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

Poland*

Małgorzata SKÓRZEWSKA-AMBERG*

(A) Introduction

Oryginał

Na początku XXI wieku faktem stało się społeczeństwo informacyjne, definiowane jako społeczeństwo wysoko rozwinięte, w którym zapewniono pełen dostęp do usług i informacji przy użyciu technologii ICT, umożliwiających pozyskiwanie, przetwarzanie, przechowywanie i rozpowszechnianie informacji dźwiękowych, wizualnych, tekstowych i numerycznych za pomocą sieci teleinformatycznych.

At the beginning of the 21st century the information society - defined as a highly developed society in which full access to services and information is ensured through ICT technology[1], enabling the acquisition, processing, storage and dissemination of audio, visual, textual, and numeric information through computer networks – became a reality. Space of communication with the aid of such networks is defined as a virtual space (cyberspace)[2].

Cyberspace is defined in Polish law as a space of processing and exchange of information created by information and communication systems along with the links between them and the relations with their users (Article 2 (1b) of the Act dated 29 August 2002 on Martial Law and Powers of the Commander-in-Chief of the Armed Forces and his Subordination to the Constitutional Authorities of the Republic of Poland, Dz.U.[3] no. 156, item 1301 with later amendments). Information and communication system[4] is specified by the Law dated 17 February 2005 on Computerisation of Entities Performing Public Tasks (Dz.U. No. 64, item 565 with later amendments), as a cooperating set of hardware and software for processing[5] of data in telecommunication networks[6]. Similarly, the Data Protection Act

---

* 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.

* Ph.D (law), MSc IT, Assistant Professor at Kozminski University. Warsaw

1 Cf. Bangeman's Report http://ec.europa.eu/archives/ISPO/infosoc/backg/bangeman.html (15.04.2012);
Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations, *OJ L 204, 21/07/1998 s. 0037 - 0048;* amended by Directive 98/48/EC of the European Parliament and of the Council of 20 July 1998 amending Directive 98/34/EC laying down a procedure for the provision of information in the field of technical standards and regulations, *OJ L 217, 05/08/1998 s. 0018 – 0026*

2 See Tim Maurer, *Cyber Norm Emergence at the United Nations – an Analysis of the Acivities at the UN Regarding Cyber-Security* [w] Science, Technology, and Public Policy Program Explorations in Cyber International Relations Project, Discussion Paper #211-11 Explorations in Cyber International Relations Discussion Paper Series, Harvard Kennedy School, Belfer Center for Science and International Affairs, September 2011

3 Journal of Laws of the Republic of Poland, abbreviated Dz.U.

4 Similarly the information and communication system is defined by article 2.(3) of the Electronic Services Act of 18 July 2002 (Dz. U. No 144 item 1204, with amendments)

5 Data processing also means storage, sending and receiving of data

dated 29 August 1997 (Dz.U. 2002 No. 101 item 926 as amended by 17.06.2002, with later amendments), defines in article 7.(2a) information system as a set of cooperating hardware, software, data processing procedures and programming tools used for data processing.

Freedom and security of the individual are basic rights protected by the criminal law with regard to virtual space. These rights are understood i.a. as the right to protection of privacy of the individual, the right of the individual to trust in information and communication systems, documents and data stored in such systems, freedom to decide and act on entitled rights as free and exclusive disposal of possessed information and freedom to decide on the scope and nature of data to be disclosed. Protection given by the criminal law concerns also safety of the credibility of trade and the authenticity of documents etc.Polish criminal law protects the integrity of and access to information stored and processed in ICT networks and the integrity and security of computer systems. The broad subjective right to dispose of the information[7] is also protected, in particular the constitutionally guaranteed right to privacy and secrecy of communication[8].

Criminal law protects also the property, defined by the civil law term as ownership and other property rights[9]. Actions taken in cyberspace are often targeted directly against property - spoofing (widely understood, including phishing) can be an example of such actions.

(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).

The provisions of criminal law governing the issues related to cybercrime are primarily contained in the Penal Code (e.g. article 165 § 1.(4), article 200a, art. 202 §§ 3-5, article 267-269b, article 286-287). The criminal provisions regarding infringements of this kind are also to be found in specific laws, including i.a. the Copyright Act dated 4 February 1994 (Dz.U. 2006 No. 90, item 631 as amended by 17.05.2006, with later amendments), the Industrial Property Act dated 30 June 2000 (Dz.U. 2003 No. 119 item 1117 as amended by 13.06.2003, with later amendments), the Combating Unfair Competition Act dated 16 April 1993 (Dz.U. 2003 No. 153, item 1503 as amended by 26.06.2003, with later amendments), the Telecommunications Act dated 16 July 2004 (Dz.U. No. 171 item 1800 with later amendments), the Data Protection Act dated 29 August 1997 (Dz.U. 2002 No. 101 item 926 as amended by 17.06.2002, with later amendments), the Electronic Services Act dated 18 July 2002 (Dz.U. No. 144 item 1204 with later amendments).

---

[6] The processing is carried out by terminal equipment proper for the type of network to be connected directly or indirectly to network endings (telecommunication terminal device, article 2.(43) of the Telecommunications Act of 16 July 2004 (Dz.U. No. 171 item 1800, with later amendments))

[7] See Włodzimierz Wróbel (in) Andrzej Zoll (ed.) *Kodeks karny. Część szególna. tom II, Komentarz do art. 117-277 k.k. [The Penal Code. Special Part. Commentary vol. II, Commentary to the articles 117-277 kk]*, Wolter Kluwers, Warszawa 2008 p. 1287

[8] Andrzej Marek, *Kodeks karny. Komentarz [The Penal Code. Commentary]*, Wolters Kluwer, Warszawa 2010, p. 570;
Joanna Piórkowska-Flieger (in) Tadeusz Bojarski (ed.) *Kodeks karny. Komentarz Kodeks karny. Komentarz [The Penal Code. Commentary]*, LexisNexis, Warszawa 2012, p. 701

[9] See Małgorzata Dąbrowska-Kardas, Piotr Kardas (in) Andrzej Zoll (ed.) *Kodeks karny. Część szególna. Komentarz, tom III, Komentarz do art. 278-363 k.k. [The Penal Code. Special Part. Commentary vol. III, Commentary to the articles 278-363 kk]*, Wolter Kluwers, Warszawa 2008, p. 25

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

In a *common law* system, precedents (*de jure*) constitute laws, in addition to laws constituted by statutes. In the Polish legal system, belonging to the *civil law*, it is only possible to talk about precedents *de facto*, i.e. judicial decisions that can affect the interpretation and application of the law after settling a precedent case. The courts' judicial decisions apply only to those categories of cases that under existing rules may be subject of the settlement before the Court.

(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.

The rules of criminal law relating to cyberspace contained in the Penal Code[10], introduced by the Law dated 6 June 1997 – Penal Code (Dz.U. No. 88 item 553), were subject to changes several times. The first significant amendment in this area was made by the Law dated 18 March 2004, amending the Penal code; the amendments of –the Code of Criminal Procedure and the Code of Offences (Dz.U. No. 69 item 626) extended the circle of prohibited offences related to child pornography (article 202 kk), specifying as an offence the presenting of pornographic content to a minor or making materials of such nature available to a minor, as well as dissemination of pornographic content allowing a minor to familiarise with such content (article 202 § 2 kk). It meant also a differentiation between the offence of producing, recording and importing in order to disseminate or dissemination or public presentation of pornographic content involving a minor (under the age of 18, article 202 § 3 kk) and the offence of recording, importing, storage and possession of pornography involving a minor under the age of 15. Article 202 § 5 kk provides also the possibility to forfeit tools or other items, designed or used for committing the offences described in 202 §§ 1-4 kk, even if the perpetrator was not the owner of such tools or items.

The amendment changed the wording of article 269 kk, making protection of informatics data of particular importance for national defence, communication security and functioning of state authorities, independent of the manner and place of the storage and processing of such data.

The amendment introduced new offences related to the protection of the integrity of data and systems. The legislator decided to penalise unauthorised infringement of the integrity of computer data and significant interference or preventing automated collection, processing or transmission of data (article 268a), to penalise significant interference with computer systems or telecommunication networks by infringement of the integrity of data stored, processed and transmitted through these networks (article 269a), as well as to penalise production or trading devices or software prepared to commit enumerated crimes[11](article 269b).

Further changes in the criminalisation of child pornography were introduced by the Law dated 27 July 2005, amending the Penal Code, the Code of Criminal Procedure and the Executive Penal Code (Dz.U. No. 163 item

---

[10] Abbreviated kk

[11] Including i.a. tapping, infringement of the integrity of or hindering the access to computer data, significant interference or hindering the ICT system

1363), changing the wording in the Penal Code, (art. 202 kk), identifying among enforcement actions provided in article 202 § 3 also storage and possession of pornographic content described by this provision and gives new wording to § 4, leaving only recording of pornographic content with the involvement of a minor under the age of 15, while the rest of the content of § 4 (without recording) is indicated as § 4a[12].

The goal of the next revision was to unify the terminology. The Law dated 4 September 2008 Changing the Laws in Order to Harmonise the IT Terminology (Dz.U. No. 171 item 1056) introduced the term "computer storage media", "electronic document", "information and communication system" and " means of electronic communication", mentioned in article 3.(1-4) of the Law dated 17 February 2005 on the Computerisation of Entities Performing Public Tasks (Dz.U. No. 64, item 565 with later amendments), to other laws, including the Penal Code.

The two most significant changes resulting from the Law dated 24 October 2008 Amending the Law - Penal Code and Some Other Laws (Dz.U. No. 214 item 1344) concern the introduction of punishment for generated child pornography and the change of scope of protection of the information in ICT systems. The amendment adds to article 202 kk the new § 4b, which penalises production, possession and trafficking in generated child pornography, defined as sexual content of created or processed image of a minor involved in sexual act. The second important change to come about is the change of the wording of article 267 kk, i.a., moving the protection from secured information to the access, to such information[13], while also introducing punishment for unauthorised access to a system.

