; *Fischer,* § 303a, Rn. 1;
[29] *Lenckner/Winkelbauer,* CR 1986, 658f.
[30] BT-Drs. 10/318, S. 21; *LK/Tiedemann*Rn. 22; MüKo-StGB*/Hefendehl/Wohlers*, § 263a, Rn. 12.
[31] SK-StGB*/Hoyer*, § 303b, Rn. 8.
[32] BT-Drs. 10/5058, S. 35; Sch/Sch*/Stree*, § 303b, Rn. 3.
[33] BT-Drs. 10/5058, S. 35.
[34] LK/*Tolksdorf*, § 303b StGB, Rn. 11; Sch/Sch*/Stree*, § 303b, Rn. 10
[35] *Gercke/Brunst,* Rn. 137.
[36] Vgl. dazu SK-StGB*/Hoyer* § 303b, Rn. 10; *Fischer,* § 303b, Rn. 6;
[37] Vgl. dazu *Ernst*, NJW 2007, 2665; *Fischer,* § 303b, Rn. 6.
[38] BT-Drs. 16/3656, S. 13.
[39] BT-Drs. 16/5058, S. 13.
[40] *Fischer,* § 303b, Rn. 18; Wabnitz/Janovsky*/Bär,* Kap. 12, Rn. 75.

Actus Reus:

Sec. 202b Penal Code protect the confidentiality of communication.[41] Until the provision was introduced in 2007 data was only partly covered during the transmission process.[42] The provision only protects electronic data. This requires covers data that can be stored or transmitted electronically or magnetically or otherwise in a manner not immediately perceivable. A data processing requires that data is transmitted from a source to a destination.[43] The physical relocation of data storage devices is not covered.[44] Operations within a computer system are however included.[45] The application of the provision further requires that the transmission takes place "non-public". This includes any transmission not intended for public.[46] In this regard not the content but the type of transmission process is crucial.[47] Sending an e-mail is consequently non-public[48] while interception of the upload of a file to a public Internet website is not covered by Sec. 202b.[49] Interception covers any act where the offender obtains data by using technical means.[50] Technical means includes hardware and software solutions.[51] Interception includes live/real-time monitoring of computer data processes.[52]

Mens rea:

Sec. 202b requires that the offender acts intentionally.[53]

(c) forgery and manipulation of digitally stored data

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

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

---

41 *Gercke* in Gercke/Brunst, Praxishandbuch Internetstrafrecht, page 71.
42 Vgl. dazu BT-Drs. 16/3656, S. 11. Vgl. dazu auch *Schreibauer/Hessel*, KR 2007, 617.
43 *Gercke/Brunst,* Rn. 105.
44 Ebenso: *Gröseling/Höfinger*, MMR 2007, 552.
45 Dies wird in Art. 3 der Cybercrime Konvention anders als in § 202b StGB ausdrücklich hervorgehoben: „... from or within a computer system".
46 *Gröseling/Höfinger*, MMR 2007, 552; *Vassilaki*, CR 2008, 132.
47 BT-Drs. 16/3656, S. 11.
48 Vgl. dazu *Fischer,* § 202b, Rn. 2; BT-Drs. 16/3656, S. 11
49 *Gercke/Brunst,* Rn. 105.
50 *Hilgendorf*, JuS 1996, 704; LK/ *Schünemann*, § 202a, Rn. 6; *Sch/Sch/Lenckner*, § 202a, Rn. 10.
51 *Gercke/Brunst,* Rn. 109.
52 Vgl. dazu auch BT-Drs. 16/3656, S. 11; *Schreibauer/Hessel*, KR 2007, 617.
53 *Fischer,* § 202b, Rn. 8.

(d) distribution of computer viruses

The transmission of computer viruses is not specifically addressed in the Penal Code. The introduction/installation of computer virus can – depending on the payload – be covered by Sec. 303a and/or Sec. 303b.

Sec. 202c Penal code criminalizes the production of a computer virus. A computer virus in general needs to be installed on the victims computer system. This installation process can be covered by Sec. 303a StGB. Consequently the production of such software to commit a crime is covered by Sec. 303a, paragraph 3 (that refers to Sec. 202c).

Based upon a more extensive interpretation of „distribution" (in relation to pornography) by the German Federal Court (Bundesgerichtshof) „distribution" may also cover the transmission of a computer virus through a computer network.

