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

POLAND*

Dr Celina NOWAK
Dr Małgorzata SKÓRZEWSKA-AMBERG*

(A) Introduction

At the beginning it seems useful to stress that several notions related to the cybercrime are defined in the Polish law or in Polish official documents. Firstly, in the official *Strategy of development of information society in Poland until 2013*[1], which is an official governmental document, the information society is defined as a society for which processing information with the use of information and communication technologies constitutes a significant economic, social and cultural value.

In Polish law cyberspace is defined as a space of processing and exchanging information created by electronic systems, networks thereof and their relations with users (Art. 2 para 1(b) of the Act of 29 August 2002 on the State of War and Competencies of Commander-in-Chief of the Armed Forces and Rules of His Subordination to the Constitutional Authorities of the Republic of Poland[2]). Pursuant to Art. 3(3) of the Act of 17 February 2005 on Computerization of Activities of Entities Implementing Public Tasks[3], an electronic system is defined as a set of cooperating devices and software ensuring processing[4] data in telecommunication networks[5]. Accordingly, Art. 7 (2a) of the Act of 29 August 1997 on Data Protection[6] defines an electronic system as a set of cooperating devices, programs (software), procedures of data processing and programming tools used to process data.

(B) Criminalisation

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

The main legal interest protected by criminal law with regard to virtual space (cyberspace) is the traditional freedom

---

* 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.

* Dr Celina Nowak, Ph.D. Assistant professor at Kozminski University and the Institute of Legal Studies of the Polish Academy of Sciences.
Dr Małgorzata Skórzewska-Amberg, Ph.D. (law), MSc IT, assistant professor at Kozminski University.

1 See: http://www.msw.gov.pl/portal/SZS/495/6271/ (viewed on 1 November 2012).

2 Official Journal of the Republic of Poland (hereinafter as „O.J.") No 156, item 1301 as amended.

3 O.J. No 64, item 565 as amended.

4 The notion of "processing" data encompasses data storage, sending and receiving.

5 Processing takes place with the use of an ending device, appropriate for a given type of network, destined to be plugged directly or indirectly to the ending of the network (so called telecommunication ending device, pursuant to Art. 2(43) of the Act of 16 July 2004 – Telecommunication Law, published O.J. No 171, item 1800 as amended).

6 Unified text in O.J. of 2002, No 101, item 926 as amended.

and security of an individual, yet understood from a specific, cyberspace-oriented perspective. Therefore, the right is understood inter alia as the right to privacy of the individual, as trust of individuals to electronic system, as trust to documents and data stored in such a system. Also an individual's right to decide on information is protected (i.e. an individual's right to freely decide for instance as to the free and exclusive right to administer information in the individual's disposal, as well as to freely decide on the scope and type of disclosed data referring to the individual)[7], as well as the constitutionally guaranteed right to protection of privacy and secret of communication[8].

Criminal law protection of cyberspace also means protection of credibility of economy, authenticity of documents, etc. Criminal law also offers protection to property, defined by civil law as property and other property rights[9]. This is due to the fact that often criminal activity in cyberspace is directly aimed against property – for instance spoofing (in particular phishing).

Concerning more specific interests related to the cyberspace, one should note that Polish criminal law mainly protects integrality and access to information stored and processed in electronic network, as well as integrality and safety of computer systems.

It seems useful to point out that sometimes the Polish legislator has had difficulty in clearly defining protected interest with regard to cybercrime and in consequence in correct formulating the legal provisions. Art. 267 PC may be a good example here. As of now, the provision protects unauthorized access to information. The penalty for such a breach of a computer system is related with opening of an enclosed letter, connecting to telecommunications network or breaking or omitting electronic, magnetic, software or other specific information security, as well as an unauthorized installing or use of a tapping device or any other visual device, software or technology. However, Art. 267 PC in its previous wording[10], apart from the protection of communication secrecy also ensured the protection of messages against unauthorized access. In fact, not access to information was protected, but information itself. This was quite an unfortunate solution, as it limited the scope of application of the provision in an unjustified manner. Namely, in cases when access to a system was gained without visibly obtaining any information (e.g. the offender obtained information in a completely different network, another country or in a manner which did not necessarily link the losing of information in one system with an unauthorized entry to another system), the perpetrator could have avoided the responsibility for his action. Doubts also arose whether activities such as bypassing security or taking advantage of software gaps were equivalent to protection breaking.