The Law dated 5 November 2009, amending the Penal Code, the Code of Criminal Procedure, the Executive Penal Code, the Fiscal Penal Code and some other laws (Dz.U. No 206 item 1589), introduces penalisation of the usage of ICT systems or telecommunication networks in order to make contact with a minor under the age of 15 and bringing[14] to a meeting with the minor in question i.a. in order to produce or to record pornographic content (article 200a kk) and penalisation of public promotion of or support for paedophilic behaviour (article 200b

---

[12] Changes in article 202 kk seem inconsistent. Enforcement actions described in article 202 § 3 kk, including pornographic recording involving a minor under the age of 15 (the provision refers to a minor under the age of 18, so it comprises also a minor under age of 15) are at a lower penalty than recording of pornographic content with such a minor described in § 4, although § 3 concerns directional crime – made for dissemination, and furthermore – recording, which - if it is not a production at the same time – does not involve the participation of a minor, will be punished more severely than the production.

[13] Art. 267 protects unauthorised access to information. The penalty for such a breach of a computer system (§ 2) is on a par with opening of an enclosed letter, connecting to telecommunication network or breaking or omitting electronic, magnetic, software or other specific information security (§ 1), as well as an unauthorised installing, handling and tapping or any other visual, device, software or technology (§ 3). The provision in its previous wording, apart from the protection of communication secrecy also ensured the protection of messages against unauthorised access. Only the information was protected, hence in cases when access to a system was gained without visibly obtaining any information (e.g. the offender has obtained information in completely different network, another country and in a manner which does not necessarily link the loss of information in one system with an unauthorised entry in another system), the perpetrator could avoid the responsibility for his action. Doubts also arised whether activities such as bypassing security or taking advantage of software gaps is equivalent to protection breaking. The change made by the legislator moves the protection of information to the access to it, essentially changing the scope of protection, allowing prosecution of gaining access to information without entry into possession of its content.

[14] By means of deception of such a minor, exploiting his or her error or inability to properly understand the situation or using unlawful threat

kk).

The last amendment to the criminal law directly relating to offences committed in cyberspace was introduced in 2011. The Law dated 25 February 2011, amending the Penal Code (Dz.U. No. 72 item 381) introduced punishment for stalking[15] (article 190a § 1) and identity theft[16] (article 190 and § 2).

(C) The Specific Cybercrime Offenses

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

On the basis of the criminal law a perpetrator of cybercrime is generally liable of intentional misconduct. In most cases a specific intent is not required to meet the criteria defining it a criminal offence. However, the legislator introduces such intent for certain crimes, e.g. in case of:

- child pornography and pornography with violence or presenting animal - activity for the purpose of dissemination (article 202 § 3 kk),
- unauthorised data interception (i.e. installing or handling of tapping, visual or any other device, software or technology) - activity in order to obtain information in an unauthorised way (article 267 § 3 kk),
- theft of computer programme – activity with the purpose of financial gain (article 278 § 2 kk)
- computer fraud – activity with the purpose of financial gain or to cause harm to another person (article 287 § 1 kk).

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

In some cases the legislator introduces in this field liability also based on unintentional guilt.

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

In the Polish Penal Code the legislator allows liability based on unintentional guilt with regard to the offence of bringing danger to the life or health of numerous persons or the property of numerous persons or the property of considerable size by interfering with or preventing or in other ways affecting automatic processing, collecting or transmitting of computer data (article 165 § 2).

(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 ?

The Penal Code, in article 269a, penalises significant interference with the performance of computer systems or ICT networks, carried out through the action of an unauthorised person with regard to transmission, erasing, damaging, obstructing access to or changing of computer data.

---

[15] "who by persistent harassment of another person or a person's nearest raises in him or her a sense of danger motivated by the circumstances or cause significant infringement on that person's privacy

[16] "(...) who, pretending to be another person, uses his or her image or other personal information in order to cause property or personal damage to him or her (...)"

Articles 268a and 269 kk also introduces penalty for interference with a computer system, understood as a system of automatic processing, collecting or transmission of such data. Criminal law criminalises significant interfering with or preventing automatic processing, collecting or transmission of computer data (article 268a § 1 kk), as well as interfering with or preventing automatic processing, collecting or transmission of computer data of particular interest to national defence, security in communication, functioning of government administration, other governmental body or institution or local government (article 267 § 1 kk) and destruction of or damage to equipment for automatic processing, collecting or the transmission of computer data (article 267 § 2 kk).

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?

Polish Penal Code does not specify any method of violation of a computer system, penalising in article 267 different forms (with a rather large degree of generality) of such breach. An offence is:

- unauthorised access to information as a result of opening of an enclosed letter, connecting to telecommunication networks or breaking or omitting electronic, magnetic or other specific information security (article 267 § 1 kk),
- unauthorised access to whole or part of a computer system (article 267 § 2 kk)
- unauthorised installing, handling and tapping or any other visual, device, software or technology (article 267 § 3 kk).

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.

The object of protection provided by the Polish Penal Code refers primarily to computer data or information. In some cases the legislator uses the concept of computer programme, computer system and ICT network, computer storage media and document.

Article 115 § 14 kk defines document as any object or other written media, with which a specific right is related or which, due to its content, is a proof of such right, legal relationship or circumstances of legal significance.

An ICT network (information and communication system) is defined, as already mentioned, in the Law of 17 February 2005 on Computerisation of Entities Performing Public Tasks (Dz.U. No. 64, item 565 with later amendments), as a set of cooperating devices and software enabling processing of data in telecommunication networks. The same statute specifies computer storage media as a material or a device for recording, storing and reading data in digital form.

Polish law does not specify the meaning of the term computer data. In doctrine some opinions can be found referring to computer data as "any string of characters of functional importance in computer systems, responsible for carrying out specific operation within the system. Computer data can function as carriers of cultural information

(...) but can also have exclusively operational functions within the system"[17].

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?**

Penal Law criminalises unauthorised destruction, erasing, damaging or altering significant information or in other ways foiling or obstructing an authorised person's access to the content (art. 268 §§ 1-2 kk). Unauthorised destruction, modification, erasing, damaging or altering of computer data is also forbidden (art. 268a kk). Enhanced criminal liability is provided for destruction, erasing, damaging or altering information data of particular importance for national defence, communication security, functioning of governmental administration or other state organs or institutions, as well as local government, disturbing alternatively rendering impossible automatic processing and transmission of such information[18] (art. 269 § 1 kk).

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?**

Criminal law penalises unauthorised data interception regardless of how it was done. Polish Penal Code protects against unauthorised access to information, as well as unauthorised data interception. It is an offence to obtain without authorisation access[19] to secured information (art. 267 § 1 kk), computer systems (art. 267 § 2 kk) as well as carry out unauthorised installing and handling of any tapping device (including software) in order to access any information (also unprotected) without permission (article 267 § 3 kk).

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.

---

[17] Włodzimierz Wróbel (in) Andrzej Zoll (ed.) *Kodeks karny. Część szczególna. Komentarz, tom II, Komentarz do art. 117-277 k.k. [Penal Code. Special Part. Commentary vol. II, Commentary to articles 117-277 kk]*, Wolters Kluwer Polska, Warszawa 2008, p.1306

[18] Special criminal liability, under article 130 kk, concerns person who in order to transfer information to a foreign country's intelligence service - information which may harm the Republic of Poland if it becomes available to that country's intelligence service - enters a computer system in order to obtain such information.

[19] As a result of the opening of an enclosed letter, connecting to telecommunications network or breaking or omitting electronic, magnetic, software or other specific information security.

(Ad. a and b) Polish criminal law, in the chapter concerning provisions relating to the protection of information (Chapter XXXIII kk), penalises actions directed against information, including computer data. It is not possible to explicitly specify provisions criminalising unauthorised implementation, modification, deletion or suppression of computer or electronic data only to protect it against counterfeiting (ad a) or against using incomplete (spurious) data for legal purposes (ad. b). Computer data is protected i.a. against unauthorised destruction, removal, modification or hiding (articles 268 - 269 kk).

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 (e.g. password grabbers and key loggers, blue boxing programs, war-dialers, encryption software, program password crackers, security vulnerability scanners, packet sniffers etc.) for the unauthorized access to computer or electronic systems or transmissions?

