Preparatory Colloquium
24-27 April 2013, Moscow (Russia)
Section II: Information Society and Penal Law

AUSTRIAN NATIONAL REPORT*

Madalena PAMPALK

(B) Legislative Practices and Legal Concepts

(1) How are criminal laws related to cyber-crimes codified in your country? Are they contained in a unified title or code or are they to be found in various codes or titles? (Please, provide appropriate citations).

Criminal laws related to cyber-crimes are primarily codified in the **Austrian Penal Code** ("Strafgesetzbuch", in the following "StGB"). Additionally, they can be found in **various codes**, including the Austrian Telecommunications Act 2003 ("Telekommunikationsgesetz 2003", in the following "TKG"), the Austrian E-Commerce Act ("E-Commerce-Gesetz", in the following "ECG"), the Federal Act on the Protection of Personal Data ("Datenschutzgesetz", in the following "DSG"), the Federal Act on the Protection of Conditional Access Services ("Zugangskontrollgesetz", in the following "ZuKG"), the Act on Pornography and the Federal Act on Copyright of Literature and Artwork and on Related Rights.

(2) What is the impact of judicial decisions on the formulation of criminal law related to cyber-crimes?

In general, the Austria legal system is based on the civil law system and Austrian courts are only bound by the jurisprudence of the Austrian Supreme Court. So far there exists little jurisprudence regarding cyber-crimes. Most judicial decisions relate to the pornographic presentation of minors.[1] However, as in the last two years complaints related to cyber-crimes, in particular internet fraud, phishing and hacking, have increased dramatically, jurisprudence will be developing rapidly.[2]

(3) To catch up with changing needs and circumstances and to attain new objectives, some laws are subject to frequent amendment. Normally, such amendments take the form of new laws. In certain cases these new laws, instead of simply modifying the parts of the law that need to be changed, present the required amendments into a consolidated text together with all past amendments. This technique is called recasting. Is that how cyber-crime laws are updated and adapted to changed realities in your country? Please provide appropriate references and citations.

No, in Austria the parts of the law that require change are amended; recasting is not applied.

---

* 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.

[1] Cf. *Reindl-Krauskopf*, Computerstrafrecht im Überblick, 2nd ed., at 7; *Birklbauer/Hilf/Tipold*, Strafrecht - Besonderer Teil I, remarks at the respective Articles.

[2] While from January to September 2011 3.114 complaints related to cyber-crimes were registered, within the same period in the year 2012 there were 7.729 complaints. Complaints regarding internet fraud increased from 1.179 to 3.530, complaints concerning phishing from 92 to 331 and those related to hacking from 158 to 515 (cf. Report by the Austrian Federal Criminal Police Office, 16 Oct. 2012, http://www.bmi.gv.at/cms/BK/presse/files/OTS_KrimStat_3QU2012.pdf).

(C) The Specific Cybercrime Offenses

(1) Concerning mens rea, must cybercrime offenses be intentional? Do they require a specific intent?

Cyber-crime offenses must be **intentional**. If the regulation does not state differently, *dolus eventualis* (conditional intent), i.e. the intent to seriously consider it possible that the crime could be accomplished and to accept this, is sufficient. Some crimes additionally require a specific intent ("erweiterter Vorsatz"), e.g. the crime "fraudulent misuse of data processing" (Art. 148a StGB) implies the intent to unlawfully enrich oneself or a third person. Some crimes require a higher level of intent than dolus eventualis, e.g. the crime "unlawful access to a computer system" (Art. 118a StGB) premises the (unconditional) intent ("Absicht") to (1) obtain data without right for oneself or for another unauthorized person, which are stored in a computer system, and to (2) make it available to another person for whom it is not destined by using it or making it public, and to (3) procure in this way an economic gain for oneself or another person or causing a disadvantage for another person. The far reaching mens rea requirement of Art. 118a StGB is rightly criticized.[3]

(2) Are there also negligent offenses in this field?

No.

(3) If yes, please, provide a list of those offenses.

-

(a) Integrity and functionality of the IT system

1. Illegal access and interception of transmission

a. Object – system or data?

Does your criminal law establish as a criminal offense the serious hindering, without right, of the functioning of a computer and/or electronic system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing information or data from a computer system, software or program?

b. Requirement of infringement of security measures?

Is it a requirement of your criminal law that the hacker conduct the hack of the computer system by using one or more software needed to defeat security measures and gain entry-level or higher level of access?

According to **Art. 126b StGB**, the **serious interference with the functioning of a computer system**, without right, by inputting or transmitting data is a criminal offense. A serious interference is the deadlock or slowing down of a computer system to such an extent that the remaining utility value of the user is not much higher than in the case of a deadlock of the system. The **infringement of security measures** is **not** required. The offender is to be sentenced to imprisonment up to six months or to pay a penalty up to 360 day-fines. Higher sentences apply if the functioning of the computer system is hindered over a longer period of time or if the crime was committed by a member of a criminal organisation.

A perpetrator is only to be sentenced according to this Art. 126b StGB if he/she is not punishable for the crime of "damaging of data" pursuant to Art. 126a StGB. Interference with the functioning of a comupter system by deleting,

[3] Cf., e.g., Salimi, Zahnloses Cyberstrafrecht? – Eine Analyse der gerichtlichen Straftatbestände zum Daten- und Geheimnisschutz, ÖJZ 2012, 998.

deteriorating, altering or suppressing information or data causes the damage of data and is, thus, penalized by Art. 126a StGB.[4]

Art. 118a StGB criminalizes the **unlawful access to a computer system** or a part of such a system by **infringing specific security precautions** within the computer system. Common examples of specific security precautions within the computer system are firewalls or computer passwords. Art. 118a StGB requires the (unconditional) intent (1) to obtain data without right for oneself or for another unauthorized person, which are stored in a computer system, (2) to make it available to another person for whom it is not destined by using it or making it public, and (3) to procure in this way an economic gain for oneself or another person or causing a disadvantage for another person. The offender is to be prosecuted only with the consent of the aggrieved party and is to be sentenced to imprisonment up to six months or to a penalty up to 360 day-fines.

2. Data and system interference

a. Object – protection of system/hardware/data?

Does your criminal law define "computer and/or electronic data"? Does this definition include programs or software or similar coding? If you have a definition, please provide it and the reference to the related paragraphs/articles of your code.