Section 202c Acts preparatory to data espionage and phishing
(1) Whosoever prepares the commission of an offence under section 202a or section 202b by producing, acquiring for himself or another, selling, supplying to another, disseminating or making otherwise accessible
1. passwords or other security codes enabling access to data (section 202a(2)), or
2. software for the purpose of the commission of such an offence,
shall be liable to imprisonment not exceeding one year or a fine.
(2) Section 149(2) and (3) shall apply mutatis mutandis.

(e) crimes related to virtual identities of users, e.g., forging, stealing or damaging virtual personalities

Currently identity-related crime as such is not criminalized under German law.[54] The European Union currently evaluates if a criminalization is required.[55] If the European Union decides to harmonize legislation throughout the 27 member states could be introduced.

(f) other innovative criminal prohibitions in the area of ICT and internet, e.g., criminalisation of the creation and possession of certain virtual images, violation of copyright in the virtual sphere.

One "innovative" approach with regard to criminalization is Sec. 176, paragraph 4

Section 176 Child abuse
(3) In especially serious cases the penalty shall be imprisonment of not less than one year.
(4) Whosoever
[...]
3. presents a child with written materials (section 11(3)) to induce him to engage in sexual activity with or in the presence of the offender or a third person or allow the offender or a third person to engage in sexual activity with him; or
[...]

The provision criminalizes „grooming"/solicitation of children for sexual purposes. The approach that criminalizes preparatory acts to sexual abuse of children follows the concept of the 2007 Council of Europe Convention the protection of children. However, the main difference to the Council of Europe approach is the fact that Sec. 176 does not criminalize contacting child through ICT but requires the interaction with written materials. Written material is defined in Sec. 11(3). It includes data storage devices – but not data itself. Therefore sending a child messages on a data storage devices is covered but not sending a data message through a computer network.

[54] *Gercke*, CR 2005, 606ff.
[55] *Gercke*, ZUM 2012, 628.

(3) How is criminal conduct (actus reus) typically defined in these crimes (by description of act, by consequence, other)? How is the object defined ("data", "writings", contents)?

The dogmatic concept used to define the crimes varies significantly. Some offences (such as Sec. 86) describe an act without requiring a consequence. This is a common approach especially with regard to illegal content. Provision related to this category of crime do in general not require that a consequence (such as actual download of child pornography by user) occurs. It is sufficient that an act leads to an abstract endangerment.

Provisions related to the category "confidentiality of computer data and system" in general define consequences (e.g. Sec. 202a).

(4) Is criminal liability for certain cyber crime limited to particular groups of perpetrators and/or victims?

The Penal Code contains some provisions that limit the criminalization to particular groups of offenders. Such offences can especially be found in Sec. 331 et seq. The core set of offences related to computer crime and cybercrime does however not limit the applicability to certain offenders. A provision that is at least partly limited to certain "victims" is Sec. 184 Penal Code. The provision in general requires an abstract endangerment of minors. With regard to the "abstract" nature of the endangerment does not require a concrete victim the provision is however only partly comparable to offences that limit criminal liability to certain groups of victims.

(5) Does criminal liability in the area of ICT and internet extend to merely reckless or negligent conduct?

Almost all provisions related to the core group of computer and cybercrime offences do only criminalize intentional acts. Based on Sec. 15 Penal Code negligence is only criminalized if expressly mentioned in the provision. As this is not the case with regard to most provisions negligence is not covered.

	Title	Provision	Intent	Negligence
Penal Code (Strafgesetzbuch)	Dissemination of propaganda material of unconstitutional organisations	Sec. 86	Yes	No
	Using symbols of unconstitutional organisations	Sec. 86a	Yes	No
	Incitement to hatred	Sec. 130	Yes	No
	Distribution of Pornography	Sec. 184	Yes	No
	Distribution of pornography depicting violence or sodomy	Sec. 184a	Yes	No
	Distribution, acquisition and possession of child pornography	Sec, 184b	Yes	No
	Distribution, acquisition and possession of juvenile pornography	Sec. 184c	Yes	No
	Data espionage	Sec. 202a	Yes	No
	Data interception	Sec. 202b	Yes	No
	Acts preparatory to data espionage and data interception	Sec. 202c	Yes	No
	Fraud	Sec. 263	Yes	No
	Computer-related Fraud	Sec. 263a	Yes	No
	Forgery of data intended to serve as evidence	Sec. 269	Yes	No
	Data manipulation	Sec. 303a	Yes	No
	System manipulation	Sec. 303b	Yes	No
Copyright Act (Urheberges etz)	Unlawful exploitation of copyrighted works	Sec. 106	Yes	No
	Infringement of related rights	Sec. 108	Yes	No
	Infringement of technological measures and rights-management information	Sec. 108b	Yes	No

Interstate Agreement on Protection of Minors in relation to Media (Jugendmedienschutz-Staatsvertrag)	Criminal Sanctions	Sec. 23	Yes	Yes

(6) Are there specific differences between the definition of cyber crimes and "traditional" crimes?