The Penal Code, in article 269b, criminalises the production of equipment or computer programmes adapted to commit enumerated offences[20]. The provision "who manufactures, acquires, disposes of or shares with others any device or computer programmes designed for committing the offence specified in (...), as well as computer passwords, access codes or other data enabling access to information stored in a computer system or ICT network" is not entirely clear, because in its current wording, the reference of the term "produce" with regard to passwords, access codes or other data enabling access to digital data is not straightforward and obvious. It seems that production refers to both hardware and software used to commit certain offences and software in general (i.e. with respect to offences other than those specified in the provision), e.g. to generate passwords or

[20] • bringing danger to the life or health of numerous persons or property of considerable size, by interfering with, preventing or in other ways affecting automatic processing, collecting or transmitting of computer data - article 165 § 1.(4) kk;

- an unauthorised installing, handling and tapping or any other visual, device, software or technology in order to obtain information – article 267 § 3 kk;
- violation of integrity (destroying, damaging, erasure, altering) or hampering of access to computer data, as well as significant interfering with or preventing automatic processing, acquisition and transmission of such data- art. 268a § 1 kk (aggravation of the perpetrator's liability if the activities set out in article 268a § 1 kk result in substantial damage to property - article 268a § 2 kk);
- violation of the integrity or interfering with or preventing automatic processing of computer data of particular interest to national defence, security in communication, functioning of government administration, other state authorities, state-run institution body or local government authorities (article 269 § 1 kk);
- destruction or replacement of computer storage media, destruction or damage of a device for automatic processing, collecting or transmitting of computer data – in order to breach the integrity (destruction, erasing, damaging or altering) of computer data of particular interest to national defence, security in communication, the functioning of government administration, other state body or institution or local government or disrupt or disable automatic processing, storage or transmission of such data – article 269 § 2 kk;
- seriously disturbing the functioning of a computer system or an ICT network through unauthorised transmission, damage, destruction, erasure, deterioration, modification or hampering of the access to computer data - art. 269a kk;
- significant interfering with the work of computer through violation of the integrity of data being processed in the system (article 269a kk).

access codes (e.g. programmes to conduct brute-force attack in order to break any password of access), though in doctrine some opinions imply that "produces" applies only to tools serving to commit enumerated offences[21]. In this respect, the provision should therefore be defined more precisely. Also, in the literature the term "produces" are interpreted in an ambiguous way. Some authors[22] apply production only to cases where the hacking tools came about through the action of the perpetrators, while others[23] set the range of punishment much wider, including not only those who are to be seen as co-creators in the meaning of copyright law, but also to all who in any other way are involved in creating such tools, e.g. person providing financing for the offender. With such interpretation of the provision, it should be noted that the decisive element in this respect should always be the intention of persons involved.

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*?**

Liability for unauthorised access to information is regulated in article 267 kk. The access to information is protected, while the information is protected indirectly. Installing and handling of tapping, visual or any other device, software or technology in order to obtain information is penalised in § 3 of the same article.

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

Article 267 § 4 of the Penal Code introduces criminal liability for disclosure to another person of information fraudulently obtained, as described in article 267 §§ 1-3 kk, i.e. without authorisation:

- breaking or omitting electronic, magnetic, software or other specific information security (§ 1),
- obtaining access to the whole or a part of a computer system (§ 2),
- installing and handling of tapping, visual or any other device, software or technology (§ 3).

c. Possession?

Does your criminal law criminalize the possession of a hacker's "tool kit" or any part of it (e.g. password grabbers and key loggers, blue boxing programs, war-diallers, encryption software, program password crackers, security vulnerability scanners, packet sniffers etc.) for the unauthorized access to computer or electronic systems or transmissions?

Article 269b § 1 kk penalises manufacture, acquirement, disposal or sharing with others any devices or computer software adapted to commit enumerated offences[24]. Activities in connection to computer passwords, access

---

[21] Such interpretation is proposed i.a. by Włodzimierz Wróbel (in) Andrzej Zoll (ed.) *Kodeks karny. Część szczególna. Komentarz, tom II, Komentarz do art. 117-277 k.k. [Penal Code. Special Part. Commentary vol. II, Commentary to articles 117-277 k.k]*, Wolters Kluwer Polska, Warszawa 2008, p. 1317

[22] See Patrycja Kozłowska-Kalisz (in) Marek Mozgawa (ed.) *Kodeks karny. Komentarz [Penal Code. Commentary]*, Wolters Kluwer Polska 2012

[23] See Krzysztof Gienas, *Uwagi do przestępstwa stypizowanego w art. 269b Kodeksu karnego [Remarks to the offence specified in the article 269bof the Penal Code]*, Prokurator 1/2005

[24] • bringing danger to the life or health of numerous persons or the property of considerble size by interfering with, preventing or otherwise affecting automatic processing, collecting or transmitting computer data - article 165 § 1.(4) kk;

codes or other data enabling illicit access to information stored in a computer system or an ICT network are also penalised. Acquisition, as referred to by the article, is interpreted as gaining, coming into possession and using, i.e. any action by which the perpetrator gains access to such tools[25]. Disposal is to be understood as any contractual action (bilateral or multilateral) aiming at transfer of power over the tools in question[26]. Sharing means any action allowing or facilitating[27] the use of both hardware tools (e.g. equipment, media with software), as well as software tools (e.g. downloadable software) [28]. Sharing does not mean getting rid of the power over the tools in question. Different views regarding fulfillment of the constituent elements of a criminal offence by providing links to Web pages containing hacking tools, are to be found in doctrine and writing. Some authors take the view that "just informing other people how specific data or software can be acquired (e.g. by sharing the link to a spe-

---

- an unauthorised installing, handling of tapping, visual or any other device, software or technology in order to obtain information – article 267 § 3 kk;
- violation of integrity (destroying, damaging, erasure, altering) or hampering of access to computer data, as well as significant interfering with or preventing automatic processing, acquisition and transmission of such data- art. 268a § 1 kk (aggravation of the perpetrator's liability if the activities set out in article 268a § 1 kk result in substantial damage to property - article 268a § 2 kk);
- violation of the integrity or interfering with or preventing automatic processing of computer data of particular interest to national defence, security in communication, functioning of government administration, other state authorities, state-run institution body or local government authorities (article 269 § 1 kk);
- destruction or replacement of computer storage media, destruction or damage of a device for automatic processing, collecting or transmitting of computer data – in order to breach the integrity (destruction, erasing, damaging or altering) of computer data of particular interest to national defence, security in communication, the functioning of government administration, other state body or institution or local government or disrupt or disable automatic processing, storage or transmission of such data– article 269 § 2 kk;
- seriously disturbing the functioning of a computer system or an ICT network through unauthorised transmission, damage, destruction, erasure, deterioration, modification or hampering of the access to computer data - art. 269a kk;
- significant interfering with the work of a computer through violation of the integrity of data being processed in the system (article 269a kk).

[25] Cf. Włodzimierz Wróbel (in) Andrzej Zoll (ed.) *Kodeks karny. Część szczególna. tom II, Komentarz do art. 117-277 k.k. [Penal Code. Special Part. Commentary vol. II, Commentary to articles 117-277 kk]*, Wolters Kluwer Polska, Warszawa 2008, p. 1317; also Patrycja Kozłowska-Kalisz (in) Marek Mozgawa (ed.) *Kodeks karny. Komentarz. [Penal Code. Commentary].*, Wolters Kluwer Polska 2012

[26] Cf. Patrycja Kozłowska-Kalisz (in) Marek Mozgawa (ed.) *Kodeks karny. Komentarz. [Penal Code. Commentary]*, WoltersKluwer Polska 2012; Małgorzata Dąbrowska-Kardas, Piotr Kardas (in) Andrzej Zoll (ed.) *Kodeks karny. Część szczególna. Komentarz, tom III, Komentarz do art. 278-363 k.k. [Penal Code. Special Part. Commentary vol. III, Commentary to articles 278-363 kk]*, Wolters Kluwer Polska, Warszawa 2008, p. 418

[27] Cf. Dictionary of Polish Language

[28] Cf. Włodzimierz Wróbel (in) Andrzej Zoll (ed.) *Kodeks karny. Część szczególna. tom II, Komentarz do art. 117-277 k.k. [Penal Code. Special Part. Commentary. vol. II, Commentary to articles 117-277 kk]*, Wolters Kluwer Polska, Warszawa 2008, p. 1317; also Patrycja Kozłowska-Kalisz (in) Marek Mozgawa (ed.) *Kodeks karny. Komentarz. [Penal Code. Commentary].*, Wolters Kluwer Polska 2012

cific website) already constitutes a realisation of the constituent elements of the offence set out in article 269b"[29], others argue that sharing hacking tools is implemented i.a. through "the creation of links leading directly to such application, sharing hard drive resources containing such components by exchange of data using such applications as peer-to-peer"[30]. The second view seems to be more appropriate. "To share" in a dictionary meaning of the word means also to "to facilitate". Information about the place where something can be found is definitely facilitating in finding the object of interest, hence even sharing of links not leading directly to the hacking tools but only providing instructions how to construct such a tool or where to look for it, may fulfill the constituent features of an offence specified in article 269b kk.

The Penal Code, in article 269b, among the constituent elements of an offence does not mention possession. Taking into account that manufacture, acquisition or sharing concern obtaining power over an object, it can be presumed that also possession will be punished, although it does not seem to be the intention of the legislator. Possession, next to others, is repeatedly mentioned by the Penal Code - e.g. who "manufactures, processes, collects, possesses, uses" (article 171 § 1 kk), "manufactures, processes, transports, imports from abroad, exports abroad, collects, uses, stores, possesses, uses, removes, drops or leaves" (article 184 § 1 kk), "produces, records or imports, stores or possesses or disseminates or publicly presents " (article 202 § 3 kk), "produces, records or imports, acquires, stores, possesses, presents, carries or transmits" (article 256 § 2 kk). It seems therefore that the mere possession of hacking tools will not be penalised. The absence of a reference to ownership in article 269b kk is a gap difficult to explain.

The construction of the provision is inaccurate not only in this respect. Article 269b § 1 kk penalises i.a. the sharing with others of computer passwords, access codes or other data enabling illicit access to information stored in a computer system or an ICT network. The legislator's intention was to indicate the illicitness of action intended to breach the integrity of information. However, the lack of precise definition of what kind of information, stored in computer systems or networks should be protected, results in a provision that penalises any behaviour which leads to access to any information in ICT networks (e.g. links to Web pages). The simple addition to the provision content may completely change its application in practice – in accordance, moreover, with the likely intention of the legislator. Instead of "access to information stored on a computer system or an ICT network" should be therefore "access to secured information stored on a computer system or an ICT network".

(b) Privacy

1. Violation of Secrecy of Private Data

a. Object – type of private data?