In the Austrian Criminal Code **data** is defined as personal and non-personal data as well as computer programs (Art. 74 para. 2 StGB).[5] A **computer system** is defined as single as well as combined devices which serve automation-aided data-processing (Art. 74 para. 1 subpara. 8 StGB).

b. Act – destruction/alteration/rendering inaccessible?

i. Does your penal law penalize the unauthorized erasure, alteration, rendering inaccessible, acquiring or other similar interference with information or data from a computer or electronic system or program?

Art. 126a StGB criminalizes **damaging of data**. The actus reus is causing damage to another person by altering, erasing or otherwise rendering useless or suppressing automation-aided processed, transmitted or entrusted data without right. The perpetrator is to be sentenced to imprisonment up to six months or to a penalty up to 360 day-fines. Higher sentences apply if the damage of data exceeds EUR 3,000 or EUR 50,000 respectively or if the crime was committed as member of a criminal organisation.

ii. Does your penal law penalize the unauthorized interception of the transmission in any manner or mode of computer or electronic data and/or information?

According to **Art. 119a StGB**, it is a criminal offense to make use of technical means which were attached to the computer system or otherwise prepared to receive information or to intercept the electromagnetic radiation of a computer system (**unlawful interception of data**). Similar to the mens rea of Art. 118a StGB (unlawful access to a computer system), Art. 119a StGB requires the intent to (1) unlawfully obtain information on data which is transmitted by a computer system, and to (2) make it available to another person for whom it is not destined by using it or making it public, and to (3) procure in this way an economic gain for himself or another person or causing a disadvantage for

[4] Cf. *infra*, answer to question (C)(a)2.b.i.

[5] In other codes, the term data may be used differently, e.g. the DSG only protects personal data. Thus, Art. 51 DSG solely criminalizes the illegal use of personal data.

another person. The offender is to be prosecuted only with the consent of the aggrieved party and is to be sentenced to imprisonment up to six months or to pay a fine up to 360 day-fines.

Art. 119a StGB is overridden by the more specific **Art. 119 StGB** which penalizes the **infringement of the secrecy of telecommunications**, i.e. making use of technical means which were attached to the telecommunication device or the computer system or otherwise prepared to receive information. Art. 119 StGB entails the intent to unlawfully obtain information on messages transmitted through a telecommunication or a computer system. Just as Art. 119a StGB, the offender according to Art. 119 StGB is to be prosecuted only with the consent of the aggrieved party and is to be sentenced to imprisonment up to six months or to pay a fine up to 360 day-fines.

3. Data Forgery

a. Object – authenticity?

Does your penal law define as a criminal offense the unauthorized input, alteration, deletion or suppression of computer or electronic data resulting in inauthentic data in order to protect the authenticity of the data to be used or acted upon for legal purposes? If you have a definition, please provide it along with the reference to the related paragraphs/articles of your code and/or special statutes.

b. Act – alteration/deletion?

Does your penal law penalize as a criminal offense the unauthorized input, alteration, deletion or suppression of computer or electronic data/information resulting in inauthentic data/information with the intent that it be considered or acted upon for legal purposes as if it were authentic? If yes, please provide the reference to the applicable paragraphs/articles of your code.

Pursuant to **Art. 225a StGB**, it is a criminal offense to **produce false data** by input, alteration, erasure or suppression of data or to **falsify authentic data** with the intent for using it legally as evidence of a right, legal relationship or fact. This law was enacted in 2002 in order to protect the reliance on the authenticity of electronic documents to be used or acted upon for legal purposes. The maximum sentence for this offense is one year of imprisonment. A person shall not be punished under Art. 225a if he/she voluntarily – before the false or falsified data is used as evidence of a right, legal relationship or fact – destroys the data or otherwise prevents the danger of its use. If there is no danger of such a use or if it has been removed without action of the offender, he/she shall not be punished in case he/she, unaware of that fact, voluntarily and seriously makes an effort to remove the danger (§ 226 StGB).

Moreover, **Art. 148a StGB** criminalizes the **fraudulent misuse of data processing**, i.e. causing economic damage to another's property by influencing the result of automation-aided data processing through arrangement of the program, input, alteration or erasure of data or through other interference with the course of data processing. This crime requires the intent to unlawfully enrich oneself or a third person. A person who committed this crime is to be sentenced to imprisonment up to six months or to a penalty up to 360 day-fines.

Art. 108 TKG penalizes operators and all persons who are involved in the operator's activities who falsify, incorrectly relate, modify, suppress or incorrectly convey a **communication** or withhold it from the intended recipient without authorisation. Perpetrators are to be sentenced to imprisonment up to three months or to a penalty up to of up to 180 day-fines unless the offence carries a more severe penalty under another regulation.

4. Misuse of Devices

a. Object – type of device?

Does your criminal law criminalize the development of a hacker's "tool kit" or any part of it for the unauthorized access to computer or electronic systems or transmissions?

b. Act – public distribution/transfer to another person?

i. Does your criminal law penalize the unauthorized use of any of the hacker's tools listed above under a?

ii. Does your criminal law penalize the public distribution and/or transfer to other parties of hacked electronic information?

c. Possession?

Does your criminal law criminalize the possession of a hacker's "tool kit" or any part of it for the unauthorized access to computer or electronic systems or transmissions?

Art. 126c StGB penalizes the **misuse of computer programs or access data**, i.e. the production, import, distribution, sale, otherwise making accessible, procurement or possession of,

1. a computer program or a comparable equipment which – in view of its particular nature – has obviously been created or adapted to commit any of the following crimes:
   a. unlawful access to a computer system (Art. 118a),
   b. infringement of the secrecy of telecommunications (Art. 119),
   c. unlawful interception of data (Art. 119a),
   d. damaging of data (Art. 126a),
   e. interference with the functioning of a computer system (Art. 126b), or
   f. fraudulent misuse of data processing (Art. 148a),

or

2. a computer password, an access code or comparable data allowing the access to a computer system or a part of it,

with the **intent** that it will be used for the commitment of any criminal offence mentioned above. The offender is to be sentenced to imprisonment up to six months or to penalty up to 360 day-fines.

A person shall not be punished under Art. 126c if he/she voluntarily prevents that the computer program or comparable equipment, the pass word, the access code or the comparable data will be used in a way mentioned in Arts. 118a, 119, 119a, 126a, 126b or 148a. If there is no danger of such a use or if it has been removed without action of the offender, he/she shall not be punished in case he/she, unaware of that fact, voluntarily and seriously makes an effort to remove the danger.

The unauthorized **use** of a hacker's "tool kit" as such is not explicitly criminalized as the use will always imply the possession with the intent that it will be used for the commitment of a criminal offence mentioned above. However, once the computer program, computer password or alike is used to commit such a criminal offence, the perpertator is punishable according to the respective offence (either for the commission or for the attempt). Hence, Art. 126c StGB is a preparatory offence.