German criminal law does neither provide a definition for traditional crimes nor for cybercrimes. Cybercrime compromises a core set of offences. The mere fact that ICT is used at one or more stages of the offence does not turn a traditional crime into a cybercrime. One example is auction fraud. Even if most of those offences intensively involve computer system those offences remain traditional fraud (Sec. 263) and not computer-related crime (Sec. 263a).

(C) Legislative technique

(1) Are there specific problems with respect to the principle of legality (e.g., vagueness, open-ended reference of the crime definition to other regulations)?

In general most provision in the Penal Code follow international best practices. With regard to those provision there are no intensive discussions related to legality. One provision that was controversially discussed during the implementation was Sec. 263a.

Section 263a Computer fraud
(1) Whosoever with the intent of obtaining for himself or a third person an unlawful material benefit damages the property of another by influencing the result of a data processing operation through incorrect configuration of a program, use of incorrect or incomplete data, unauthorised use of data or other unauthorised influence on the course of the processing shall be liable to imprisonment not exceeding five years or a fine.
[...]

The element that was controversially discussed was „data or other unauthorised influence on the course of the processing". [56] This part of the provision is designed as catchall element[57] that requires a restrictive interpretation.[58]

[56] *Schulz*, JA 1995, 539.
[57] *Hilgendorf/Frank/Valerius*, Computer- und Internetstrafrecht, Rn. 51; *Ranft*, Jus 1997, 21; *Achenbach*, JR 1994, 293; *Füllkrug*, Kriminalistik, 1987, 590; *Bühler*, MDR 1987, 450f.; *Lenckner/Winkelbauer,* CR 1986, 658; *Tiedemann* in LK, § 263a Rn. 62.
[58] Gercke in Gercke/Brunst, Praxishandbuch Internetstrafrecht, page 101.

(2) How does legislation avoid undue chilling effects on legitimate use of ICT or of the Internet?

It is possible to differentiate between general and specific measures. General measure to avoid unintended effects related to the legitimate use of the Internet is the requirement of an intent. The limitation of criminalization to intentional act may go along with challenges for law enforcement – but it ultimately servers as a safeguard with regard to possible effects on the legitimate use of ICT.

A more specific measure can be demonstrated by referring to Sec. 202c Penal Code. In order to avoid an interference with legitimate penetration tests carried out by system administrators the Sec. 202c (1) 2. requires

- that the purpose of the software is the commission of a crime, and
- the offender prepares the commission of an offence

Section 202c Acts preparatory to data espionage and phishing
(1) Whosoever prepares the commission of an offence under section 202a or section 202b by producing, acquiring for himself or another, selling, supplying to another, disseminating or making otherwise accessible
1. passwords or other security codes enabling access to data (section 202a(2)), or
2. software for the purpose of the commission of such an offence, shall be liable to imprisonment not exceeding one year or a fine.
(2) Section 149(2) and (3) shall apply mutatis mutandis.

(3) How does criminal legislation avoid becoming obsolete in light of rapid technological innovation? E.g., how are changes in the use of internet and social networks taken into account? - how is the law adapted to technological progress (e.g., by reference to administrative regulations)?

The cybercrime related provisions of the Penal Code do not make use of the possibility of referring to regulations. Taking into account that various technical developments took place in the last decades the need for amendments was and is limited. The stability of criminal law and its independence from technical developments was mainly achieved by a technology neutral drafting. By not referring to concrete technical applications or services (such as social networks) but to concrete acts the law is applicable independently of technical developments. The computer crime related provisions that were introduces by the Second Act to Combat Economic Crime[59] are for example even applicable with regard to Internet-related conduct.

However, there are areas where legal reforms are required. One area is illegal content and more specifically the provisions related to pornography. All of them refer to "writings". Despite the fact that the definition of "writings" in Sec. 11 (3) was amended in 1997 and now also covers "data storage devices" the provision does not cover mere data transfer processes. This limits the applicability of the provision with regard to certain Internet-related acts (such as the use of streaming-video to watch child pornography content).