(Note: private data are data that belong to people's private life but do not identify or make it possible to identify a person, e.g., civil status, sexual orientation, health status, buying habits or preferences)

Polish law uses the term *personal data*, both with regard to data for identification of a person (personal data), as well as data understood as private data belonging to the private life of a person, such as marital and health status

---

[29] Cf. Włodzimierz Wróbel (in) Andrzej Zoll (ed.) *Kodeks karny. Część szczególna. tom II, Komentarz do art. 117-277 k.k. [Penal Code. Special Part. Commentary vol. II, Commentary to articles 117-277 kk]*, Wolters Kluwer Polska, Warszawa 2008, p. 1317

[30] See Krzysztof Gienas, *Uwagi do przestępstwa stypizowanego w art. 269b Kodeksu karnego [Remarks to the Offence Specified in the Article 269b of the Penal Code]*, Prokurator 1/2005

etc. Article 6.(1) of the Data Protection Act dated 29 August 1997 (Dz.U. 2002 No. 101 item 926 as amended by 17.06.2002 with later amendments) defines personal data as any information relating to an identified or identifiable natural person ("data subject"). Therefore "personal data are any information relating to an identified or identifiable person, not only information used to identify a person"[31].

Data Protection Act repeatedly uses the term "data erasure" (e.g. article 2.(3), article 35.(1)), which means both the destruction of personal data and modification which will not allow identification of the data subject (anonymous data), i.e. "such procedures, which result in depriving the controller the possibility of any further processing of personal data"[32]. Anonymous data are no longer personal data.

Polish law regulations do not apply to anonymous data, i.e. data on individuals impossible to identify[33].

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?

Processing of data in accordance with article 23.(1) of the Data Protection Act is permitted i.a. if it is necessary for the performance of a contract in which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract.

The Data Protection Act, in the case of obtaining data directly from the data subject (article 24.(1)), requires, prior to the undertaking of data recording, the disclosure of the purpose of data collecting, data recipients or categories of data recipients known at the time of the provision of information as well as of the existence of the right of access to and right to correct data concerning the data recipient and if providing data is voluntary or obligatory (and any legal basis of such obligation). If data are collected from a third party, the Data Protection Act (article 5.(25)) requires, immediately following the data recording, that the data subject be informed of i.a. the purpose and the scope of data collection, data recipients or categories of data recipients, data source, any existence of right of access to and right to correct data concerning the data subject.

Personal data protection with respect to services provided by electronic means (including the Internet) is regulated by the Electronic Services Act dated 18 July 2002 (Dz.U. No. 144 item 1204 with later amendments).

In accordance with article 17 of the Act, personal data (as defined in the Data Protection Act) of a recipient of

---

[31] Cf. Janusz Barta, Paweł Fajgielski, Ryszard Markiewicz*, Ochrona danych osobowych. Komentarz [Personal Data Protection. Commentary]*, Wolters Kluwer Kraków 2007, p. 344

[32] Cf. Janusz Barta, Paweł Fajgielski, *Ryszard Markiewicz, Ochrona danych osobowych. Komentarz [Personal Data Protection. Commentary]*, Wolters Kluwer Kraków 2007, p. 374

[33] In accordance with article 26.(1) of Data Protection Act, processed data, having achieved the purpose of the processing, are no longer to be kept in a form which permits identification of the data subject. The Electronic Services Act in the article 19.(1) prohibits also the processing of data of the service recipient after the services have been provided by electronic means. After that moment, the service provider (as an exception) can only process the data indicated in article 19.(2) of the Electronic Services Act, including i.a. data necessary for settlement services and claims for payment for the use of the services, data necessary to clarify the circumstances of an unauthorised use of the service or data allowed for processing under separate laws or agreements.

the service can be processed by a service provider solely for the purpose and to the extent specified in the Electronic Services Act, i.e. any data identifying a party of the service, necessary for the execution of the service and processed for its implementation.

Providing personal data in dealings with an entrepreneur is voluntary, unless such data are necessary for the performance of an agreement (e.g. drawing up a telecommunication service agreement, lodging a complaint, drawing up a credit agreement).

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?

Article 5 of the Electronic Services Act obliges a service provider to render accessible in a clear, unambiguous, direct and permanent way (via an ICT system used by the recipient of the service) the service provider's electronic addresses and data[34]. The service provider is obliged to ensure that the recipient of the service have access to updated information about specific risks associated with the use of electronic services and the function and the purpose of the software or data which are not a component of the service content, entered by the service provider into the ICT system and used by the recipient of the service (article 6).

The provisions of Chapter 4 of the Electronic Services Act, concerning the principles of personal data protection in connection with the provision of electronic services, are *a lex specialis* with regard to the Data Protection Act, not applicable if the Electronic Services Act provides otherwise (article 16 of the Electronic Services Act).

The service provider processing personal data of a service recipient is obliged to ensure that the recipient of the service is given permanent and easy access[35] (article 20.(2)) to updated information about the possibility to use the electronic service anonymously or with a pseudonym, providing technical means to prevent unauthorised obtaining and modification of personal data transmitted by electronic means, as well as information about the entity entrusted with the processing of data, the scope of processing and intended date of transfer – if the service provider drew up an agreement to assign the data processing (article 20.(1)).

The service provider is obliged to ensure the functioning of the ICT system in use. The service provider is also obliged to enable the recipient of the service to use the electronic service gratuitously (in cases where

---

[34] e-mail, name, surname and place of residence or company name and head office address of the service provider, as well as any possible additional information:

1. if the service provider is an entrepreneur and the provision of services requires a permit – information on such permit and permitting authority (article 5.(3)),
2. if the service provider is a natural person with a right to practice depending on certain legal requirements – i.a a professional body or similar institution with which the service provider is registered; the professional title which he uses and the name of the country where it was granted; the name of the public registry and registration number as well as the name of the body conducting the registry; a reference to any applicable professional code of contuct and the means to access it; in the case of establishing of a representative, name and surname, place of residence and address or company name and address (article 5.(3)).

[35] Via ICT system used by the recipient of the service

the service properties require it), in a way that prevents unauthorised access to the content of the transfer being part of the service[36], suitable for the service properties, as well as unambiguous identification of the parties to the electronic services, together with confirmation of presented declaration of will and its content, necessary for the conclusion of an electronic contract for the provision of electronic services[37] (article 7.(1)). The termination of use of electronic services should be possible at any time (article 7.(2)).

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?

In accordance with article 8 of the Electronic Services Act, the service provider is obliged to define and make available free of charge the regulations of the provision of the electronic services. Such release must occur before the conclusion of an agreement on the provision of the electronic services, and the recipient of the service must be allowed (on-demand) acquisition, restoration and recording of the regulations through the ICT system used by the recipient of the service (article 8.(1)). The regulations specify types and scope of electronic services in particular, conditions of the provision of electronic services, non-delivery of illegal content by the recipient of the service, conditions of conclusion and termination of an agreement on the provision of electronic services as well as complaint procedures (article 8.(3)). The service recipient is not bound by regulation provisions which have not been made available to the service recipient in the described way (article 8.(2)).

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

Article 23 of the Electronic Services Act penalises non-disclosure by the service provider with regard to the recipient of the service in a clear, unambiguous and direct way and accessible through an ICT system or provide false or incomplete data concerning i.a. e-mails and service provider identification data[38] - data on the permit for the provision of electronic service and permitting authority (if such permit is required by legal provisions), data concerning service providers in cases these are natural persons and their right to practice if depending on additional requirements[39].

b. Act – illegal use and transfer/distribution?

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

The processing of any data relating to a specific (identified or identifiable) person is governed by provisions of the Data Protection Act and other laws, including the Electronic Services Act. The processing of anonymous

---

[36] In particular with the use of the cryptographic techniques

[37] In particular with the use of a qualified electronic signature

[38] Name, surname and place of residence or the company name and the head office address of the service provider

[39] Such service provider is obliged to disclose the following information: name, surname and place of residence or name or company name and address of the representative (if established), a professional body or similar institution with which the service provider is registered; professional title used and the name of the country where it was granted; name of public registry and registration number as well as name of the body conducting the registry; a reference to any applicable professional code of conduct and the means to access it.

data is not regulated by law.

Criminal law does not define the concept of illicit transfer and distribution of private data, criminalising unauthorised processing of data which, in accordance with statutory definition (article 7.(2) of the Data Protection Act) means any operations performed on data, including their transfer and distribution.

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

Criminal law penalises unauthorised processing of any information relating to an identified or identifiable natural person (article 49.(1) of the Data Protection Act), including their use, transfer and distribution.

The processing of anonymous data (impossible to bind with a specific person) is not regulated by law.

c. Justification?

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

The law regulates only the processing of data relating to a particular person. Under article 23.(1) of the Data Protecting Act, processing of such data is permitted under strict condition, of which the primary is the explicit consent of the data subject. The Act also allows the processing of data i.a. when it is necessary to execute a right or an obligation resulting from the provisions of the law or for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract.

In case the data is connected to the provision of the Electronic Services Act, in accordance with article 17 of the Electronic Services Act, any personal data (as defined in the Data Protection Act) of the service recipient can be processed by a service provider for the purpose and to the extent specified in the Electronic Services Act. The service provider may process: name and surname of the recipient of the service, personal number or, in its absence, number of passport, identity card or other identification document, permanent residence address, post address (if different than residence), electronic signature verification data and e-mails of the service recipient (article 18.(1)). Other data can also be processed, if required due to the kind of provided services or its settlement – in order to perform a contract or other legal action with the recipient of the service (article 18.(2)). However, the service provider must determine which of these data are indispensable for providing the electronic service (article 18.(3)). With the consent of the service recipient and for the purpose of advertising, market research and behaviour and preferences of the intended recipients' research, the results of these studies need to improve the quality of services provided by the service provider. The service provider may process such data based on the service recipient and which are not necessary for the provision of the electronic service in question (article 18.(4)).

The Act also allows the service provider to process operational data[40], including markings which identify the service recipient as well as markings indicating end of a telecommunication network or an ICT system used by the service recipient, information on the beginning, end and scope of every use of an electronic service (article 18.(5)).