Art. 126c StGB is overridden by the more specific regulation **Art. 10 ZuKG**. This rule penalizes **professional interference with the right to conditional access services**. The actus reus is the selling, renting, leasing,

production and import – for commercial purposes – of devices and procedures designed or specially adapted to facilitate unauthorised access to protected services such as, e.g., pay-TV or password-secured internet services against payment. Furthermore, the purchase or possession of such devices with the intent to market them or to use them with the help of others to access protected services is criminalized. Perpetrators are to be sentenced to imprisonment up to two years or to penalty up to 360 day-fines. The main difference to Art. 126c StGB is the prerequisite of a commercial purpose.

(b) Privacy

1. Violation of Secrecy of Private Data

a. Object – type of private data?

i. Do your country's laws require that data collectors disclose their information practices before collecting private information from consumers like, for example, which information is used, how it is collected and for what purpose, whether it is shared with others and whether consumers have any control over the disclosure of their private data?

There is no general law requiring data collectors to disclose their information practices before collecting private information from consumers. Both the Federal Act on the Protection of Personal Data (DSG) and the respective provisions of the Austrian Telecommunications Act 2003 (TKG) refer only to personal data.

ii. Do your country's laws require companies and entities doing business on the internet to inform consumers of the identity of who is collecting the data, if the provision of the requested data is voluntary or required and the steps taken by the data collector to ensure the confidentiality, the integrity and the quality of the data?

*iii. Do your country's laws require websites to display a privacy policy and explain how **personal** information will be used before consumers enter the purchase process or any other transaction for which they must provide sensitive information?*

The Austrian E-Commerce Act (**ECG**) requires a service provider (i.e. a natural or legal person or other institution with legal capacity which provides an information society service such as, e.g., online marketing of goods and services or online information offers) to **inform consumers**, *inter alia*,

- of its identity including the geographic address at which the service provider is established and contact details;
- if the activity is subject to administrative supervision, the supervisory authority competent for the service provider; and
- if the service provider is subject to trade or professional rules, the chamber, professional association or similar institution to which the service provider belongs, the professional title and the Member State where the title has been granted, as well as a reference to the applicable trade and professional rules and the means to access them (**Art. 5** para. 1).

According to **Art. 96 para. 3 TKG**, providers of public communication services and providers of information society services according to the ECG are obliged to inform the subscriber or user of the **personal data** it will collect, process and transmit, on which legal basis and for which purposes this will take place and for how long the data will remain stored. Collection of these data is only permissible if the subscriber or user consented. This does not apply to technical storage or access if the sole purpose is to perform the transmission of a communication via a communications network or, if it is absolutely necessary for the provider of an information society service who was explicitly requested by the sub-scriber or user to provide its service. The subscriber has to be informed of the usage

possibilities based on search functions embedded in electronic versions of the directories. This information has to be given in an appropriate form, in particular within the framework of general terms and conditions and, at the latest, upon commencement of the legal relations. This does not affect the right to information pursuant to the DSG.[6]

iv. Does the criminal law of your country penalize failing to provide the disclosures mentioned above (a.i; a.ii and a.iii)?

No. Failure to inform subscribers according to Art. 96 para. 3 TKG is an administrative offense; the offender is to be punished with a fine of up to Euro 37,000 (Art. 109 para. 3 subpara. 16. TKG).

b. Act – illegal use and transfer/distribution?

*i. Does the criminal law of your country define the illegal transfer and distribution of **private data**?*

ii. Does the criminal law of your country penalize the illegal use, transfer and/or distribution of private data?

No, **Art. 51 DSG** only penalizes the use, making available to others and publishing of data relating to persons who are identified or identifiable (i.e. **personal data**)[7].

Data, both private and personal, are protected by the criminal laws regarding professional confidentiality of specific professions such as doctors and lawyers (see below) or of public officials[8] and the offenses mentioned above, in particular Art. 119a StGB (unlawful interception of data), Art. 119 StGB (infringement of the secrecy of telecommunications) and Art. 118a StGB (unlawful access to a computer system). Furthermore, regulations concerning business secrecy (Art. 122 StGB et seq.) and misuse of wiretaps and sound recorders (Art. 120 StGB) are significant.

c. Justification?

*i. Under which conditions does your country's law allow for the authorized collection, processing, transfer and distribution of **private data**?*

ii. What standard of need is required for an authorized collection and/or distribution (compelling, important, reasonable, convenient)?

-

[6] According to **Art. 26 para. 1 DSG**, a controller has to **provide** any person or group of persons who request so with **information** about the (personal) data being processed concerning that person or group of persons. The information has to contain the processed data, the information about their origin, the recipients or categories of recipients of transmissions, the purpose of the use of data as well as its legal basis in intelligible form. Upon request of a data subject, the names and addresses of processors shall be disclosed in case they are tasked with processing data relating to the person concerned. If no data of the person requesting information exist it is sufficient to disclose this fact (negative information). With the consent of the person requesting information, instead of in writing the information may be provided orally alongside with the possibility to inspect and make duplicates or photocopies.

[7] Cf. answer to question (C)(b)2.c., *infra.*

[8] Cf. in particular **Art. 310 StGB** (**violation of official secrecy**).

2. Violation of professional confidentiality

*a. Object – type of **private data**?*

i. Do your country's laws require that professionals disclose:

*- Their information collection and management practices before collecting **personal** information from their patients or clients;*

- Their disclosure practices;

- Their professional ethical obligations;

*- And whether patients or clients have any control over the disclosure of their **personal** data?*

Doctors and other medical staff, psychologists, psychotherapists, lawyers, solicitors, authorized experts and staff of banks are subject to the professional duty of confidentiality.[9] They are not, however, obliged to disclose their professional ethical obligations towards patients and clients without being asked.

With regard to data relating to persons who are identified or identifiable (i.e. personal data), the controller[10] of a data application has to **inform the data subject** when collecting data in an appropriate manner about (**Art. 24 DSG**)

- the **purpose** of the data application for which the data are collected, and
- the name and address of the controller,

insofar as this as this information is not already available to the data subject with regard to the particular circumstances of the case. **Further information** has to be given if this is necessary for a fair and lawful processing, in particular if

- the data subject has a right to object to the intended processing or transmission of data pursuant to Art. 28 (the premises are that the use of data is not authorised by law and an overriding interest in secrecy deserving protection is infringed),
- it is not clear for the data subject whether he/she is required by law to reply to the questions posed, or
- the data are to be processed in a joint information system that is not authorised by law.