The change of PC adopted in 2008 moved protection of information to the access to it, essentially changing the scope of protection, allowing to prosecute gaining access to information without entry into possession of its content.

---

[7] See Włodzimierz Wróbel (in:) Andrzej Zoll (ed.) Kodeks karny. Część szególna. Komentarz, tom II, Komentarz do art. 117-277 k.k., Wolter Kluwers, Warszawa 2008, p. 1287.

[8] See Andrzej Marek, Kodeks karny. Komentarz, Wolters Kluwer, Warszawa 20101, p. 570; Joanna Piórkowska-Flieger (in:) Tadeusz Bojarski (red.) Kodeks karny. Komentarz, 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., Wolter Kluwers, Warszawa 2008, p. 25.

[10] The changes were introduced by Act of 24 October 2008, O.J. No 214, item 1344.

(2) Please give typical examples of criminal laws concerning

(a) attacks against IT systems

Polish criminal law provides for numerous provisions referring to both content and data processed in electronic systems and integrality of such systems. For instance there are legal norms directly referring to protection of ICT system against unauthorized access (Art. 267 para 2 of the Penal Code, hereinafter as "PC"[11]) as well as to protection of operational security of an ICT system (Art. 269a PC). These norms penalize significant disturbance of work of ICT system or computer network caused by actions of an unauthorized person who transmits, destroys, removes, impedes access or changes computer data.

Although other provisions of the Penal Code do not refer to attacks against IT systems directly, in the event of such an attack it is possible to apply provisions which penalize actions against the content of such systems (e.g. information stored, transmitted and processed in IT systems) and thus indirectly protect the system. As an example one could cite provisions on protection of access to information stored in IT system (Art. 267 para 1 PC).

(b) violation of IT privacy

Violation of integrality of IT system is directly penalized in chapter XXXIII of the PC, which provides for offences against protection of information. In Art. 267 paras 1-3 PC the legislator penalizes inter alia unauthorized access to secured information (if it is related to gaining access to strictly private data) as well as unauthorized interception of data (tapping).

(c) forgery and manipulation of digitally stored data

Other provisions contained in the mentioned chapter (Art. 268-269 PC) also refer to acts which violate integrality of information. Acts such as unauthorized destruction, damaging, removal or modification of digital information are penalized, alongside with disturbance of access to computer data.

(d) distribution of computer viruses

Polish criminal law does not contain a provision expressly penalizing distribution of computer viruses. This does not however mean that such actions are allowed. Development and distribution of computer viruses may be penalized on the basis of provisions referring to protection of information (Chapter XXXIII PC) as acts violating integrality of ICT systems and data stored therein.

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

It seems obvious that progress and wide expansion of ICT systems contributed to a wide extent to a transfer of a large part of human activity to virtual reality (cyberspace). There are more and more applications allowing for creation of different type of "virtual identities". On the one hand one may mention chatbots, i.e. applications using artificial intelligence, mainly created to enable interactive communication between a human being and a computer (Internet), on the other – personal profiles created by users of ICT networks.

Polish criminal law does not provide for provisions which would directly refer to acts against chatbots and/or virtual profiles. However, provisions on violation of integrality of digital data may be used here. In addition, a new provision

[11] Penal Code of 6 June 1997, entered into force on 1 September 1998, O.J. No 88, item 553 as amended.

of Art. 190a para 2 PC could be used in such situations. This provision was introduced into the PC in 2011[12]. It provides for criminal responsibility of a person who impersonates someone else and uses this person's image or other personal data in order to cause this person a material or personal damage. Such behavior is punishable with the penalty of deprivation of liberty for a term up to 3 years. It seems that this provision may be used to acts against network profiles of users – for instance when the perpetrator impersonates a victim in cyberspace, stealing his/her virtual profile.