---

[40] I.e. characterising a method of use of the electronic service by a service recipient

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

Personal data, i.e. any data about an identified or identifiable individual, including private data (defined as data belonging to the private life of a person e.g. marital status, health status, etc.), in accordance with article 1.(2) of the Data Protection Act**,** may be processed if of public interest, of interest to the data subject or of interest to third parties, to the extent and manner laid down by the statute.

The processing of personal data related to the provision of electronic services, and according to article 17 of the Electronic Services Act, is permitted solely for the purpose and extent specified in the Electronic Services Act and primarily affects the data necessary to execute the service and processed for the purpose of its implementation.

The standard of the requirements for lawful data processing can thus be specified as legitimate.

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?**

The Data Protection Act, in article 24.(1), requires, prior to the undertaking of data recording, the disclosure of the purpose of data collection, data recipients or categories of data recipients known at the time of the provision of information, as well as of the existence of the right of access to and right to correct data concerning the data recipient, if providing data is voluntary or obligatory (and any legal basis of such obligation). In accordance with article 23.(1) of the Data Protection Act, any person whose data are processed has the right to control the processing of his or her data and particularly to obtain information about methods of sharing data and information about data recipients. The controller, who breaks the duty to inform the data subject on his or her rights or to convey to the data subject information enabling the use of his or her statutory rights, is subject to criminal penalties (article 54 of the Data Protection Act).

If the service is provided by electronic means and if the service provider is a natural person with a right to practice depending on certain legal requirements (e.g. lawyer, physician), then the service provider is obliged to disclose i.a. the name of the professional body or similar institution with which the service provider is registered; professional title used and the state where it was granted; the name of the public registry and the public registration number, a reference to any applicable code of professional conduct and the means to access it.

ii. Which data are specifically protected, if any?

So-called sensitive data are particularly protected and defined in article 27.(1) of the Data Protection Act. This provision prohibits the processing of personal data revealing racial or ethnic origin, political opinions, religious

or philosophical beliefs, religious and political affiliation, trade-union membership, data on health status, genetic code, addictions or sex life and data relating to convictions, decisions on penalty and fine, as well as other data on decisions issued in court or administrative proceedings. The processing of such data is permitted only in cases specified in article 27.(2) of the Act[41].

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)?

Articles 179-183 of the Code of Criminal Procedure[42] (the Law dated 6 June 1997 – Code of Criminal Procedure, Dz.U. No 89 item 555 with later amendments) regulates questions of secrecy with regard to persons obliged to keep secrets. There is no exception in the law when it comes to the seal of confession. According to article 178.(2) kpk, a priest must not be cross-examined as to facts which he learned in confession. Similarly, a lawyer must not be questioned as to facts which were learned in connection to legal advice or when leading a case (article 178.(1) kpk). Lawyers required to keep professional secrets[43], tax advisors, physicians or journalists[44] may be heard with regard to facts covered by secrecy only if it is necessary for the interest of the system of justice and when the fact which is protected by secrecy can not be determined on the basis of other evidence (article 180 § 2 kpk, the Court decides in preparatory proceedings on hearing or to allow hearing as to facts covered by secrecy). Other persons bound to maintain confidentiality of information can be heard in connection to circumstances covered by the obligation only after being released from the obligation of secrecy by authorised superior body (article 179 kpk - information classified as "secret" or "top secret"), Court or Prosecutor (article 180 § 1 kpk - information classified as "reserved" or "confidential").

---

[41] I.a. if the data subject has given consent to the processing of those data in writing (unless it concerns the erasure of his or her data); special provisions of other laws allow the processing of such data without the consent of the data subject, providing full guarantees for their protection; processing is necessary to protect the vital interests of the data subject; data processing is necessary to perform the statutory tasks of the churches and other religious organisations and other entities operating with political, scientific, religious, philosophical or trade-union aims (the processing relates solely to the members of those entities or persons maintaining regular contact with them in connection with their activities and if full guarantees of protection of the processed data are provided); processing relates to data which are necessary for the assertion of rights before the court; the processing is carried out in order to protect the health, the provision of medical care or treatment of patients and if full guarantees of the protection of personal data are provided; the processing relates to data which are made public by the data subject.

[42] Abbreviated kpk

[43] Notaries, barristers, solicitors

[44] Releasing a journalist from the obligation of secrecy can not apply to the data allowing the identification of the author of the press release, letter to the editor or other naterial of such nature, as well as identification of persons providing published information or information submitted for publication – if they expressed reservation as to non-disclosure of such data (article 180 § 3 kpk). This rule is not applicable (article 180 § 4 kpk) if the information covered by secrecy relates to an offence specified in the article 240 § 1 kk, (the Penal Code requires a person having reliable information about a punishable preparation, attempt or achievement of any enumerated most serious criminal offences (including genocide, the production and use of means of mass destruction, coup d'état, espionage, manslaughter, threat to life or property of many people or terrorist crimes), to notify law enforcement authorities – failing to do so is punishable).

b. Subject – Type of perpetrators ?

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

Criminal law defines the categories of persons required to maintain specific rules of confidentiality. Unauthorised disclosure of state secrets (article 265 § 1 kk) as well as inadvertent disclosure of state secrets, to which the offender is familiar in connection with the performance of public function or received authorisation (article 265 § 2 kk), is penalised. Any person who, contrary to the law or undertaken obligation, discloses or uses information acquired in connection with his or her function, work, public activities, social, economic or scientific interest (article 266 § 1 kk) as well as in the capacity of a public servant, disclosing information classified as " reserved" or "confidential" or information obtained in connection with the performance of official duties, disclosure of which may jeopardise legally protected interest (article 266 § 2 kk) – also commits an offence. Criminal procedure indicates also categories of persons particularly obliged to maintain specific rules of confidentiality. These include persons mentioned in the provisions of the Code of Criminal Procedure concerning the hearing of people particularly obliged to secrecy, including lawyers, physicians, priests in the realm of the seal of confession, notaries, tax consultants (articles 178-180 kpk) as well as persons belonging to the category of bearers of state and professional secrets.

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?

Article 7.(2) of the Data Protection Act defines data processing as any operations[45] performed on personal data[46], including their collection, recording, storage, development, alteration, making available and erasure. The processing of personal data carried out without legal authorisation is not allowed, with the exception of entities referred to in article 3a.(1) of the Data Protection Act, i.e. natural persons processing data solely for personal or domestic purposes and entities established or resident in a third country, using technical means located on Polish territory and only for data transmission[47].

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?

Article 49.(1) of the Data Protection Act penalises unauthorised processing of personal data, i.e. all operations on

---

[45] Especially operations performed in computer systems

[46] Defined as any information relating to an identified or identifiable natural person (personal and private data understood as the data belonging to the private life of a person e.g., marital status, health status, etc.)

[47] Data Protection Act (with the exception of the provisions concerning the security of the data and their inspection by authorised bodies) does not apply to the release for journalistic and literary or artistic activities, unless the freedom to express the views and the dissemination of information significantly violates the rights and freedoms of the data subject (Article 3a.(2) of the Data Protection Act).

personal data where processing is not permitted[48] or executed by a person who is not authorised. Criminal liability is enhanced if the unauthorised processing relates to sensitive data[49] (article 49.(2) of the Act).

b. Subject?

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

Any person (natural or legal), which processes personal data in violation to the Data Protection Act and other specific laws, including the Electronic Services Act, comes under penal sanctions.

A controller or a person liable for the protection of personal data is penalised separately (article 51 of the Data Protection Act) if providing or allowing access to such data (also unintentionally) to the administrator or person responsible for the protection of such data. A controller who violates, even unintentionally, the duty to protect data from an unauthorised person, damage or destruction (article 52 of the Data Protection Act) or who violates the duty to inform the data subject on his or her rights or to convey to the data subject information enabling the use of his or her statutory rights (article 54 of the Data Protection Act), also comes under penal sanctions. Failing to register a personal data filing system (article 53 of the Data Protection Act) and thwarting or disrupting inspection of the regularity of processing and data security (article 54a of the Data Protection Act) is also criminalised.

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**

   Article 49.(1) of the Data Protection Act criminalises illegal processing of personal and private data, including their collection.

2. **Illegal use**

   Article 49.(1) of the Data Protection Act criminalises illegal processing of personal and private data, including their usage.

3. **Illegal retention**

   Article 49.(1) of the Data Protection Act criminalises illegal processing of personal and private data, including their retention.

4. **Illegal transfer**

   Article 49.(1) of the Data Protection Act criminalises illegal processing of personal and private data, including illegal transfer of such data.

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

---

[48] I.e. obtained contrary to the law

[49] I.e. data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, religious and political affiliation, trade-union membership, as well as data on health status, genetic code, addictions or sex life, data relating to convictions, decisions on penalty and fine.

enforcement purposes?

Article 7.(6) of the Data Protection Act defines a data recipient as every recipient to whom personal data are exposed, with the exception of state or local government authorities where data are made available in connection with legal proceedings. Therefore, a controller has no obligation to inform the person in question (and respectively the data subject is not entitled to obtain such information) of entities to whom data are disclosed if they do not belong to the category of recipients[50], and in particular not to inform about the transmission of a person's processed data to the law enforcement authorities in connection with an investigation.

If personal data are processed in connection with the provision of services by electronic means, article 18.(6) of the Electronic Services Act allows the service providers to inform, for investigation needs, state authorities (including law enforcement agencies) about processed personal data.

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?**

According to article 23.(1) of the Data Protection Act, processing of personal data is permitted if and only if:

1. the data subject has given his or her consent[51] (unless it concerns the erasure of his or her data),
2. it is necessary to execute a right or an obligation resulting from the provision of the law,
3. it is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract,
4. it is necessary for performing certain legal tasks carried out in public interest,
5. it is necessary to carry out legally justified purposes[52], pursued by controllers or data recipients and if processing does not affect any rights and freedoms of the data subject.