This duty to provide information does not apply with regard to only indirectly personal data (i.e. the data relate to the subject in such a manner that the controller, processor or recipient of a transmission cannot establish the identity of the data subject by legal means) (Art. 24 para. 4 DSG).

If the controller learns that data from his data application are systematically and seriously misused and the data subject may suffer damages, he/she is obliged to immediately inform the data subject in an appropriate manner.

---

[9] Art. 54 Act on the Medical Profession ("Ärztegesetz", in the following "ÄrzteG"); Art. 14 Act on the Psychologists' Profession ("Psychologengesetz", in the following "PG"); Art. 15 Act on Psychotherapy ("Psychotherapiegesetz", in the following "PthG"); Art. 9 Attorneys' Code ("Rechtsanwaltsordnung", in the following "RAO"), Art. 37 Act on the Notarial Profession ("Notariatsordnung", in the following "NO"), Art. 121 StGB and Art. 38 Austrian Banking Act „Bankwesengesetz", in the following „BWG").

[10] "**Controller**" is defined as natural or legal person, group of persons or organ of a territorial corporate body that decides (alone or jointly with others) to use data, without regard whether it uses the data itself or involves a service provider for this purpose (Art. 4 fig. 4 DSG).

Such obligation does not exist if the information would require an inappropriate effort in light of a minor damage to the data subjects and the costs of informing all persons concerned (Art. 24 para. 2a DSG).

Generally, before commencing a data application every controller of **data relating to persons who are identified or identifiable** has to file a **notification with the Data Protection Commission** for the purpose of registration in the Data Processing Register (Art. 17 DSG). Such duty of notification also applies to manual filing systems if they involve sensitive data.[11] Data applications which are not subject to notification include, *inter alia*, those which contain only indirectly personal data or correspond to a standard application[12] and those for the purpose of preventing and prosecuting of crimes (Art. 17 paras. 2 and 3 DSG).

Apart from the right to raise an objection with the controller of the data application against the use of data (Art. 28 DSG) mentioned above, data subjects are further entitled to the right to information about the data being processed (Art. 26 DSG) and the right to rectification and erasure of data that are incorrect or have been processed contrary to the provisions of the DSG (Art. 27 DSG). Yet, beyond Art. 24 DSG there are no obligations that data subjects have to be informed about these rights.

ii. Which data are specifically protected, if any?

"**Sensitive data**" are specifically protected, i.e. data relating to natural persons concerning their racial or ethnic origin, political opinion, trade-union membership, religious or philosophical beliefs and data concerning health or sex life (**Art. 4 subpara. 2 DSG**). Such data may only be transmitted if the interests in secrecy of the data subject deserving protection are not infringed by the purpose and content of the transmission (Art. 7 para. 2 subpara. 3 DSG).

Art. 9 para. 1 DSG offers an exclusive list of circumstances in which the use of sensitive data does not infringe interests in secrecy deserving protection. The enumeration includes the following:

- The person concerned has obviously made the data public himself/herself (subpara. 1);
- The data are used only in indirectly personal form (subpara. 2);
- The obligation or authorisation to use the data is stipulated by law and serves an important public interest (subpara. 3);
- The use is necessary for the establishment, exercise or defence of legal claims of the controller before a public authority and the data were collected legitimately (subpara. 9); or
- The data are required for the purposes of preventive medicine, medical diagnosis, **health care** and treatment or the management of health-care services and the use of data is performed by medical personnel or other persons subject to an equivalent duty of secrecy (subpara. 12).

iii. Does your country's penal law allow or even require clinicians, lawyers, priests, etc. to breach the confidentiality in certain situations or for certain reasons established by law? Under which standards would that be done? (e.g. reasonable cause to believe that there is abuse vs. seeing an abused child, women, elderly)?

There are no such regulations in the Austrian penal law. However, they can partly be found in those laws which determine the respective duty of confidentiality. On this note, a **doctor** is required to **immediately report** to a law

[11] A definition of sensitive data in provided in the answer to question (C)(b)2.a.ii, *infra.*

[12] Nevertheless, controllers of a standard application have to inform anyone on request which standard applications they actually carry out (Art. 23 para. 1 DSG).

enforcement agency if he/she in the course of practising his/her profession comes to suspect that the death or serious bodily harm of a person was caused by a criminal offense. The same applies if the doctor suspects that an adult who is not capable of representing his/her own interests or a minor[13] was maltreated, tortured, neglected or sexually abused. In the case of minors the doctor is additionally obliged to immediately report to the youth welfare agency. If the doctor believes that the offense against the minor was committed by a close relative, the report to the law enforcement agencies may be omitted as long as is necessary for the welfare of the minor provided the collaboration of the youth welfare agency and where applicable the involvement of a medical child protection institution (**Art. 54 ÄrzteG**).

The obligation to maintain **banking secrecy** does not apply vis-à-vis the Public Prosecutor and criminal courts in connection with criminal court proceedings on the basis of a court approval and vis-à-vis the fiscal authorities in connection with initiated criminal proceedings due to wilful fiscal offences, except in the case of financial misdemeanours (**Art. 38 para. 2 subpara. 1 BWG**). Moreover, a **credit** or **financial institution** which suspects or has reasonable grounds to suspect that a banking transaction or the assets component originates from specific criminal activities or is related to a criminal or terrorist organisation, a terrorist crime or terrorist financing is obliged to **immediately report** this to the Financial Intelligence Unit and to refrain from any further execution of the transaction until the matter is resolved (**Art. 41 para. 1 BWG**).

Lawyers are obliged to breach their professional confidentiality and file a report to the Financial Intelligence Unit Prevention only if their client – noticeable to the lawyer – obviously seeks his/her legal advice in order to launder money or finance terrorism (**Art. 8c para. 1 RAO**).

Furthermore, doctors and lawyers are not bound by professional confidentiality if they are litigating for their own cause, e.g. concerning their claims for fees, or in order to defend themselves in a criminal case or against claims for alleged damages. However, this confinement is restricted to information inevitable necessary (Austrian Supreme Court, legal rules RS0127872 and RS0127872).

b. Subject – Type of perpetrators?