(D) Extent of criminalisation

(1) To what extent do criminal laws cover mere preparatory acts that carry a risk of furthering abuse, e.g., acquisition or possession of software that can be used for "hacking", "phishing", computer fraud, or

[59] Zweites Gesetz zur Bekämpfung der Wirtschaftskriminalität, BGBl. 1986 I 721; Vgl. zum 2. WiKG *Lenckner/Winkelbauer*, CR 1986, 483ff.; *dies.* CR 1986, 654ff.; *dies.* CR 1986, 824ff.; *Haft*, DSWR 1986, 255ff.; *Achenbach*, NJW 1986, 1835ff.; *Weber*, NStZ 1986, 481ff. *Haft,* NStZ 1987, 6ff.; *Möhrenschlager*, wistra 1986, 123ff.; *ders*. Wistra 1986, 128ff. *Schroth*, wistra 1986, 158ff.; *Sieber*, Informationstechnologie und Strafrechtsreform, Zur Reichweite des zukünftigen Zweiten Gesetzes zur Bekämpfung der Wirtschaftskriminalität, 1985.

bypassing download protection? If so, has there been controversy about introducing such laws? Have legislatures made specific efforts to avoid over-criminalization?

For many decades German Criminal Law took a very restrictive approach when it comes to the criminalization of preparatory acts. Especially through EU harmonization processes various preparatory acts are today criminalized.

	Title	Commission	Preparation
Penal Code (Strafgesetzbuch)	Dissemination of propaganda material of unconstitutional organisations	Sec. 86	(-)
	Using symbols of unconstitutional organisations	Sec. 86a	(-)
	Incitement to hatred	Sec. 130	(-)
	Distribution of Pornography	Sec. 184	(-)
	Distribution of pornography depicting violence or sodomy	Sec. 184a	(-)
	Distribution, acquisition and possession of child pornography	Sec, 184b	Partly (see paragraph 4)
	Distribution, acquisition and possession of juvenile pornography	Sec. 184c	Partly (see paragraph 4)
	Data espionage	Sec. 202a	Yes, Sec. 202c
	Data interception	Sec. 202b	Yes, Sec. 202c
	Fraud	Sec. 263	(-)
	Computer-related Fraud	Sec. 263a	Yes, Sec. 263a (4)
	Forgery of data intended to serve as evidence	Sec. 269	Not only use but also creation is covered
	Data manipulation	Sec. 303a	Yes, Sec. 202c
	System manipulation	Sec. 303b	Yes, Sec. 202c
Copyright Act (Urhebergesetz)	Unlawful exploitation of copyrighted works	Sec. 106	(-)
	Infringement of related rights	Sec. 108	(-)
	Infringement of technological measures and rights-management information	Sec. 108b	Yes
Interstate Agreement on Protection of Minors in relation to Media (Jugendmedienschutz-Staatsvertrag)	Criminal Sanctions	Sec. 23	(-)

(2) To what extent has the mere possession of certain data been criminalised? In what areas, and on what grounds?

The criminalization of possession is limited to certain offences related to illegal content. The most relevant provisions are Sec. 184b (4) and Sec. 184c (4). Both do not only criminalize the possession of certain illegal content (child pornography and juvenile pornography) but also "undertaking" to obtain possession. Based on Sec. 11 (1) No. 6 "undertaking" includes attempt and completion. The criminalization is justified with the risk that the possession of such material may motivate the offender to commit sexual offences or he may use such material to convince (groom) children to get engaged in sexual activities.

Section 11 Definitions
(1) For the purposes of this law
[...]
6. 'Unternehmen (undertaking)' of an offence means both attempt and completion;
[...]

Section 184b Distribution, acquisition and possession of child pornography
[...]
(4) Whosoever undertakes to obtain possession of child pornography reproducing an actual or realistic activity shall be liable to imprisonment not exceeding two years or a fine. Whosoever possesses the written materials set forth in the 1st sentence shall incur the same penalty.
[...]

Section 184c Distribution, acquisition and possession of juvenile pornography
[...]
(4) Whosoever undertakes to obtain possession of child pornography reproducing an actual or realistic activity shall be liable to imprisonment not exceeding one year or a fine. The 1st sentence shall not apply to acts of persons related to juvenile pornography produced by them while under eighteen years of age and with the consent of the persons therein depicted.
[...]

How is "possession" of data defined? Does the definition include temporary possession or mere viewing?

Possession is not defined by law. Possession is interpreted as control executed with the will to control.[60] The question if this requires a certain duration of control is controversially discussed.[61] This question is from particular relevance with regard to the criminalization of watching child pornography online. Depending on the software configuration images that are watched online are only downloaded to the temporary RAM memory. If the offender closes the website the information are deleted. It is uncertain if this is sufficient to prosecute him.