The Data Protection Act, in the case of obtaining data directly from the data subject (article 24.(1)), requires, prior to the undertaking of data recording, the disclosure of the purpose of data collection, data recipients or categories of data recipients known at the time of the provision of information, as well as the existence of the right of access to and the right to correct data concerning the data recipient, if providing data is voluntary or obligatory (and any legal basis of such obligation). In the case data are collected from a third party, the Data Protection Act (article 5.(25)) requires, immediately after data recording, that the data subject is informed of i.a. the purpose and the scope of the data collection, the data recipients or categories of data recipients, the data

---

[50] Cf. Janusz Barta, Paweł Fajgielski, *Ryszard Markiewicz, Ochrona danych osobowych. Komentarz [Personal Data Protection. Commentary]*, Wolters Kluwer Kraków 2007, p. 388

[51] Understood as a declaration of intent, which content constitutes consent to the processing of personal data of the person who made the statement; consent that can not be presumed or implied from the content of other statements of will and can be cancelled at any time (article 7.(5) of the Data Protection Act); if it is not possible to obtain the consent of the person whom the data concerns and their processing is necessary to protect the vital interests of that person, processing of such data is permitted until consent can be obtained (article 23.(3) of the Data Protection Act); consent may also include the processing of data in the future, if the purpose of the data processing is not changed (article 23.(2) of the Data Protection Act)

[52] In particular, direct marketing of the controller's own products or services, as well as pursuing claims from running business activity (article 23.(4) of the Data Protection Act)

source and the existence of the right of access to and the right to correct the data concerning the data recipient.

The data controller must provide the data subject, whose data are processed, with information enabling the data subject to be identified[53]. The Act provides for situations in which the controller is released from the obligation to disclose the aforementioned information to the data subject, in particular if the provisions of another law permits the processing of data without revealing the purpose of their collection (article 24.(2)), or provides, or allows the collection of personal data without the knowledge of the data subject (article 25.(2)) as well as in case this person has such information.

Article 27.(1) of the Data Protection Act prohibits the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, religious or political affiliation, trade-union membership, data on health status, genetic code, addictions or sex life and data relating to convictions, decisions on penalty and fine, as well as data on other decisions issued in court or administrative proceedings (so-called sensitive data). Processing of such data, however, is allowed in cases specified in the Act (article 27.(2)), in particular if the data subject has consented in writing to the processing of such data (unless it concerns the erasure of his or her data); special provisions of other laws allow the processing of such data without the consent of the data subject, providing full guarantees for their protection; processing is necessary to protect vital interests of the data subject; data processing is necessary to perform the statutory tasks of churches and other religious organisations and entities operating with political, scientific, religious, philosophical or trade-union aims (the processing relates solely to members of those entities or persons maintaining regular contact with them in connection with their activities and when full guarantees of protection of the processed data are provided); processing relates to data which are necessary for the assertion of rights before the court; the processing is carried out in order to protect health, the provision of medical care or treatment of patients and when full guarantees of the protection of personal data are provided; the processing relates to data which are made public by the data subject.

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

The processing of personal data, i.e. any data relating to an identified or identifiable individual, including private data (defined as data belonging to the private life of a person e.g., marital status, health status, etc.), in accordance with article 1.(2) of the Data Protection Act**,** may take place due to public interest, the interest of the data person, whom the data concerns or interest of third parties to the extent and manner laid down by the Data Protection Act.

The processing of personal data related to the provision of electronic services (services by electronic means), in accordance with article 17 of the Electronic Services Act, is permitted solely for the purpose and extent specified in the Electronic Services Act and is primarily related to the data necessary to perform the service and processed for its implementation.

The standard of need required for lawful data processing can be defined as legitimate.

---

[53] The full name of the controller and office address, and, in the case when the controller is a natural person - name and place of residence

4. Identity theft

(Note: identity theft occurs when someone appropriates another's personal information without his or her knowledge to commit theft or fraud. Identity theft is a vehicle for perpetrating fraud schemes. Typically, the victim is led to believe they are divulging sensitive personal information to a legitimate business or entity, sometimes as a response to an e-mail solicitation to update billing or membership information, or as an application for a fraudulent Internet job posting or loan.)

a. Object

***i.* Does your criminal law penalize identify theft? Please, cite the relevant law.**

***ii.* Does your criminal law proscribe specific forms of identity theft, like phishing, for example? Phishing is defined as a form of online identity theft that uses spoofed emails designed to lure recipients to fraudulent websites which attempt to trick them into divulging personal financial data such as credit card numbers, account usernames and passwords, social security numbers, etc.**

The Penal Code, in article 190a§ 2 criminalises behaviour of an offender, who, pretending to be another person, uses his or her image or other personal information in order to cause property or personal harm to that person.

The Penal Code provisions on fraud can also be used to protect an individual against cheating and various kind of spoofing. The legislator defines fraud as bringing (in order to obtain financial benefit) another person to an unfavourable disposition of one's own or someone else's property by misleading this person or making use of any mistake, as well as taking advantage of this person's inability to assess properly the actions taken (art. 286 § 1 kk). Computer fraud, specified in a separate provision, is described as unauthorised affecting automatic processing, storing or transferring of computer data, as well as modifying, deleting or entering computer data in order to obtain financial benefit or to cause harm to another person (art. 286 § 1 kk).

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.)? Please cite the relevant law.

Polish criminal law have no provisions directly related to actions against chatterbots or virtual profiles, although provisions concerning digital data integrity protection can be applied, as well as article 190a § 2 kk penalising impersonating another person – providing the perpetrator's aim is to cause personal or property harm to that person. (this provision may in some way refer to actions against the profiles of network users). Any action taken against a virtual personality of a real individual, causing harm to that person in the real world (e.g. stealing virtual currency in *Second Life* purchased with real money) can be punished on the basis of relevant provisions of the criminal law, e.g. fraud, theft, etc.

(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 dis-

seminating child pornography? If so, please, cite the relevant law.

Polish criminal law, in Chapter XXV "Crimes against sexual freedom and morality", criminalises i.a. possession, distribution and sharing of child pornography (article 202 §§ 3-4a kk). The Penal Code does not specify *expressis verbis* methods of storage, access and dissemination of child pornography. Such activities carried out with the help of and over the Internet are not separately regulated and are subject to criminal liability in general.

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;

  The criminal law introduces a new offence directly related to the use of ICT networks. Liable to penalty is the perpetrator who, in order to produce or to record pornographic content[54] through an ICT system[55], enters into communication with a minor under the age of 15 and by misleading this minor or making use of any mistake, or taking advantage of this minor's inability to assess properly any actions taken, as well as by unlawful threat - is bringing this minor to a meeting (article 200a § 1 kk). The offender, who, through an ICT system[56], proposes a minor under the age of 15 to participate in the production or recording of pornography[57], also bears criminal liability. The condition of criminalisation of such proposal is the perpetrator's implementation efforts (article 200a § 2 kk).

- **Allow judges to order the deletion of child pornography posted on computer systems in your country;**

  There is no provision in the Polish criminal law, which *expressis verbis* would allow a judge to order the removal of child pornography available in a computer system in Poland, although such action may be taken pursuant to the provisions which allows to forfeit the tools and items intended to commit an offence related to child pornography (article 202 § 5 kk).

- **Allow a judge to order the forfeiture of any materials or equipment used in the commission of a child pornography offense;**

  Article 202 § 5 provides for the possibility of forfeiture tools or other items which served or were intended to serve to commit offences related to child pornography[58], even if they did not constitute the perpetrator's

[54] As well as rape, sexual intercourse with a minor under the age of 15 as well as presenting a sexual act to a minor
[55] Or telecommunications network
[56] Or telecommunications network
[57] As well as sexual intercourse, or to submit or to perform and other sexual activity
[58] Defined in article 202 §§ 1-4b kk

property.

- **Criminalize:**

  1. Knowingly accessing child pornography on the Internet

  2. Transmitting child pornography on the Internet

  3. Exporting child pornography on the Internet

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

  Polish criminal law, in article 202 § 3 kk, prohibits the production, recording, storage, possession or importation, as well as public presentation of pornographic content involving a minor (under the age of 18) – when made in order to disseminate. Article 202 § 4 kk penalises the recording of pornographic content involving a minor under the age of 15. Importation, storage and possession of such content is prohibited in article 202 § 4a kk. Executive actions defined in article 202 § 4 concern only the recording, apart from producing pornography (i.e. the action stipulated in article 202 § 3 kk). The provision, in its present form, applies to recording, which, depending on an adopted definition can refer to the reproduction of media or taking steps to save specific content on the media[59]. Disregarding which definition is adopted and taking into account the wording of article 202 § 3 kk – where both recording and producing is mentioned - it seems appropriate to add in the future the word "producing" to article 202 § 4 kk. Article 202 § 3 applies to directional offence – in order to disseminate, § 4 and 4a concern a minor under the age of consent (15 in the Polish criminal law), thus production, importation, storage, recording or possession of pornographic content involving a minor over the age of 15 is not penalised if done not aiming at dissemination (e.g. for private purpose).