*Does the **criminal law** of your country identify the categories of professionals who are bound by specific confidentiality rules?*

Leaving the duty of confidentiality of officials (Art. 310 StGB) out of account, the Austrian material penal law only identifies two categories of professionals who are bound by specific confidentiality rules. According to **Art. 121 para. 1 StGB** it is a criminal offense for **professionals in the health sector** which are regulated by law, persons who professionally fulfil tasks regarding the administration of a hospital or other health service provider or tasks in the health, accident, life or social insurance sector to disclose or to use data concerning the health status of a person. The second group of professionals Art. 121 StGB applies to are **experts** appointed by a court or another authority for a particular process (**para. 3**). Both categories include assistants and trainees (para. 4). The data has to be confided or accessible to the professionals' exclusively because of his/her profession. The disclosure or use has to be able to infringe legitimate rights of the person concerned. The offender is to be prosecuted only on request of the aggrieved party (para. 6).

[13] According to Austrian law, a minor is a person under 18 years of age.

Art. 157 para. 1 Austrian Code of Criminal Procedure ("Strafprozessordnung", in the following "StPO") enumerates groups of persons which may **refuse to give evidence**, thus respecting categories of professionals who are bound by specific confidentiality rules, these include:

- **defence counsels**, attorneys-at-law, patent agents, notaries public and chartered accountants with regard to matters that have come to their attention in their respective capacities (subpara. 2),
- specialists in **psychiatry**, psycho-therapists, psychologists, probation officers, registered mediators and staff members of recognized institutions for psycho-social counselling and care with regard to the matters that have come to their attention in their respective capacities (subpara. 3),
- media proprietors (publishers), media staff members and staff members of a media company or media service with regard to questions that relate to the person of the author, the supplier of or informant for programs/articles and records or that relate to communications that they received with a view to their activities (subpara. 4).

The right of these groups of persons to refuse to give evidence must not be evaded, especially not by seizing or confiscating documents or information saved on data carriers or by examining auxiliary staff or trainees. Otherwise, the information is null and void (para. 2).

c. Act – illegal use and transfer/distribution?

Which acts (e.g. illegal collection, use, transfer and distribution) are specifically penalized by your country's criminal law?

As mentioned, **Art. 121 StGB** criminalizes the **disclosure** and **use** of data by professionals in the health sector and alike as well as by appointed experts. Moreover, **unlawfully requesting** a person to disclose data on his/her health is penalized. This offense requires the intention of harming or endangering the earning or career advancement of the person concerned or any other person in the event of refusal (Art. 121 para. 1a StGB).

Art. 51 DSG penalizes the **use** of personal data, **making such data available to others** or **publishing** such data despite the data subject's interest in secrecy deserving protection. Contrary to Art. 121 StGB, Art. 51 DSG is not restricted to specific groups of professionals. However, it is necessary that the data have been entrusted or made accessible to the offender solely for professional reasons or that the offender has acquired the data illegally. The offense presupposes the conditional intention to unlawfully enrich oneself or a third person or the unconditional intent to harm someone in his fundamental right to data protection. The offender is to be sentenced to imprisonment up to one year, unless the offence is subject to a more severe punishment pursuant to another provision.

The practical significance of Art. 121 StGB and Art. 51 DSG is low as there are very few convictions pursuant to these offenses.

3. Illegal processing of personal and private data

a. Object?

Does your criminal law penalize the illegal and unauthorized acquisition, processing, storage, analysis, manipulation, use, sale, transfer etc. of personal and private data?

b. Subject?

Does your criminal law identify specifically the categories of persons and entities included in this criminal prohibition and sanctions?

c. Act?

i. Does your criminal law penalize specific acts that constitute all or part of the illegal processing of personal and private data? *Reply for each category listed below citing the relevant law and its provisions, if available:*

1. Illegal collection

2. Illegal use

3. Illegal retention

4. Illegal transfer

Art. 51 DSG – see answer to question (C)(b)2.c, *supra*.

Insofar as the act does not realise the legal elements of a criminal offence, it can constitute an **administrative offence** (**Art. 52 DSG**), such as:

- intentionally and illegally gaining access to a data application or maintaining an obviously illegal means of access;
- intentionally transmitting data in violation of the rules on confidentiality;
- using or failing to grant information, to rectify or to erase data in violation of a final judicial decision or ruling.

The offender is to be punished with a fine of up to Euro 25,000.

ii. Does it make a difference if these personal and private data are used, transferred etc. for police or law enforcement purposes?

Yes. According to **Art. 8 para. 4 DSG**, the use of personal **data concerning** acts and omissions punishable by the courts or administrative authorities, and in particular concerning **alleged criminal offences**, as well as data concerning criminal convictions and preventive measures does **not infringe interests in secrecy deserving protection** if

1. there exists an explicit legal obligation or authorisation to use the data exists; or
2. the use of such data is an essential requirement for a controller of the public sector to exercise a function assigned by law;
3. the legitimacy of the data application otherwise follows from statutory responsibilities or other legitimate interests of the controller that override the data subjects' interests in secrecy deserving protection and the manner of use of the data safeguards the interests of the data subject according to the DSG; or
4. the data is transmitted for the purpose of filing charges with an institution which is in charge of prosecution of a reported criminal act (or criminal omission).

Likewise regarding **data recorded by video surveillance**, interests for secrecy deserving protection of data subjects concerned are not infringed if such data are transmitted

1. to the competent authority or court and the controller has reasonable cause to believe that the data could document a criminal act which has to be prosecuted ex officio; or
2. to police authorities so they can carry out their competency pursuant to the Police Act (SPG),

even if the action or attack is not directed against the object or the person surveyed. The rights of authorities and courts to enforce the submission of documented evidence and to secure means of evidence and the corresponding obligations of the controller remain unaffected (**Art. 50a para. 6 DSG**).

d. Justification?

i. Under which conditions does your country's law allow for the authorized collection, processing, transfer and distribution of personal and private data?

ii. What standard of need is required for an authorized collection and/or distribution of personal and private data (compelling, important, reasonable, convenient)?

According to **Art. 6 para. 1 DSG**, personal data shall only

1. be used fairly and lawfully;
2. be collected for **specific, explicit and legitimate purposes** and not further processed in a way incompatible with those purposes;
3. be used insofar as they are **essential** for the purpose of the data application and are not excessive in relation to the purpose;
4. be used so that the results are factually correct with regard to the purpose of the application, and the data must be kept up to date when necessary;
5. be kept in a form which permits identification of data subjects (i.e. the persons concerned) as long as this is necessary for the purpose for which the data were collected.

Personal data shall be **processed** only insofar as the purpose and content of the data application are covered by the statutory competencies or the legitimate authority of the respective controller and the data subjects' interest in secrecy deserving protection is not infringed (**Art. 7 para. 1 DSG**).