[60] BT-Drs. 12/3001, S.4f. *Hilgendorf/Frank/Valerius,* Computer- und Internetstrafrecht, Rn. 418; *Hilgendorf/Wolf,* K&R 2006, 544. Zur Verklammerung beim Verschaffen, Besitz und der anschließenden Weitergabe von kinderpornographischen Bilddateien nach § 52 StGB vgl. BGH NStZ 2005, 444 f.

[61] *Gercke,* ZUM 2003, 349; *ders.*, Rechtswidrige Inhalte im Internet, S. 76 f.; *Harms* NStZ 2003, 648ff.; *Hörnle* in MüKo-StGB, § 184b, Rn. 26.

(3) To the extent that possession of or granting access to certain data have been defined as criminal, does criminal liability extend to service providers (e.g., hosting or access providers)?

In general criminal law provisions criminalizing access to certain material can also be committed by service provider. As a consequence the prosecution service in Munich (Germany) started preliminary proceedings against the CEO of CompuServe Germany.[62] The prosecution based their investigation on the fact that pornographic images showing the sexual abuse of children that were stored on servers of CompuServe US were available to customers of CompuServe Germany.[63] The investigation and the subsequent trial against the CEO of CompuServe Germany were based on the assumption that access providers are responsible for the content to which they provide users access.[64] These investigations started an intensive discussion process about the need for legislation limiting the liability of Internet Service Providers.[65] The discussion process was facilitated by the fact that at the same time the European Union started a similar discussion within the drafting process of the E-Commerce Directive.[66] In 1997 – three years before the EU E-Commerce Directive[67] was finalized – the Act on the Utilization of Teleservices came into effect.[68] Among other regulations for Internet-based services, this act contained a specific provision dealing with the responsibility of Internet Service Providers (Sec. 5).[69]

---

[62] Regarding the Compuserve case see *Local Court (Amtsgericht) Munich, Multimedia und Recht* (MMR) 1998, page 432 et seqq. with annotation *Sieber*; *District Court (Landgericht) Munich*, *Neue Juristische Wochenschrift* (NJW) 2000, page 1051 et seq; *Hoeren*, *Neue Juristische Wochenschrift* (NJW) 1998, page 2792 et seqq

[63] *Derksen*, *Neue Juristische Wochenschrift* (NJW) 1997, 1878 et seqq.

[64] *Local Court (Amtsgericht) Munich, Multimedia und Recht* (MMR) 1998, page 432 et seqq. For a summary of cases in the English language see: http://www.qlinks.net/comdocs/somm.htm (last visited: June 2008); *Frydman/Rorive*, Regulating Internet Content through Intermediaries in Europe and the USA, *Zeitschrift fuer Rechtssoziologie*, 2002, page 52 – available at: http://www.isys.ucl.ac.be/etudes/cours/linf2202/Frydman_&_Rorive_2002.pdf (last visited: June 2008). For the court decision in English see http://www.kuner.com/data/reg/somm.html (last visited June 2008).

[65] *Pichler*, *Multimedia und Recht (*MMR) 1998, page 79.

[66] Directive 2000/31/EC of the European Parliament and the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) – available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:178:0001:0016:EN:PDF (last visited June 2008); Apart from the E-Commerce Directive, the US Digital Milenium Copyright Act was used as model legislation for the drafting of the German legislation on provider liability. For more information on model laws used in the drafting process, *see Spindler*, *Multimedia und Recht*, page 496; *Freytag*, Multimedia und Recht 1999, page 207.

[67] Directive 2000/31/EC of the European Parliament and the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) – available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:178:0001:0016:EN:PDF (last visited: June 2008); Regarding the liability related regulations see: *Frydman/Rorive*, Regulating Internet Content through Intermediaries in Europe and the USA, Zeitschrift fuer Rechtssoziologie, 2002, page 52 – available at: http://www.isys.ucl.ac.be/etudes/cours/linf2202/Frydman_&_Rorive_2002.pdf (last visited: June 2008).

[68] Regarding the development of the Teleservice 1997 *see Bundestagsdrucksachen* (BT-Drs) 13/7385, page 16 et seq..; *Paul*, *Primawrrechtliche Regelungen zur Verantwortlichkeit von Internetprovidern aus strafrechtlicher Sicht,* 2005, page 73; *Spindler* in Spindler/Schmitz/Geis, TDG, Vor § 8 Rn.2.

[69] Section 5 - Responsibility

(1) Providers shall be responsible in accordance with general laws for their own content which they make available for use.