  There is in the Polish criminal law no provision for obtaining intentional access to child pornography (including accessing child pornography content on the Internet). Possession, interpreted in the Polish criminal law by referring to the civil definition of possession as the actual power over the object. However, the concept of possession in criminal law includes not only autonomous and dependent possession, but also wielding, i.e. exercising actual power over another person. Hence, commentary to the Penal Code interprets possession in relation to the content described above as physical disposition of such content even if it is during a short time[60]. Thus getting access to illicit content can be treated as possession of such content. From an evidential point of view it is argued i.a. that access to content in ICT networks, linked with saving temporary

---

[59] Cf. O.Górniok [in:] *Kodeks karny. Komentarz. Tom II [The Penal Code. Commentary. Vol. II]*, ed. O.Górniok, S.Hoc, M.Kalitowski, S.M.Przyjemski, Z.Sienkiewicz, J.Szumski, L.Tyszkiewicz, A.Wąsek, Gdańsk 2005, p. 214; M.Rodzynkiewicz [in:], *Kodeks karny. Cześć szczególna, tom II. Komentarz do art. 117-277 k.k. [The Penal Code. Special Part, Commentary vol. II. Commentary to articles 117-277 kk]*, ed. A.Zoll, Kraków 2006, p. 680; similarly J. Piórkowska-Flieger [in:] *Kodeks karny. Komentarz [The Penal Code. Commentary]*, ed. T.Bojarski, Warszawa 2012, p. 508; M.Bielski [in:], *Kodeks karny. Cześć szczególna, tom II. Komentarz do art. 117-277 k.k. [The Penal Code. Special Part, Commentary vol. II. Commentary to articles 117-277 kk]*, ed. A.Zoll, Warszawa 2008, p. 680;

[60] Cf. Marek Bielski (in:) Andrzej Zoll (ed.) Kodeks karny. Część szególna. Komentarz, tom II, Komentarz do art. 117-277 k.k. *[The Penal Code. Special Part. Commentary vol. II, Commentary to articles 117-277 kk]*, Wolter Kluwers, Warszawa 2008 p. 680-81

files on the media, can be regarded as possession[61].

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

Liable to penalty is the perpetrator who, in order to produce or to record pornographic content[62] through an ICT system[63], enters into communication with a minor under the age of 15 and by misleading this minor or making use of any mistake, or taking advantage of this minor's inability to properly assess any actions taken, as well as by unlawful threat - is bringing this minor to a meeting (article 200a § 1 kk). The offender, who, through an ICT system[64], proposes to the minor under the age of 15 to participate in the production or recording of pornography[65], bears also criminal liability. The condition of criminalisation of such proposal is the perpetrator's implementation efforts (article 200a § 2 kk).

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

The Polish Penal Code does not contain a definition of child pornography. The Code uses the term "pornography involving a minor". In doctrine, this term is defined as "any kind of pornographic content presenting a minor, therefore a person under the age of 18, involved in any kind of sexual activity "[66].

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

A child who is a victim of sexual abuse or has been forced to take part in child pornography will not be prosecuted or punished.

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.

The Polish Penal Code limits the responsibility for production, distribution, presentation, storage or possession of virtual (simulated) child pornography (article 202 § 4b kk) to the produced or processed image of a minor involved in sexual activity.

---

[61] Por. Arkadiusz Lach, *Pojęcie posiadania pornografii dziecięcej w art. 202 § 4a Kodeksu karnego w odniesieniu do danych informatycznych [The Concept of Possession of Child Pornography in Article 202§ 4a of the Penal Code in Regard to the Computer Data],* Ruch Prawniczy, Ekonomiczny i Socjologiczny 2010/1 str. 69

[62] As well as rape, sexual intercourse with a minor under the age of 15 as well as presenting a sexual act to such a minor

[63] Or telecommunications network

[64] Or telecommunications network

[65] As well as sexual intercourse, or to submit or to perform and other sexual activity

[66] Cf. Marek Bielski (in) Andrzej Zoll (red.) *Kodeks karny. Część szczególna. Komentarz, tom II, Komentarz do art. 117-277 k.k. [The Penal Code. Special Part, Commentary vol. II. Commentary to articles 117-277 kk]*, Wolter Kluwers, Warszawa 2008, p. 678

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?

Offences related to child pornography defined in the Penal Code are intentional crimes and require therefore an awareness of the perpetrator with regard to actions taken.

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?

Such activities are not regulated in the Polish criminal law.

2. cyber-bullying?

The Penal Code criminalises a number of behaviours that can be considered as cyber-bullying. Cyber-stalking must be mentioned in the first place (article 190a kk), but also criminal acts against bodily integrity and inviolability (defamation of natural and legal persons, organisations not having the status of legal person with regard to such acts or features, which could bring discredit in the face of public opinion or result in loss of confidence, necessary for a given position, occupation or kind of activity (defamation – article 212 kk), offending other persons using mass communication (article 216 § 2 kk), acts aiming at threats (as defined in article 115 § 12 kk) against other persons (e.g. sending threatening letters by electronic mail or publishing material of threatening character on network sites; illegal threats based on national and ethnic identity, race or with reference to religious denomination (or lack of), as well as public instigation of violence or illegal threats with reference on such basis, applies to penalty according to article 119 kk), as well as offences against integrity of information and ICT systems (articles 267-269b kk).

3. cyber-stalking?

The Penal Code criminalises behaviour of the offender who, by persistent harassment of another person or person's nearest, gives rise to a reasonable sense of danger or substantial violation of that person's privacy (article 190a § 1 kk) as well as the perpetrator who, by pretending to be another person, uses his or her image or other personal information in order to cause property or personal harm (article 190a § 2 kk).

4. cyber-grooming?

The already featured article 200a kk penalises i.a. cyber-bullying. Liable to penalty is the perpetrator who, in order to produce or to record pornographic content[67], through an ICT system[68] enters into the communication with a minor under the age of 15 and by misleading this minor or making use of any mistake, or taking advantage of this minor's inability to assess properly any actions taken as well as by unlawful threat - is bringing this minor to a meeting (article 200a § 1 kk). The offender, who, through an ICT system[69], proposes a minor

[67] As well as rape, sexual intercourse with a minor under the age of 15 as well as presenting a sexual act to such a minor

[68] Or telecommunications network

[69] Or telecommunications network

under the age of 15 to participate in the production or recording of pornography[70], bears also criminal liability. The condition of criminalisation of such proposal is the perpetrator's implementation efforts (article 200a § 2 kk).

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.

Global computer networks can be considered as a public place of speech. This is the reason why regulations in the Penal Code concerning violation of public order can apply to content appearing in public network forums (public promotion of fascism or any other form of totalitarian systems or public spreading of nationalistic, ethnic, racist or religious dissention – article 256 kk, as well as defamation based on national identity, ethnicity, racism, religious affiliation or lack of denomination – article 257 kk), criminal acts against freedom of conscience and religion (violation of religious feelings of other persons committed by offence towards religious cult objects – art 196 kk).

The Polish Penal Code punishes also public presentation of pornographic content, forced upon a person who may not wish it (art. 202 § 1 kk); presentation and making available content and objects of pornographic character to minors below the age of 15 and distributing content of such character in ways that would enable such minor to get access to it (art. 202 § 2 kk).

(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

The legislator defines fraud as bringing (in order to obtain financial benefit) another person to unfavourable disposition of one's own or someone else's property by misleading this person or making use of any mistake, as well as taking advantage of this person's inability to assess properly any actions taken (art. 286 § 1 kk). Computer fraud, specified in a separate provision, is described as unauthorised affecting automatic processing, storing or transferring of computer data, as well as modifying, deleting or entering computer data in order to obtain financial benefit or to cause harm to another person (art. 286 § 1 kk). Criminal liability for computer fraud is separated, because fraud committed with the use of devices for automatic processing, storing or transferring of computer data comprises no element of misleading another person by the offender or making use of his or her mistake. To exhaust the constituent elements of the offence, the fact of technological influence on data processing is essential. Activity of the offender who acts in order to obtain financial benefit or to cause damage to another person is not aimed directly at the wronged person[71].

---

[70] As well as sexual intercourse, or to submit or to perform and other sexual activity

[71] Bogusław Michalski (in): Kodeks karny. Część szczególna. Tom II. Komentarz pod redakcją Andrzeja Wąska [*Criminal Code. Specific section. Volume II. Commentary by Andrzej Wąsek*], C.H. Beck, Warszawa 2010, p. 1174

2. Infringement of Intellectual Property IP rights

Modern technology, particularly ICT, allows wide and direct access to content protected by copyright. Sharing of such materials in the cyberspace space can in many cases be treated as piracy. Therefore, the criminal code and special laws contain provisions in order to protect such rights.

The Penal Code criminalises unauthorised obtaining of someone else's computer programme in order to achieve financial benefit (278 § 2 kk), as well as fencing of a computer programme (article 293§ 1 kk).

The basic legal act that aims to protect copyright is the Copyright Act dated 4 February 1994 (Dz.U. 2006 No. 90, item 631 as amended by 17.05.2006, with later amendments). Chapter 14 of this statute contains a catalogue of regulations introducing criminal liability for violation of its provisions. The Copyright Act penalises i.a. appropriation or misrepresentation as to the authorship of the whole or any part of another person's work (article 115. (1)) and the distribution of someone else's work without providing the name of its creator (article 115.(2)), enhancing the liability if such operations are carried out in order to achieve financial benefit (article 115.(3)). Unauthorised distribution of someone else's work is also prohibited (article 116.(1), as is unintentional action - article 116.(4)), to record or to reproduce in order to record (article 117.(1)). The liability for such action is enhanced if the perpetrator works to gain assets (article 116.(2)), has made himself a regular source of income by committing such an offence, as well as organises or directs such activities (article 116.(3) of the, art. 117.(2)). Fencing of track media is also penalised (article 118.(1), action in negligence – article 118.(3)), while liability is enhanced if the perpetrator has made himself a regular source of income by committing such an offence, as well as organises or directs such activities (article 118.(2)). An offence is the producing, trading and advertising for sale or rental of devices (or components of such devices) for removal or omitting of technical measures designed to protect the subject of copyright (article 118^1.(1)), as well as possession, storage or use of such equipment or their components (article 118^1 (2)). Punished is also preventing or obstructing the exercise of the right to control the use of works protected by copyright (article 119).