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

It seems clear that IT systems and networks have contributed at the same time to the emergence of new types of crime as well as new forms of "old" crimes. The offences related to pornography are an example of "old" crimes which have taken new forms due to the progress of computer technologies. The pornography in cyberspace encompasses three types of pornographic activity: pornography, child pornography and so-called generated pornography. The latter, which is sometimes called simulated pornography is an example of a new behavior closely related to the emergence of advanced computer technology. Advancement and expansion of digital technologies have contributed to the development of relatively cheap tools allowing to create virtual reality, including pornographic materials, mostly simulated child pornography, ie. artificially generated materials showing more or less realistic images of a non-existing person or modified images of adults made to look like children, or children used "virtually", which means modifying children's images. Some of these behaviors are criminalized in the Polish criminal law. Namely it provides for responsibility for simulated pornography, when it was made with the use of produced or transformed image of a minor taking part in sexual activity (Art. 202 para 4b PC).

Concerning new types of crimes, which have developed in the area of ICT, one can cite violations of copyrights. New technologies make possible wide and direct access to materials and contents covered by copyrights. Sharing these materials in virtual space often violates rights of authors. Therefore the Penal Code and Act of 4 February 1994 on Copyrights and Similar Rights[13] include provisions referring to protection of computer software and production and trade of devices (of components of devices) used to remove or omit technical means aimed at protecting works covered by copyrights.

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

Concerning *actus reus* with regard to offences committed in cyberspace in the Polish law, one should note that it is usually defined by description of act, e.g.:

- whoever gains access without authorization to information which has not been designed to him by connecting to the telecommunication network,
- whoever gains access without authorization to the whole or part of an electronic system
- whoever produces, gains, sells or makes accessible to other persons devices or computer programs adapted to commit crimes,
- whoever gains someone else's computer program without a consent of the entitled person.

[12] Act amending the PC of 25 February 2011, entered into force on 6 June 2011, O.J. No 72, item 381.
[13] Unified text in O.J. of 2006, No 90, item 631 as amended.

In some cases *actus reus* is defined at the same time by description of the behavior and consequence of the act – as it is in Art. 269a PC, which provides for a liability for a person who "without authorization, by transmitting, destroying, removal, damaging, hindering access or change of electronic data significantly disturbs work of a computer system or an IT network". It results from this provision that the behavior is punishable only if it is aimed against proper functioning of the computer system or an IT network.

Concerning the definition of the object in Polish criminal law, it is most of all "computer data" or "information". In some cases the legislator uses a term of "computer programme" (software), "computer system", "ICT network", "computer storage device" and "document". Some of these notions have legal definitions. Pursuant to Art. 115 para 14 PC, a document is any object or carrier of information with which a given right is related or which – due to its content – constitutes a proof of right, legal relation or legally significant circumstance. As it has been mentioned, an ICT network (ICT system) is defined in the Act on computerization of activities of entities implementing public tasks. According to the same Act, a computer storage device is defined as material or device used to record, store and read digital data. The notion of "computer data" is not defined in law.

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

No, generally speaking criminal liability for cyber crimes is not limited to any particular groups of perpetrators and/or victims.

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

No, in principle, according to the Polish law cyber crimes can only be committed intentionally. However, there are rare cases of offences which may also be committed unintentionally (e.g. offence set forth in Art 165 para 2 PC which provides for liability for unintentional endangering lives or health of many persons or property in great amount committed *inter alia* by disturbing, making impossible or otherwise influencing automatic processing, storage or transmission of computer data).

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

No, generally speaking Polish criminal law does not make a difference between the definitions of cyber crimes and "traditional" crimes, except for differences due to the specific character of the regulated matters (ie. specific object of crime, specific legal interest protected).

However, there may be rare cases when there is a difference in definitions between a cybercrime and traditional crime. That is an example of the so-called computer fraud. Pursuant to Art. 286 PC, a traditional (simple) fraud takes place when a person acting with the purpose of gaining an economic benefit, causes another person to disadvantageously dispose of his own or someone else's property, by misleading this person, taking advantage of his mistake or inability to properly understand undertaken actions. Whereas computer fraud is provided for in a separate provision (Art. 287 PC) and consists in unauthorized influence on automatic processing, storage or transmission of computer data, change, removal or introduction of new computer data entry – in order to gain material benefit or cause damage to another. The difference between simple fraud and computer fraud is that the perpetrator of

computer fraud does not mislead another person or does not take advantage of this person's mistake[14]. The perpetrator's behavior, who still acts in order to gain material benefit or cause a damage to another person, is not aimed against this person directly, is not carried out "on this person", but on the data[15].