(2) Providers shall not be responsible for any third-party content which they make available for use unless they have knowledge of such content and are technically able and can reasonably be expected to block the use of such content.

Within the implementation of the EU E-Commerce Directive,[70],adopted by the European Parliament in 2000, the regulation concerning the liability of Internet Service Providers in the Teleservice Act was modified in 2001 to fully meet the requirements of the Directive.[71] The regulations contained in Article 5 Teleservice Act 1997 were split up into four provisions and slightly amended. With respect to the fact that both the EU E-Commerce Directive and the Teleservice Act 1997 were based on the principle of a graded responsibility, the practical outcome of the changes was minor. The 16 States have developed a similar system of graded responsibility in the Interstate Agreement on Media services.[72]

Although the Telemedia Act of 2007 carries significant changes compared to the Teleservice Act of 2001, those changes do not affect the liability regime.[73] The drafters of the law kept the provisions of the Teleservice Act 2001 without relevant changes.[74]

Telemedia Act of 2007

Section 8 - General Principles
(1) Providers shall be responsible for their own information, which they make available for use, under terms of binding law.
(2) Providers as defined under Sections 9 to 11 shall not be obliged to supervise information they have transmitted or stored or to research to determine circumstances that indicate an illegal activity. Obligations to remove or block the use of information under binding law shall remain unaffected even if the provider is not responsible pursuant to Sections 9 to 11. The confidentiality of communications under Section 85 of the Telecommunications Act shall be observed.

Section 9 - Transmission of Information [Mere Conduit]
(1) Providers shall not be responsible for third-party information that they transmit in a communications network or to which they provide user access if they have 1. not initiated the transmission 2. not selected the addressees of the information that has been transmitted 3. not selected or modified the information that has been transmitted.
Sentence 1 shall not apply when the service provider deliberately collaborates with one of the recipients of his service in order to undertake illegal acts.
(2) The transmission of information pursuant to Paragraph 1 and the provision of access to it shall also constitute the automatic, short-term intermediate storage of such information to the extent that this is done only to facilitate the transmission in the communications network and the information is not stored any longer than normally required for transmission purposes.

---

(3) Providers shall not be responsible for any third-party content to which they only provide access. The automatic and temporary storage of third-party content due to user request shall be considered as providing access.
(4) The obligations in accordance with general laws to block the use of illegal content shall remain unaffected if the provider obtains knowledge of such content while complying with telecommunications secrecy under § 85 of the Telecommunications Act (*Telekommunikationsgesetz*) and if blocking is technically feasible and can reasonably be expected.

[70] Directive 2000/31/EC of the European Parliament and the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) – available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:178:0001:0016:EN:PDF.

[71] *Harting*, *Gesetzesentwurf zur Umsetzung der E-Commerce-Richtlinie*, CR 2001, page 271et seq

[72] Section 6 – 9 Interstate Agreement on Media services.

[73] For more information regarding the changes see: *Schmitz*, *Kommunikation und Recht* (KR), 2007, page 135 et seq.; *Hoeren*, *Neue Juristische Wochenschrift* (NJW), 2007, page 801 et seq.; *Rossnagel*, *Neue Zeitschrift fuer Verwaltungsrecht* (NVwZ), 2007, page 743 et seq.

[74] *See: Bundestagsdrucksachen* (BT-Drs) 16/3078, page 15. *Schmitz* in Spindler/Schuster, *Recht der Elektronischen Medien*, 2008, *Allg. Vorbemerkung zum* TMG Rn. 1

Section 10 - Intermediate Storage to Accelerate Data Transmission [Cacheing]
Providers shall not be responsible for automatic, intermediate storage for a limited period of time, carried out solely to enhance the efficiency of the transmission of third-party information to other users upon the latter's request, if they
1. do not modify the information
2. comply with conditions on access to the information
3. comply with rules regarding the updating of the information, specified in a manner widely recognized and used by the industry
4. do not interfere with the lawful use of technology, widely recognized and used by industry, to obtain data on the use of the information
5. act expeditiously to remove or to disable access to the information it has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement
Section 9 (1) Sentence 2 shall apply mutatis mutandis.

Section 11 - Storage of Information [Hosting]
Providers shall not be responsible for third-party information that they store for a user if
1. they have no actual knowledge of illegal activity or information and, with respect to claims for damages, are not aware of facts or circumstances from which the illegal activity or information is apparent, or
2. they act\ expeditiously to remove or to disable access to the information as soon as they become aware of such circumstances.
Sentence 1 shall not be applied if the user is subordinate to or supervised by the provider.