Regulations regarding the copyright protection are also included in the Industrial Property Act dated 30 June 2000 (Dz.U. 2003 No. 119 item 1117 as amended by 13.06.2003, with later amendments). The statute penalises false claim of authorship or misleading as to the authorship of an inventive design, or otherwise violates the rights of the creators of such project (article 303.(1)), enhancing the liability of the offender who acts in order to gain financial or personal benefit (article 303.(2)). It is forbidden to submit someone else's invention, utility model, industrial or someone else's topography of an integrated circuit in order to obtain patent, right of protection or registration right - made by person not permitted to obtain patent, protection right or registration right (article 304.(1)), as well as action to prevent grant of patent or protection right or registration right – i.a. by disclosure of the obtained information about someone else's invention, utility or industrial model or someone else's topography (article 304.(2). An offender who is obliged to maintain secrecy and who acts unintentionally is also punished - article 304 (3)). It is an offence marking of goods by counterfeit trademark or trading of such goods (article 305.(1)). A perpetrator who has made himself a regular source of income by committing such an offence or who commits an offence in relation to goods of significant value is subject to more severe punishment (article 305 (2)).

3. Industrial espionage

The Penal Code prohibits the unauthorised disclosure or use of secret information. Article 265 § 1 kk penalises disclosure or use, contrary to the provisions of the law, of information classified as "secret" or "top secret". Crimi-

nal liability is enhanced if such information is disclosed to a person acting on behalf of or for the benefit of a foreign entity (article 265 § 1 kk). An unintentional disclosure of such information obtained in connection with the performance of public function or received authorisation is also an offence (article 265 § 3 kk).

The Penal Code also protects professional secrecy, penalising unauthorised (against the law or an obligation he or she has undertaken) disclosure or use of information, to which the offender is familiar as a result of his or her function, work, public activities and acquaint with in connection with its function, work, activities, social, economic or scientific research (article 266 § 1 kk). More rigorous liability applies to a public functionary who reveals information classified as "restricted" or "confidential" to an unwarranted person or information which he or she obtained in connection with the performance of his or her official duties and when a disclosure may cause harm to the legally protected interest (article 266 § 2 kk).

The criminal provisions of the Combating Unfair Competition Act dated 16 April 1993 (Dz.U. 2003 No. 153, item 1503 as amended by 26.06.2003, with later amendments) prohibit the disclosure to another person, or used in his or her own business, of company secrets by a person in relation to an entrepreneur - if it causes serious harm to an entrepreneur (article 23.(1)) and the person who unlawfully obtained a company's confidential information (article 23.(2)).

(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.

The development and broad dissemination of information and communication systems has resulted in the transfer of a wide range of human activity to the virtual sphere. There are more and more applications for creating "virtual personalities". On the one hand, we talk about chatterbots, i.e. applications that use artificial intelligence, created mainly in order to enable interactive communication between man and computer (Internet), on the other – about user-created network profiles. In the Polish criminal law there are no provisions directly related to actions against chatterbots or virtual profiles, but provisions concerning digital data integrity protection can be applied, as well as article 190a § 2 kk penalising impersonating another person – if the perpetrator's aim is to cause personal or property harm to that person (this provision may in some way refer to actions against profiles of network users).

(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 cybersystems 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.

The Penal Code requires that a person who have reliable information about a punishable preparation, attempt or achievement of any of enumerated most serious criminal offences[72], notify law enforcement authorities. Failing to do

[72] Including genocide, the production and use of means of mass destruction, coup d'état, espionage, manslaughter, threat to life or property of many people, or terrorist crimes

so is punishable (article 240 § 1 kk).

The Code of Criminal Procedure imposes on state and local government authorities legal obligation to report criminal offences prosecuted *ex officio*[73] (article 304 § 2 kpk). In relation to the citizen "the duty of denunciation carries penalty only in clearly established cases "[74], i.e. cases related to the most serious crimes specified in article 240 kk. In other situations, obligation imposed by provision of the Code of Criminal Procedure is only a social obligation. The obligation of reporting a crime imposed in article 304 § 2 kpk on state and local government authorities "refers not only to crimes affecting the welfare of the institution but also to other criminal offences prosecuted *ex officio*, which have come to the institution's knowledge in connection with its legal or statutory activity"[75], and the "failure to comply with the legal obligation to report a crime may result in criminal liability under article 231 kk, i.e. for action to the detriment of public or private interest, by failure to comply with the obligation"[76].

Internet access in Poland is implemented by means of broadband data transmission. Regardless of whether it takes the form of stationary or mobile access, telecommunications technologies (i.a. phone lines, cable and satellite TV, radio access, mobile telephony) are used to ensure such access. The Telecommunications Act dated 16 July 2004 (Dz.U. No. 171 item 1800 with later amendments) is applicable to the area of such technologies and services. The statute (article 2.(42)) defines telecommunications as broadcast, the reception or transmission of information, regardless of their nature, by wire, radio, optical or other electromagnetic means.

Article 159.(1) of the Telecommunications Act defines the scope of data embodied by telecommunication secrecy ("privacy of network communication "). According to the statute, data about the user, the content of individual messages[77], the transmission data[78], the location data, means location-based data beyond what is necessary for mes-

---

[73] In relation to cybercrime, this applies to i.a. the bringing of danger to the life or health of numerous persons, or property of considerable size, by interfering with, disabling, or otherwise affecting automatic processing, collecting or transmitting computer data (article 165 § 1.(4) kk); making contact with minors below the age of 15 (e.g. in order to produce or to record pornographic content) through an ICT system (article 200a § 1 kk); child pornography offences (article 202 §§ 3-4b kk); violation of integrity or interfering with or preventing automatic processing of computer data of particular interest to national defence, security in communication, functioning of government administration, other state authorities, state-run institution body or local government authorities (article 269 § 1 kk); significant interfering with the work of a computer by violation of the integrity of the data being processed in the system (article 269a kk); manufacture and trading of devices or computer software adapted to commit certain offences (article 269b § 1 kk); fraud (article 286 kk) and computer fraud (article 287 kk).

[74] Tomasz Grzegorczyk, *Kodeks postępowania karnego, Komentarz [The Code of Criminal Procedure, Commentary]*, Zakamycze 2001, p. 691 – 692;
Feliks Prusak, *Komentarz do Kodeksu postępowania karnego t. 2 [The Commentary to the Code of Criminal Procedure, vol. 2]*, Wydawnictwo Prawnicze, Warszawa 1999, p. 855.

[75] Wincenty Grzeszczyk, *Obowiązek zawiadomienia o przestępstwie [Obligation to Report a Crime]*, Prokuratura i Prawo 1998 r., nr 10, s. 124.

[76] Wincenty Grzeszczyk, *Obowiązek zawiadomienia o przestępstwie [Obligation to Report a Crime]*, Prokuratura i Prawo 1998 r., nr 10, s. 124-125.

[77] I.e. information exchanged or transmitted between certain users via publicly available telecommunications services (this does not apply to information submitted as part of radio or television broadcasts transmitted via telecommunication networks, with the exception of information relating to an identifiable subscriber or user receiving the information).

sage transmission or billing, or data on attempts to achieve connection between certain telecommunication network endings[79]. Telecommunication companies are required to perform tasks in relation to national defence, state security and public order and safety (article 179). This obligation includes i.a. ensuring (at the expense of the operator) technical and organisational conditions for simultaneous and mutually independent access to the content of telecommunication transmission and to data held by the operator[80], related to the provided service, any recording of such content and data[81] by the competent authorities (Police, Polish Border Guard, the Internal Security Agency, the Military Counterintelligence Service, Military Police, the Central Anti-Corruption Bureau, Tax Intelligence), as well as any recording of such data and content of telecommunication transmission data and of the duration of such data and of any telecommunication transfers for the benefit of the court and the prosecutor.

The Telecommunications Act requires also the telecommunication operator to block, without delay, and at the request of competent entities or allow these entities to block, any telecommunication links or information transfers that may jeopardise the defence, security of the state, public order and safety (article 180).

The network service providers are required to retain and store (article 180a - 180c) any data necessary to determine network endings, telecommunication terminal equipment and end-users (initiating connection and connection recipient) and to determine type, date and time of the connection and its duration as well as the location of telecommunication terminal equipment[82].

---

[78] Data processed for the purpose of message transmission in telecommunications networks or billing for telecommunication services, including location-based data, meaning any data processed in telecommunications network indicating the geographical location of the device of an end user of publicly available telecommunication services.

[79] Network ending - physical point, where a subscriber receives access to a public telecommunication network; in the case of a network using switching or routing, network ending is identified with a certain network address, which may be attributed to the number or name of the subscriber.

[80] From article 179.(9) the electronic list of subscribers, users, or network endings, with regard to data obtained at the conclusion of a contract; from the article 159.(1) i.a. user data, content of individual messages and data on attempts to achieve connection between certain telecommunication network endings; from the article 161.(2) user data (natural person) such as i.a. names and surname, date and place of birth, name, series and number of identity document.

[81] Implementing rules regarding an authorised interception imposed on entities that provide cryptographic support an obligation to decrypt intercepted content (§ 7 and § 8 of the regulation of Minister of Justice dated 24 June 2003 on technical preparation of the network used for transmission of information to control transfers of information and manner of making, registration, storage, playback, and destruction of records with controlled transfers, Dz.U. No 110, item 1052).

[82] Regulation of the Minister of Infrastructure dated 28 December 2009 on the detailed list of data and the types of public telecommunication network operators, or publicly available telecommunications services providers, obliged to their retention and storage (Dz.U. No 226 item 1828), lists of data i.a. name and surname or the name and address of the subscriber, as well as the address of the location of telecommunication equipment in the stationary public telecommunications network; MSISDN, IMSI, IMEI or ESN numbers for mobile devices; the IP address, the name and surname or the name and address of the user, the MAC address of the device in the case of access to the Internet.