(C) Legislative technique

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

It seems that sometimes the Polish legislator has had difficulty in clearly defining protected interest with regard to cybercrime and in consequence in correct formulating the legal provisions. This may lead to some problems with respect to the principle of legality. The definition of crime set forth in Art. 269b para 1 PC may be an example here[16]. It is unnecessarily vague, formulated in an imprecise manner (e.g. there is a risk of a wide interpretation of the expression "devices or computer programs adapted to commit crimes").

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

These issues are not object of the debate in Poland.

(3) How does criminal legislation avoid becoming obsolete in light of rapid technological innovation? E.g.,

- how are changes in the use of internet and social networks taken into account?

- how is the law adapted to technological progress (e.g., by reference to administrative regulations)?

These issues are not object of the debate in Poland.

(D) Extent of criminalisation

(1) To what extent do criminal laws cover mere preparatory acts that carry a risk of furthering abuse, e.g., acquisition or possession of software that can be used for "hacking", "phishing", computer fraud, or bypassing download protection? If so, has there been controversy about introducing such laws? Have legislatures made specific efforts to avoid over-criminalization?

To some extent the Polish criminal law does criminalize preparatory acts to offences against protection of information or other offences which may be committed with the use of IT. Namely, pursuant to Art. 269b para 1 PC it is punishable to produce, gain, sell or make accessible to other persons devices or computer programs adapted to commit crimes listed in the provision. Furthermore, on the basis of this provision it is also punishable to produce, gain, sell or make accessible to other persons computer passwords, access codes or any other data enabling to gain access to information stored in computer system or ICT network. In fact, the imprecise formulation of the subject provision referring to "information stored in computer system or ICT network" extends the scope of penalization to practically any information stored in computer system or ICT network, such as e.g. links to websites. It seems that such a wide scope of application of this provision was not intended by the legislator – only secured information should be protected – and should therefore require a legislative change.

---

[14] For this reason some authors argue that the offence set forth in Art. 287 PC should not be called "computer fraud" as it is not a real fraud, which consists precisely in cheating someone else. They propose to call it "computer manipulation". See R. Korczyński, R. Koszut, "Oszustwo" komputerowe, Prokuratura i Prawo 2002, No 2.

[15] See more on this in M. Janowski, Przestępstwo tzw. oszustwa komputerowego, Prokuratura i Prawo 2011, No 10, p. 52-63.

[16] Definition cited below, in D1.

(2) To what extent has the mere possession of certain data been criminalised? In what areas, and on what grounds? How is "possession" of data defined? Does the definition include temporary possession or mere viewing?

In Polish law, the prohibition to posses illegal data (materials, contents) with regard to cyberspace covers the following types of data: someone else's computer program, child pornography, data propagating fascist or otherwise totalitarian regime or data inciting to hatred for national, ethnic, racial, religious reasons.

In Polish law the possession is defined following the civil law notion of actual power over a thing. In criminal law possession of the aforementioned data is understood as having them in someone's disposal even for a short period of time[17].

(3) To the extent that possession of or granting access to certain data have been defined as criminal, does criminal liability extend to service providers (e.g., hosting or access providers)? What are the requirements of their liability, especially concerning mens rea? Are providers obliged to monitor and control what information they provide or offer access to? Are providers obliged to provide information on the identity of users? Are providers obliged to prevent access to certain information? If so, under what conditions, and at whose cost? Is there criminal liability for violating such obligations?

Obligations of service providers related to the electronic performance of services[18], including rules on excluding liability of service providers, are regulated by the Act of 18 July 2002 on Electronic Services Providing[19].

It should be pointed out that the subject Act regulates the scope of responsibility of service providers in a negative way, ie. by providing for a catalogue of clauses excluding their responsibility. These clauses refer to intermediating providers, ie. providers who only transmit and store data coming from other parties. The exclusions do not refer to so-called content providers, which are responsible for contents they provide.