According to **Art. 7 para. 2 DSG**, personal data shall only be **transmitted** if

1. they originate from a legal data application according to para. 1,
2. the recipient has satisfactorily demonstrated to the transmitting party his statutory competence or legitimate authority with regard to the purpose of the transmission, insofar as it is not beyond doubt, and
3. the interests in secrecy of the data subject deserving protection are not infringed by the purpose and content of the transmission.

The legitimacy of a use of data requires that the interference with the right to data protection be carried out only to the extent required, using the least intrusive of all effective methods and that the principles of Art. 6 DSG be respected (**principle of proportionality**, **Art. 7 para. 3 DSG**).

4. Identity theft

a. Object

i. Does your criminal law penalize identify theft?

ii. Does your criminal law proscribe specific forms of identity theft, like phishing, for example?

b. Subject

Does your criminal law contain penal responsibility connected to a person's digital personality, or to his/her Avatar, or to his/her digital role in an internet based simulation game (e.g. Cityville, Farmville, etc.)?

No.

(c) Protection Against Illegal Content: ICT Related

1. Object

a. Child pornography - images of real or virtual children?

i. Does your penal law criminalize the use of the internet for the purpose of storing, accessing, and disseminating child pornography? If so, please, cite the relevant law.

Art. 207a StGB penalizes producing, offering, providing, ceding, presenting or otherwise making available to another person, procuring or possessing a **pornographic depiction of a minor**. The **use of the internet** is **no requirement**. Its para. 3a, however, specifically criminalizes knowingly accessing a pornographic depiction of a minor using the internet.

Moreover, **Art. 215a para. 2a** criminalizes knowingly viewing a **pornographic** (live) **performance** which involves a minor. This includes performances which are made accessible through a computer system.

ii. In particular, does your criminal law:

- *Create a new offense that targets criminals who use the Internet to lure and exploit children for sexual purposes? Make it a crime:*
    - *1. to transmit,*
    - *2. make available,*
    - *3. export*
    - *4. and intentionally access child pornography on the Internet;*

As stated above, Art. 207a StGB (pornographic depictions of minors) and Art. 215a StGB (promotion of prostitution and pornographic performances involving minors) are general crimes and are not restricted to the use of internet. They were, however, adapted recently to comply with international instruments.[14]

- *Allow judges to order the deletion of child pornography posted on computer systems in your country;*
- *Allow a judge to order the forfeiture of any materials or equipment used in the commission of a child pornography offense;*

If this seems necessary to counter the commission of unlawful acts, a judge can order the **forfeiture** of objects ("Einziehung") which the perpetrator used or intended to use for committing an unlawful act or has acquired as a result thereof. Usually the decision on the forfeiture is included in the verdict (Art. 443 StPO).

However, the forfeiture of an object may also be ordered if no person in particular can be prosecuted or convicted (Art. 26 para. 3 StGB). In this case the Public Prosecutor files an independent motion for the forfeiture of the object (Art. 445 StPO). If the object is not worth more than EUR 1,000 or if the possession of the object is forbidden (such as pornographic depictions of minors), the district court decides on this independent application after hearing the Public Prosecutor and anyone concerned regarding the forfeiture of the object. If such a person's domicile is outside Austria or if the person cannot be determined without exceptional effort, the court can refrain from hearing him/her

[14] The last amendment of Art. 207a StGB came into force on 1 June 2009, the last amendment of Art. 215a StGB on 1 January 2012.

(Art. 445a StPO). If forfeited objects cannot be used meaningfully or commercialised as in the case of child pornography, they have to be **destroyed or deleted** (Art. 408 para. 2 StPO).

Moreover, objects whose possession is generally forbidden may be seized by the criminal police at their own discretion (Art. 110 para. 3 StPO). The criminal police have to report to the Public Prosecutor immediately about such a seizure. Thereupon, the Public Prosecutor has to apply to the court immediately for the confiscation or order the repeal of the seizure of the object if the requirements do not prevail or have lapsed (Art. 113 StPO). The court shall decide immediately on a confiscation (Art. 115 para. 2 StPO).

- *Criminalize:*
    1. *Knowingly accessing child pornography on the internet*

Yes, Art. 207a para. 3a StGB criminalises **knowingly accessing a pornographic depiction of a minor** using the internet. The punishment depends on the age of the minor. If the minor is over 14 years of age, the perpetrator will be sentenced to up to one year imprisonment; if the minor is under 14 years of age and this circumstance is covered by the perpetrator's intent, he/she will be sentenced to up to two years' imprisonment.

2. *Transmitting child pornography on the internet*

All forms of **making** a pornographic depiction of a minor **available to another person**, including offering, procuring, ceding and presenting it, are punishable under Art. 207a para. 1 StGB. Irrelevant whether the internet is used therefor or not, the perpetrator will be sentenced to up to three years' imprisonment.

3. *Exporting child pornography on the internet*

Anyone who produces, imports, transports or **exports** a pornographic depiction of a minor for the **purpose of dissemination** will be sentenced to six months' to five years' imprisonment. This offence is not a specific cybercrime. If the offence is committed by a member of a criminal organisation, the perpetrator will be sentenced to 1-10 years' imprisonment (Art. 207a para. 2 StGB).

4. *Possessing child pornography on the internet for the purpose of, e.g., transmitting, exporting it…?*

Procuring and **possessing** a pornographic depiction of a minor is punishable under Art. 207a para. 3 StGB, irrespective of the use of the internet. While the act has to be committed with conditional intent, a specific purpose is not required. Possessing a pornographic depiction means having sufficient control to give him/her the power of disposition. Thus, downloading child pornography from the internet meets the requirement of possession. Alike the offense of knowingly accessing child pornography (para. 3a, see above), the perpetrator will be sentenced to up to one year imprisonment if the minor is over 14 years of age; if the minor is under 14 years of age and this circumstance is covered by the perpetrator's intent, he/she will be sentenced to up to two years' imprisonment.

A person in possession of a pornographic depiction of a minor over 14 years of age shall **not be punished** (Art. 207a para. 5 StGB), if

- the depiction is possessed with the minor's consent and for minor's own private use or
- it is a pictorial representation which "only" creates the impression of being a realistic depiction of a sexual act and this representation is possessed for the person's own private use, provided there is no risk of dissemination of the depiction.

Under these circumstances decriminalisation likewise applies to the production of a pornographic depiction of a minor over 14 years of age.

iii. Does your criminal law penalize the online solicitation of children for sexual purposes via social networking websites and chat rooms?