What are the requirements of their liability, especially concerning mens rea?

The requirements regarding the liability of service provider are first of all the same as for everybody else. All requirements (especially actus reus and mens rea) must be proven. The Telemedia Act serves as an additional layer of protection. Only if the specific requirements – that are depending on the type of service provide – are fulfilled the offender is liable under criminal law.

Are providers obliged to monitor and control what information they provide or offer access to?

Based on Sec. 8 (2) access and hosting provider are not obliged to monitor stored or transmitted information.

Section 8 - General Principles
(1) Providers shall be responsible for their own information, which they make available for use, under terms of binding law.
(2) Providers as defined under Sections 9 to 11 shall not be obliged to supervise information they have transmitted or stored or to research to determine circumstances that indicate an illegal activity. Obligations to remove or block the use of information under binding law shall remain unaffected even if the provider is not responsible pursuant to Sections 9 to 11. The confidentiality of communications under Section 85 of the Telecommunications Act shall be observed.

Are providers obliged to provide information on the identity of users?

There is no obligation of internet service provider to register users. In addition there is currently not data retention regime in place.

Are providers obliged to prevent access to certain information? If so, under what conditions, and at whose cost? Is there criminal liability for violating such obligations?

Germany recently abolished legislation that required access provider to block certain content on a basis of a black list provided by the Federal Police in order to prevent access to child pornography material.

However with regard to hosting provider Sec. 11 Telemedia Act defines a "notice-and-takedown" procedure. If a hosting provider receives information about illegal activity or illegal content he is obliged to remove or disable access to the information. A violation of the obligation opens the door for criminal liability (that is otherwise excluded).

> ***Section 11 - Storage of Information [Hosting]***
> *Providers shall not be responsible for third-party information that they store for a user if*
> *1. they have no actual knowledge of illegal activity or information and, with respect to claims for damages, are not aware of facts or circumstances from which the illegal activity or information is apparent, or*
> *2. they act\ expeditiously to remove or to disable access to the information as soon as they become aware of such circumstances. Sentence 1 shall not be applied if the user is subordinate to or supervised by the provider.*

(4) What general, in particular constitutional limits to criminalising conduct have been discussed with respect to ICT and internet crime (e.g., freedom of speech, freedom of the press, freedom of association, privacy, "harm principle", requirement of an act, mens rea requirements)?

The German Penal Code quite extensively criminalizes illegal content. This leads to potential conflicts with the principle of freedom of expression. Freedom of expression is protected by Art. 5 of the German Constitution (Basic Law). However, Art. 5 limits the protection of freedom of expression and clarifies that provisions of general laws (such as the Penal Code) may limit freedom of expression.

> ***Article 5 [Freedom of expression, arts and sciences]***
> *(1) Every person shall have the right freely to express and disseminate his opinions in speech, writing and pictures, and to inform himself without hindrance from generally accessible sources. Freedom of the press and freedom of reporting by means of broadcasts and films shall be guaranteed. There shall be no censorship.*
> *(2) These rights shall find their limits in the provisions of general laws, in provisions for the protection of young persons, and in the right to personal honour.*
> *(3) Arts and sciences, research and teaching shall be free. The freedom of teaching shall not release any person from allegiance to the constitution.*

(5) Does the law provide for criminal sanctions specifically targeting cyber criminals, (e.g., a temporary ban from using the internet)?

Such measures are not defined by law.

(E) Alternatives to Criminalisation

(1) What role does criminal law play in relation to other ways of combatting abuse of ICT and the internet?

Germany is a country that follows different strategies when it comes to fighting cybercrime. Criminalization is only one component. Other components are crime prevention measures such as education and promoting technical solutions to prevent crime. However such alternative measure are not yet widely implemented.

Victims of crime do often not report crimes. If they follow up it is mostly through civil law. One example are copyright violations. Despite a criminal liability of those who intentionally violate copyright most victims that seek action make use of the means of civil law.

(2) What non-criminal means of combatting offensive websites are used/propagated (e.g., closing down websites, blocking access to websites)?