In any case, if a service provider, which is not a content provider does not qualify for exclusion, he may be held liable on general basis of civil or criminal law or other statutory acts. However, one should add that the catalogue of exclusions is very large and enforcement of these obligations seems quite doubtful.

According to the Act a service provider is an individual, a legal person or an organizational entity without legal personality.

There is one general rule related to the responsibility of service providers: they are not obliged to verify the content of the data transferred to him for storage, transmission or recording. Service providers are thus not obliged to censor the data, to verify their possible illegal character.

The exclusions refer to mere conduit, caching and hosting. Concerning mere conduit, a service provider is not responsible for transmitted data and is not obliged to verify its content if he does not initiate a transmission, does not

[17] See Marek Bielski Wróbel (in:) Andrzej Zoll (ed.) Kodeks karny. Część szczególna. Komentarz, tom II, Komentarz do art. 117-277 k.k., Wolter Kluwers, Warszawa 2008, p. 680-81.

[18] A service is provided electronically if its performance takes place through transfer of data, transmitted with the use of public networks. Hardware and software enabling to communicate in distance are called means of electronic communication.

[19] O.J. No 144, item 1204 as amended.

choose a recipient of data or does not remove or modify transmitted data. Also, he is not responsible for data stored automatically, indirectly and for a short period of time – exclusively in order to transmit it.

With respect to caching, a service provider is not responsible for automatic, indirect and short-time storage of data transmitted by service taker, provided that he does not change its content, follows conditions of access to information and updating information (in a commonly recognized and used manner), does not disturb legal usage of technology commonly recognized and applied to store information on usage of stored data. This exclusion applies provided that the service provider immediately removes or blocks access to stored data as soon as an initial source of data transmission has been removed from the network or its access to the network has been blocked, or when a court or an administrative authority orders to remove data or block access to it.

Finally, concerning hosting, service providers are not responsible for data stored in the system by the user if they are not aware of the illicit character of the data or activity related to the data. As soon as the service provider receives information on illegal character of the stored data, he is obliged to undertake steps necessary to block access to this data. If the notification on illegality of data is official, a service provider is not responsible toward the user for damages caused by blocking access to data. Otherwise a service provider is not responsible for damages caused by blocking access to data provided that he informed the user on intention to block access to data.

According to the Polish law a service provider may only be held responsible for putting contents in the network or for intentionally making his services available for such a purpose (perpetration or aiding).

A service provider may easily be prosecuted if he is an individual. In such event, general rules of criminal responsibility will apply to him. The problem arises if the service provider is a legal person or an organizational entity. Then he can be prosecuted only if an individual committed an offence to his benefit, which may be difficult to establish[20].

It may be added that prosecuting service providers for publishing contents of racist character have been difficult, for – as practice shows – they usually come from abroad. However, there has been some convictions in Poland with regard to persons editing websites publishing information inciting to hatred based on race[21].

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

In the debate on the restriction of access to websites containing content against the law, more particularly on the register of illegal websites and services, mainly arguments referring to freedom of speech and freedom of press have been raised. It has been raised it may have a reverse effect as it warns perpetrators and does not stop them.

Also the draft act implementing the Council Framework Decision 2004/68/JHA of 22 December 2003 on combating the sexual exploitation of children and child pornography, which was to introduce blocking or removal of website with

[20] See below, p. E1.

[21] Service providers came from USA.. Polish editors were convicted. See http://osnews.pl/polscy-redaktorzy-redwatch-pojda-siedziec/ (viewed on 31 October 2012).

child pornography, and later on the signature of ACTA by Poland have given raise to controversy and opposition among the society, due to the limitation of freedom of speech and privacy[22].

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

No, no specific special sanctions targeting cyber criminals are foreseen in the Polish law.

(E) Alternatives to Criminalisation

(1) What role does criminal law play in relation to other ways of combating abuse of ICT and the internet? What is the relationship of civil and administrative sanctions (payment of damages, closing of enterprise, etc.) to criminal sanctions in the area of ICT?

In Poland, without doubt, criminal law constitutes the strongest and most effective instrument to enforce the correct use of ICT and Internet. Other sanctions can only complement it, however their effectiveness may be questioned.