Art. 208a StGB penalizes proposing or arranging **a meeting with a minor** below the age of 14 years for the purpose of committing a sexual offense by means of telecommunication and computer systems as well as by any other means deceiving the child about the intention of the contact. The proposal has to be followed by material acts leading to such a meeting. This Article came into force on 1 January 2012. The maximum sentence for this offense is two years' imprisonment. A person shall not be punished under Art. 208a if he/she voluntarily – before an authority has found out about the unlawful act – quits his/her undertaking and discloses his culpability to an authority.

With a view to complying with Art. 6 para. 2 Directive No. 2011/92/EU of the European Parliament and of the Council, Austria will amend Art. 208a StGB in 2013.[15] Hence, the attempt of contacting minors below the age of 14 years by means of information and communication technology for the purpose of possessing or obtaining access to child pornography will also be criminalized.

iv. Is the definition of child pornography in your criminal code close to that contained in international instruments (e.g. EU Directives)?

Yes, Art. 207a StGB has been amended in order to comply with the international instruments. By criminalizing various acts, Austria intends to prohibit all forms of the production and dissemination of pornographic depictions of minors. Furthermore, possessing and accessing child pornography are adequately penalized. In accordance with the international guidelines, minors are all persons under 18 years of age.

Pornographic depictions of minors are defined as (Art. 207a para. 4 StGB):

1. realistic depictions of a sexual act performed on a minor under 14 years of age or by such a minor on him-/herself, on another person or with an animal,
2. realistic depictions of a scene with a minor under 14 years of age which creates the impression that it involves a sexual act performed on such minor or by the minor on him-/herself, on another person or with an animal,
3. realistic depictions of a sexual act within the meaning of subpara. 1 or of a scene within the meaning of subpara. 2, though with minors over 14 years of age, or of the genitals or pubic region of minors, provided such depictions are distorted in a sensational manner, focus on the genitals or pubic region or are devoid of other manifestations of life in order sexually to arouse the observer,
4. pictorial representations – following alteration of a depiction or without use of such alteration – which create the impression that they are a depiction within the meaning of subparas. 1-3.

v. Is secondary victimization avoided for victims of child pornography in your penal law? In States where prostitution or the appearance in pornography is punishable under national criminal law, it should be possible not to prosecute or impose penalties under those laws where the child concerned has committed those acts as a result of being victim of

[15] Sexualstrafrechtsänderungsgesetz 2013.

sexual exploitation or where the child was compelled to participate in child pornography. Is this what your criminal law contemplates?

Adult prostitution and the appearance in pornography of adults are not punishable under Austrian criminal law.

In order to avoid re-traumatization of persons, in particular of children, who have been injured in their sexual sphere the Criminal Procedure Code provides specific regulations. Noteworthy is the so-called **adversarial interrogation** ("kontradiktorische Vernehmung") pursuant to **Art. 165 StPO**. A witness who has not yet reached the age of fourteen and might have been injured in his/her sexual sphere has to be interrogated by an expert in the pre-trial phase. The accused's and his/her representative's opportunity to take part in the interrogation is restricted to such an extent that they can follow the interrogation and exercise their right to ask questions by using technical equipment for audio and video transmission, without being present during the interrogation. Care is taken that there is no encounter between the minor and the accused as well as other parties to the proceedings. The adversarial interrogation is recorded; there is no further interrogation of the victim in the trial phase. Also certain other witnesses may be examined in this manner if they or the Public Prosecutor apply for it.

vi. Does your criminal law criminalize "virtual child" pornography? "Virtual child" pornography does not use real children or images of real identifiable children. When the image is not that of a real child, but a combination of millions of computer pixels crafted by an artist, can the government in your country ban this allegedly victimless creation? Please cite the applicable law and/or court decisions.

Yes, the definition of pornographic depictions of minors includes pictorial representations – following alteration of a realistic depiction or without use of such alteration – which create the impression that they are a realistic depiction of a sexual act or of the genitals or pubic region of minors, provided such depictions are distorted in a sensational manner (Art. 207a para. 4 subpara. 4 StGB). Thus, "**virtual child" pornography**, i.e. depictions which were produced entirely artificially (by using a computer) or by altering real depictions,[16] are criminalized. On the other hand, pictorial representations which do not create the impression that they are realistic depictions – such as drawings and paintings – are not penalized.[17]

vii. Mens rea: To be liable, the person should both intend to enter a site where child pornography is available and know that such images can be found there. Penalties should not be applied to persons inadvertently accessing sites containing child pornography. Are these the requirements of your criminal law?

Accessing a pornographic depiction of a minor using the internet (Art. 207a para. 3a) is only criminalised if the perpetrator does this **knowingly** (Art. 5 para. 3 StGB), i.e. he/she is certain about accessing a pornographic depiction of a minor. Hence, it is not enough that he/she thinks that he/she might be accessing a pornographic depiction of a minor and accepts this (dolus eventualis). The mens rea can be derived from the factual circumstances, e.g. repeated access or if a fee is charged for the access.

No penalties apply to person who inadvertently access sites containing child pornography. Moreover, the access is not punishable if it serves legal professionalism such as criminal prosecution, academic research or earnest journalism.

---

[16] *Bertel/Schwaighofer*, Österreichisches Strafrecht – Besonderer Teil II, 9th ed., § 207a marginal no. 7.
[17] *Kienapfel/Schmoller*, Strafrecht – Besonderer Teil III, 2nd ed., § 207a marginal no. 13.

b. Any other object where criminalization depends on the use of Information & Communication Technologies (ICT)

Does your criminal law penalize the following conducts? Please cite the relevant law.

1. *creation and use of true anonymity sending and/or receiving material on the ICT?*

No.

2. *cyber-bullying?*

No.

3. *cyber-stalking?*

No. In 2006 the crime "**insistent persecution**" was incorporated into the Austria Criminal Code (**Art. 107a StGB**). It criminalizes insistent persecution of another person against his/her will for a longer period of time in a way that impairs the person in his/her way of living in an intolerable way. However, the criminalization does not depend on the use of ICT.

4. *cyber-grooming?*

Art. 208a StGB penalizes proposing or arranging a meeting with a minor below the age of 14 years for the purpose of committing a sexual offense by means of **telecommunication** and **computer systems** as well as by any **other means deceiving the child** about the intention of the contact.[18]

2. Act - creation/accession/possession/transfer/public distribution by ICT (give examples)

Cite specific laws that criminalize the creation (even if never used), the accession, the possession (even if only in private), the transfer, and the public distribution through the internet and other electronic means of materials beside those already mentioned above, specifically because of internet/electronic technology use.