In 2010 Germany introduced a law on mandatory blocking of child pornography. Although the law was formally in power it was not applied and only two years later it was officially suspended. Now the focus is back on removal of illegal content at the source. Within the explanatory notes to the suspension of the legislation on blocking the

government reported great success in this regard. The federal police reported that two weeks after reporting a child pornography website 90 percent of them were taken down and four weeks after the report 98 percent were taken down.[75] The government explains this by referring to a more intensive involvement of hotlines such as INHOPE.[76]

(3) To what extent are ICT users expected to protect themselves (e.g., by encryption of messages, using passwords, using protective software)? Are there sanctions for not protecting one's computer to a reasonable extent, e.g., by using anti-virus software or protecting access to private networks by password? Does the lack of reasonable self-protection provide a defense for defendants accused of illegally entering or abusing another person's network or abusing their data?

There is no general obligation under German law that users need to protect themselves. However, some criminal law provisions require that the victim implemented protection measures. One example is Sec. 202a Penal Code. If the victim did not implement protection measures obtaining access to data is not criminalized.

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

(F) Limiting anonymity

(1) Are there laws or regulations obliging internet service providers to store users' personal data, including history of internet use? Can providers be obliged to provide such data to law enforcement agencies?

Germany implemented the EU Data Retention Directive. However, the German Constitutional Court declared the implementation partly unconstitutional. As a consequence data retention obligations are not in place. Data protection law limit the ability of internet service providers to store such information outside a data retention regime. If information are stored law enforcement agencies can order the disclosure or seize them.

(2) Are there laws or regulations obliging an internet service provider to register users prior to providing services?

There is no such obligation under German law.

(3) Are there laws or regulations limiting the encryption of files and messages on the internet?

After an intensive debate about crypto regulation in the 90th the German government decided not to introduce provisions limiting encryption technology.

Can suspects be forced to disclose passwords they use?

As a consequence of the ban on self-incrimination suspects can not be forced to disclose the password they used for encryption.

[75] BT-Drs. 17/6644, S. 6.
[76] Zur Tätigkeit von INHOPE und den Bemühungen um Löschung von kinderpornographischen Inhalten im Internet vgl. INHOPE Annual Report 2011.

(*G) Internationalisation*

(1) Does domestic law apply to data entered into the internet abroad?

Jurisdictional aspects are covered by Sec. 3-9 Penal Code. The Federal Courts opened the door for a broad interpretation of the principle of territoriality. Offenders that act from abroad and cause damage within Germany can be prosecuted under German law. In addition operator of websites that are stored outside of Germany might face prosecution even if they don't target a German audience. When it comes to provisions based on the principle of abstract endangerment German law is – based on the interpretation by the Federal Court – even applicable if content is stored in another country and it is impossible to prove that the content was accessed by users from Germany. This broad interpretation was criticized as is violates the principle of national sovereignty.

Is there a requirement of "double criminality" with respect to entering data from abroad?

There is no such requirement with regard to jurisdiction and applicability of German law. However, depending on the applicable framework for international cooperation there might be the need for dual criminality when it comes to MLA requests.

(2) To what extent has your country's criminal law in the area of ICT and internet been influenced by international legal instruments?

Germany signed and ratified the Council of Europe Convention on Cybercrime. However, the government did not fully implement the standards of the Convention. It does neither criminalize illegal access to a computer system (Art. 2 Convention on Cybercrime) nor does it provide Law Enforcement Agencies with a "quick freeze" instrument (Art. 16 Convention on Cybercrime).

Germany implemented various mandatory EU framework decisions and directives. The Framework Decision on Attacks Against Information Systems (2005) [77] was however only partly implemented and the Data Retention Directive (2005) [78] is still not in power.

(3) Does your country participate in discussions about the harmonisation of cybercrime legislation (such as the U.N. intergovernmental expert group on cybercrime)?

Based on the information provided by UNODC Germany was represented by the following experts: Nora Kaiser (MOJ), Michael Lauber, Klaus Aldinger, Ines Chajewski (all UN Mission in Vienna) and Wendy Hausoe, Federal Police.

---

[77] Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems. The legal basis for the Framework Decision, indicated in the preamble of the proposal for the Framework Decision is Articles 29, 30(a), 31 and 34(2)(b) of the Treaty on European Union. See: *Gercke*, Framework Decision on Attacks against Information Systems, CR 2005, 468 *et seq.*; *Sensburg*, Schutz vor Angriffen auf Informationssystem: Weiterer Schritt zum europaeischen Strafrecht?, Kriminalistik 2007, page 607ff.

[78] Directive of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communication networks and amending directive 2002/58/EC. Document 2005/0182/COD.

(H) Future developments Please indicate current trends of legislation and legal debate in your country concerning ICT and internet crime.

Currently there is an on-going debate the need to introduce reporting obligations. In addition to existing obligations (limited to certain data protection violations) the ministry of interior initiated a discussion about a more general reporting obligation.