A victim of a cybercrime may seek compensation for damages suffered on general basis of civil law. Yet this does not seem like an effective solution. Firstly, in order to open proceedings, an introductory fee must be paid, which may seriously hinder access to the court to some persons. Secondly, a civil process may take a long time, which is not desirable from the point of the victim.

Polish criminal law has its limits, in particular it is aimed at individuals only. However, the Polish law provides for a possibility to hold liable legal persons for cybercrime. It is possible on the basis of a special statutory Act of 28 October 2002 on Liability of Collective Entities for Acts Prohibited under Penalty[23].

Pursuant to Art 2 of this Act, a collective entity is a legal person, an organization entity which does not have legal personality, which is vested legal capacity on the basis of special provisions (except for the State Treasury and self-government units), a company the share of which are owned by the State Treasury or self-government units, a company under organization, an entity in liquidation, an entrepreneur who is not an individual and a foreign organization entity.

The liability of collective entities is restricted to the commission of certain types of offences only, enumerated in Art. 16 of the Act. The list includes offences typically related to activities of corporations, including cybercrime (offences against protection of information provided for in Art. 267-269b PC; offences against property, including computer fraud; offences against sexual liberty and morality, including simulated child pornography).

The liability of collective entities is based on a two-step model. First, penal responsibility of an individual who was linked to the collective entity and acted to its benefit must be recognized in a valid and final conviction or a decision otherwise terminating the proceedings (such as e.g. conditional discontinuance of proceedings). Only then is the liability of a collective entity triggered. The liability of collective entities is therefore not autonomous, but depends upon the responsibility of individuals. It is possible that such model may seriously hinder effective prosecution of collective entities. In fact, no legal person was convicted in Poland for commission of a prohibited act so far.

In any case however, a collective entity may be sentenced to a pecuniary sanction, forfeiture of objects coming from

[22] See http://www.stopcenzurze.eu/ (viewed on 30 October 2012).
[23] Act on Liability of Collective Entities for Acts Prohibited under Penalty, published in O.J. No 197, item 1661 as amended.

an offence, destined or used to its commission, or forfeiture of benefits coming from an offence. Furthermore, a collective entity may be banned from promoting or advertising its activities, from benefiting from public funds and aid coming from international organizations to which Poland is a member, from applying for public procurement. The court may also decide to make the judgment publicly known.

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

Websites which contain content violating the law should be removed. However, it is only possible when the servers which the sites use to operate are located on the territory of the state, which considers the content a violation of law. In order to be able to do so in Poland, in November 2009 Polish government submitted a proposal to establish a register of illicit websites and services. The register was to be aimed at blocking access to websites containing content forbidden by law, including child pornography, propagating fascist or otherwise totalitarian regime, materials aimed at deceitful misleading of persons in order to gain material benefit. The proposal has been vividly discussed, constitutional guarantees have been menioned. Eventually, at the beginning of 2010 the government withdrew the proposal. As of now in Poland there is no possibility to close down or even register websites.

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

It seems obvious that ICT users should try to secure their computers and data using inter alia strong enough and often changed passwords to log in, anti-virus software, appropriate firewalls. The decision to use these means and the choice thereof depends upon the user. The Polish law does not provide for direct sanctions for users due to the lack of proper protection, unless when the users are legally obliged to apply special means of protection. For instance, a data protection manager is obliged to apply technical and organization means ensuring protection of the processed data proportionate to the threats and type of data (Art. 36 of the Data Protection Act). In addition, entities processing data covered by state or professional secrecy are obliged to apply special means to protect data.

However, even though the Polish law does not provide for a general obligation to apply special protection means with regard to data processed in ICT systems, the lack of such a protection may, in some cases, cause that a behavior does not qualify as an offence. For instance, Art. 267 PC stipulates that shall be held liable whoever gains access to information by connecting to the telecommunication network or breaking or omitting electronic, magnetic, electronic or any other special protection. Therefore, if a perpetrator gains access to information which has been stored on a computer drive, even without authorization, but the information has not been protected at all (e.g. by a password to the system), then he will not be held penally responsible.