There are no such laws in Austria at the time being.

Other ICT-related crimes include "instruction on committing a terrorist crime" (Art. 278f StGB), "incitement to and approval of a crime" (Arts. 282 and 282a StGB) and "incitement of the people" (Art. 283 StGB). Furthermore, certain laws of the **National Socialism Prohibition Act** ("Verbotsgesetz", in the following "VerbotsG") are considered to be ICT-related. Art. 3h VerbotsG criminalizes publicly denying, grossly trivializing, approving or justifying the National Socialists' crimes against humanity. Art. 3d VerbotsG penalizes publicly instigating, inciting or seeking to induce prohibited conduct, in particular re-establishing the NSDAP or participating in such an organisation. However, these criminal offenses do not require the use of the internet or other electronic means.

(d) ICT Related Violations of Property, Including Intellectual Property

Does your criminal law specifically proscribe and penalize the following conducts perpetrated through the use of the ICT?

Please, cite the relevant law.

1. *Fraud*

Art. 148a StGB penalizes the **fraudulent misuse of data processing.** Cf. answer to question (C)(a)3.a., *supra.*

[18] Cf. answer to question (C)(c)a.iii., *supra.*

2. Infringement of Intellectual Property IP rights

In order to implement the Directive 2001/29/EC,[19] Austrian amended the **Copyright Act** ("Urheberrechtsgesetz", in the following "UrhG") in 2003. In light of new technical means of exploitation three new Articles were introduced: "protection of technical measures" (Art. 90c UrhG), "protection of computer programs" (Art. 90b UrhG) and "protection of labelling" (Art. 90d UrhG). The wording of these provisions is very similar to the text of the Directive.

Art. 90c UrhG protects the owner of a copyright who uses **effective technical measures** to avoid or to restrict a violation of his/her right. "Effective technical measures" are defined as all technologies, devices and components that – in the normal course of their operation – are designed to prevent or limit breaches of a right of exclusion and which ensure achieving this protection objective. In order to comply with these requirements, the use of a protected work or other subject-matter has to be controlled by the rightholder through the application of an access control or protection process, such as encryption, scrambling or other transformation of the work or other subject-matter or a copy control mechanism, which achieves the protection objective.

Art. 90b UrhG protects the owner of an **exclusive right to a computer program** who uses technical mechanisms to prevent an infringement of his/her right if tools are issued or held for commercial purposes with the sole purpose of facilitating the unauthorized removal of the technical measures. Art. **90d UrhG** refers to the removal or change of **labelling** (rights-management information) and the distribution, import for distribution or use for an emission, public reproduction or public provision of copies of works of which the labelling was removed or changed without authority. Such rights-management information includes electronic marks, even if they are encrypted by numbers or otherwise.

These three provisions together with a list of various other infringements (Art. 86 para. 1 UrhG) constitute the catalogue of (criminal) **copyright infringements** (**Art. 91 para. 1 UrhG**). The offender is to be sentenced to imprisonment up to six months or to a penalty up to 360 day-fines and to imprisonment up to two years if the criminal offense if committed commercially. A person shall not be punished if he/she merely copied or recorded a speech or a performance without authorization for his/her own personal use or if free of charge upon order of a third party for this person's personal use. The offender is to be prosecuted only on request of the aggrieved party (para. 3).

3. *Industrial espionage*

No, industrial espionage (Arts. 123 and 124 StGB) is a general criminal offense. There is no specific offense regarding the use of ICT.

(e) Criminalization of Acts Committed in the Virtual World

Does your criminal law penalize the commission of crimes committed in the virtual world like, for example, virtual child pornography, virtual violence, virtual graffiti, cyber-defamation, sexual harassment, harassment at work, without any involvement of real persons, only virtual representation? Please cite the relevant law and provide details.

No.

[19] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society.

(f) Non-Compliance Offenses

Does you criminal law penalize non cooperation with law enforcement agencies in the field of cybercrime? Duties to cooperate can be duties to retain and store information, to produce/deliver information as required by a production order, to give access to cyber systems to install filters or devices, etc. Is the breach of the duty to cooperate also enforced through administrative sanctions? Cite the relevant law and provide details.

Since 1 April 2012 providers of public communications services are obliged to store specific data of the subscriber's use of the communication services from the time of generation or processing until six months after the communication is terminated. The data shall be stored solely for the purpose of investigating, identifying and prosecuting criminal acts of a certain severity (**data retention**, **Art. 102a TKG**). Furthermore, with a view to the fundamental right to data protection, owners of radio systems and telecommunications terminal equipment are required to **take appropriate and reasonable measures to rule out abuse** of the communications equipment (**Art. 78 para. 2 TKG**).[20]

Similarly, all organisational units of a controller or processor which use data have to take **measures to ensure data security**. Depending on the kind of data as well as the extent and purpose of the use and considering the state of technical possibilities and economic justifiability, the data must be protected against accidental or intentional destruction, loss and unauthorised access and their proper use has to be ensured (**Art. 14 DSG**).

According to **Art. 138 para. 2 StPO**, operators of public communications services and other service providers are **obliged to provide** information about data of a message transmission and **retained data** and to cooperate in the surveillance of messages to investigative authorities. Such an obligation and a possible instruction to keep the activities confidential have to be ordered by the Public Prosecutor following authorisation by the court. Moreover, providers of communication services are obliged to **provide master data and access data** of subscribers to the competent court, Public Prosecutor or the criminal investigation department if they request such data in order to investigate a suspect (**Art. 76a StPO**; **Art. 90 para. 7 TKG**; Art. 53 para. 3a Security Police Act ("Sicherheitspolizeigesetz", "SPG")).

Non-compliance with these obligations is **not penalized by the Austrian criminal law**. However, **administrative sanctions** apply partially. Any person who contrary to Art. 90 TKG fails to provide master data or contrary to Art. 102a TKG fails to retain (or delete) data commits an administrative offence and shall be punished with a fine of up to Euro 37,000 (**Art. 109** para. 3 subparas. 13, 22 and 23 **TKG**). Failure to take the appropriate measures to rule out abuse of radio systems or telecommunications terminal equipment in accordance with Art. 78 para. 2 TKG is punishable with an administrative penalty of up to Euro 4,000 (Art. 109 para. 1 subpara. 6 TKG). Anyone who grossly neglects the required data security measures according to Art. 14 DSG is sanctioned with a fine of up to 10,000 Euro (**Art. 52** para. 2 subpara. 5 **DSG**).

[20] Service providers who only provide access to communications services are not considered to be owners.