(F) Limiting anonymity

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

In principle Internet service providers are obliged to store users' personal data for purposes of the service. Namely, a provider of publicly accessible telecommunications services may process data on individual users (name, names of

parents, place and date of birth, address, identity card's number, personal identification number), if the data is included in documents related to the telecommunications services contract. Other data may be processed only in relation to the service provided, upon consent of the user (eg. number of bank account). In any other case content or data covered by the telecommunication secrecy may be processed (ie. collected, recorder, stored, elaborated, changed, removed or disclosed) only when these actions refer to the service provided to the user or are necessary for the performance of the service[24].

This is due to the fact that such data – on the basis of Art. 159 para 1 of the Act of 16 July 2004 Telecommunication Law[25] – is covered with the so-called telecommunication secrecy ("secrecy of communication through networks"). The protected data encompass data referring to the user, content of individual communications[26], transmission data[27], data on localization, which means data on localization beyond data necessary to transmit a communication or issue a receipt, and data related to attempts to establish a connection between given terminal equipment of telecommunication network[28]. According to the subject Act it is prohibited to gain access, record, store, transmit or otherwise use content or data covered by the telecommunication secrecy. The prohibition refers to persons other that the sender and receiver of communication, but it may be waived upon a consent of the sender or receiver, to whom the data concern. It does not apply in exceptional situation when such actions are necessary to perform a service or are subject to a service or when it is necessary for other reasons regulated by law.

Except for cases provided for in law[29], disclosure or processing of data covered by communication secrecy constitute a violation of obligation to keep the secrecy, which bears on entities taking part in telecommunication activity and bodies cooperating with them (Art 160 para 1 of the Act). These entities and bodies are in particular obliged to "observe due diligence, to the extent justified by technical or economical reasons, when protecting telecommunication devices, telecommunication networks and sets of data against disclosure of telecommunication secrecy" (Art. 160 para 2 of the Act).

A telecommunication entrepreneur is responsible for violation of telecommunication secrecy by entities acting on his behalf (Art. 161 para 1 of the Act). The obligation to observe telecommunication secrecy also refers to a person who gained access to a communication which has not been destined to him using a radio device or a terminal equipment device. A provider of publicly accessible telecommunication services as well as an operator of public telecommunication network are obliged to undertake technical and organizational actions in order to ensure safety of communications transmission, related to the service that they provide. If there is a particular risk of breaching security of services provided, a provider of such services is obliged to inform users that technical means he uses do not guarantee safety of transmission of communications. He should also inform users of existing possibilities to ensure such safety and costs they would entail (Art. 175).

---

[24] Processing data for other purposes is allowed only on the basis of law (Art. 161 of the Telecommunication Act).
[25] O.J. No 171, item 1800 as amended.
[26] I.e. information exchanged or transmitted between users through publicly accessible telecommunications services.
[27] Data processed for purposes of transmission of communications or charging for telecommunication services including localization data.
[28] Terminal equipment is a physical place in which a user gains access to public telecommunication network. It is identified with a specific network address, which may be attributed to the number or name of the user.
[29] For instance communications revealed on the basis of an order of a court, a prosecutor or separate provisions.

Concerning the obligation to provide personal data on users to law enforcement agencies, in Poland the law enforcement agencies may have a free and very wide access to data on users, which is subject to criticism. Telecommunication entrepreneurs are obliged to perform certain tasks for safety of the state and public order. They are obliged to provide access to certain data to the authorized authorities (Police, Border Guards, Internal Security Agency, Military Police, Military Intelligence Service, Central Anti-Corruption Bureau and treasury investigation service). The entrepreneurs are in particular obliged to ensure technical and organizational conditions allowing to have simultaneous and independent access[30] to contents of telecommunication transmissions and certain personal data referring to the user and his connections which they has at their disposal.

Internet service providers are obliged to retain and store data necessary to establish a terminal equipment of the network, telecommunication terminal equipment and terminal users (initiating and receiving the connection), to establish type, date and hour of the connection and its duration, as well as localization of the telecommunication terminal equipment device[31]. This data, generated in the telecommunication network or processed in Poland, is to be stored for a period of 24 months from the date of the connection or failed connection, at their own expense. This data may be made accessible to authorized authorities (including customs, prosecutors and courts).

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

In Poland in principle providing telecommunication services takes place on the basis of a written contract. However, this does not mean that an Internet service provider is always obliged to register users prior to providing services as the condition of concluding a written contract (where some persona data must be included) does not apply to so-called prepaid services. In Poland prepaid SIM cards do not have to be registered, which means that access to Internet provided by mobile phones networks through prepaid cards is open to users who have not been registered by the provider.

(3) Are there laws or regulations limiting the encryption of files and messages on the internet? Can suspects be forced to disclose passwords they use?

Since modern encrypting techniques may be very efficient, the legislator in Poland tends to take care for the state's interest when an authorized interception of a message has taken place. Pursuant to para 8 of the Ordinance of Ministry of Justice of 24 June 2003 on technical preparation of networks used to exchange of information, to control transmissions and manner to register, store, record and destroy records of controlled transmissions[32], a telecommunication servicer provider (including an Internet service provider) who performs encrypting services, is obliged to disclosed unencrypted information to authorized agencies.

If the message is encrypted by other entities, in particular users of telecommunication networks themselves, Polish law does not provide for mechanisms obliging them to disclose the content of such a message. This is in particular reinforced by a prohibition to oblige anyone to provide incriminating materials set forth in Polish criminal procedure.

---

[30] These words are not clear, but it seems that this means that the law enforcement agencies should have access to data in real time, independently from other agencies.

[31] Data such as name and address of the user, address of localization of telecommunication device, MSISDN, IMSI, IMEI or ESN number with regard to mobile devices; IP address, name and address of the user, address MAC with regard to access to Internet.

[32] O.J. No 110, item 1052.

(G) Internationalisation

(1) Does domestic law apply to data entered into the internet abroad? Is there a requirement of "double criminality" with respect to entering data from abroad?

Depending on the circumstances, Polish law may apply to data entered abroad. This is due to the fact that with respect to cybercrime general rules on jurisdiction apply.

Therefore, a cybercrime committed by a Polish national may be prosecuted on the basis of the Polish law provided the behavior is also prohibited in the place of its commission (Art. 109 and Art. 111 para 1 PC). Furthermore, if a foreigner commits a cybercrime he may be prosecuted in Poland, provided the "double criminality" requirement is fulfilled and that the crime is aimed against an interest of the Polish state, Polish national, Polish legal person or an act of a terrorist character (Art. 110 para 1 and Art. 111 para 1 PC).

In some cases the requirement of "double criminality" does not apply, irrespective of the nationality of the perpetrator. It is not necessary if a committed crime was aimed at the internal or external safety of Poland, at Polish offices or public officials, at Polish important economic interests. The requirement does not apply if a crime was a crime of false testimony before a Polish office or if it was a crime thanks to which the perpetrator gained a material benefit (even indirectly) on the Polish territory (Art. 112 PC).

In addition, the "double criminality" requirement does not apply in cases of crimes covered by the universal jurisdiction (Art. 113 PC).

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

The Polish legislation has changed to a great extent under the influence of international legal instruments. Several new types of crimes were adopted to the Penal Code in 2004[33] in order to implement the Council of Europe Cybercrime Convention, which was signed by Poland on 23 November 2001. Second great series of amendments to the Penal Code was adopted in 2008[34] in order to implement several framework decisions, two out of which have referred to cybercrime: the Council Framework Decision 2004/68/JHA of 22 December 2003 on combating the sexual exploitation of children and child pornography and the Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems[35].

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

Yes, Polish representatives take part in work of the UN intergovernmental expert group on cybercrime.

---

[33] Act of 18 March 2004 amending the Penal Code and several other statutory acts, O.J. No 69, item 626, entered into force on 1 May 2004.

[34] Act of 24 October 2008 amending the Penal Code and several other statutory acts, O.J. No 214, item 1344, entered into force on 18 December 2008.

[35] See more on this implementation in F. Radoniewicz, Ujęcie cyberprzestępstw w Kodeksie karnym z 1997 roku a postanowienia decyzji ramowej Rady 2005/222/WSiSW w sprawie ataków na systemy informatyczne, Ius Novum 2009, No 1, p. 48-69.

(H) Future developments

Please indicate current trends of legislation and legal debate in your country concerning ICT and internet crime.

There is hardly any debate on ICT and Internet crime in Poland, therefore it is difficult to indicate any current or future trends of legislation in this respect.