Cybercrime Legislation in Poland

by
Professor dr. Andrzej Adamski,
Chair of Criminal Law and Criminal Policy
Faculty of Law and Administration
Nicolaus Copernicus University,
Toruń, Poland

Table of contents

I. Introduction: Cybercrime and Cybercrime Legislation in Poland
1. Definitions
2. Historical development of cybercrime legislation
3. Ratification of the CoE Convention on Cybercrime
4. General development of cybercrime

II. Substantive criminal law
1. Offences against the confidentiality, integrity, and availability of computer system
    1.1. Illegal access to computer system
    1.2. Illegal interception
    1.3. Data interference
    1.4. System interference
    1.5. Misuses of devices
2. Computer-related traditional offences
    2.1. Computer-related forgery
    2.2. Computer related-fraud
3. Illegal content
    3.1. Child pornography
    3.2. Racism and xenophobia
4. Infringements of copyright and related rights
5. Privacy (or "data protection") offences
6. Liability of Internet service providers

III. Criminal procedure

1. Extended search of information systems
2. Seizure of data
3. Preservation of data
4. Retention of data
5. Production order
6. Real-time collection of traffic data
7. Interception of content data

IV. Evaluation and Summary
Annex

I. Introduction: Cybercrime and Cybercrime Legislation in Poland

1. Definitions

Computer crime and cybercrime are not legal notions in Poland. These terms do not appear in the body of substantive criminal law at all. An ancillary definition of "cybercrime" is provided by the Minister of Justice regulation concerning the European Arrest Warrant[1]. It has a narrow meaning referring to acts against the protection of computer data which are gathered, stored, processed or transmitted in the information system. Criminological definitions usually have a broader meaning and are used as an umbrella term that covers all crimes related to computer data, committed against, on and/or throughout information systems, including computer networks, especially the Internet.

As opposed to the Council of Europe Convention on Cybercrime (Article 1), the Polish Penal Code does not comprise a definition of the terms "computer system" or "computer data", despite the fact that such terms are used in a description of cybercrime offences.[2] The said definitions are also not covered by the Act of 2008 aimed at unification of computer terminology in the Polish legal system[3]. A more general problem, still under discussion in Poland in the context of constitutional law, concerns a direct application of definitions laid down in the ratified international conventions by the courts.

2. Historical development of cybercrime legislation

As in most other countries, computer crime legislation in Poland has a relatively short history. It started to be drafted by the Criminal Law Reform Commission as an integral part

[1] Rozporządzenie Ministra Sprawiedliwości z 20 kwietnia 2004 r. w sprawie europejskiego nakazu aresztowania, Dziennik Ustaw Nr 73, poz. 664 [Regulation of the Minister of Justice of 20 April 2004 on the European Arrest Warrant, *Journal of Laws 2004, No.73, item 664*]

[2] The National Office of the Public Prosecution Service is in favor of implementation of Article 1 of the Convention into the Polish Penal Code. Such a position has been taken by this highest unit of the Prosecution Service during the consultations on ratification of the Council of Europe Convention on Cybercrime (Memorandum of 23 May 2008, PR I 078-53/08).

[3] Ustawa z dnia 4 września 2008 r. o zmianie ustaw w celu ujednolicenia terminologii informatycznej, Dz. U. Nr 171, poz. 1056 [Law of 4 September 2008 on Standarisation of IT-related Terminology in the Laws, *Journal of Laws 2008, No.171, item 1056*].

of a new penal code in the early 90's.[4] First public debate on computer crime problem took place on the occasion of an international conference "Legal aspects of computer-related abuse", organised under the aegis of the Council of Europe in Poznan in 1994.[5] Three years later, most of computer-related infringements that compose "a minimum list" of the 1989 Council of Europe recommendation were criminalized under the Polish Penal Code of 1997.[6]

This code represents a "young generation" of the European criminal codes that went into force already in the Information Age[7]. Perhaps for this reason, its specific part contains a chapter entitled "Offences Against the Protection of Information", which corresponds with the proposal set forth in the literature by Professor Ulrich Sieber.[8] Originally, this chapter has included four types of offences against confidentiality, integrity and availability of computer data and systems. These were: *data espionage* (Article 267 § 1), *computer eavesdropping* (Article 267 § 2), *data interference* (Article 268 § 2), and *computer sabotage* (article 269 § 1 and 2). A number of specific provisions, such as those on *computer fraud* (article 287), *unauthorised reproduction of a protected computer programme* (Article 278 § 2), *handling of illegally copied software* (Article 293 § 1), and *telecommunication fraud* (Article 285) were included into the category of offences against property. A legal definition of document (Article 115 § 14) has also been extended in order to make prosecution of *computer forgery* possible. In addition, such specific ICT-related offences like *computer espionage* (Article 130 § 2) and *causing a general hazard as a result of interference with automatic data processing* (Article 165 § 1 point 4) were introduced to the Penal Code.

The list of computer offences has expanded in size pursuant the 2004 amendment of the Penal Code.[9] This legal change was related to accession of Poland to the European Union and it was aimed at harmonisation of Polish criminal legislation with the Council of

[4] Kazimierz Buchala, Poland, (in:) Ulrich Sieber (ed.) Information Technology Crime. National Legislations and International Initiatives, Carl Heymans Verlag KG, Köln,Berlin,Bonn, München 1994, p. 382.

[5] Andrzej Adamski (red.), Prawne aspekty nadużyć popełnianych z wykorzystaniem nowoczesnych technologii przetwarzania informacji, Materiały z konferencji naukowej [Legal Aspects of Computer-Related Abuse, Proceedings of the International Conference], Poznań, 20-22 kwietnia 1994, Towarzystwo Naukowe Organizacji i Kierownictwa „Dom Organizatora", Toruń 1994.

[6] Computer-Related Crime. Recommendation No.R (89) on computer-related crime and final report of the European Committee, Strasbourg 1990.

[7] The Penal Code of 1997 went into force on 1 September 1998.

[8] Prof. Dr. Ulrich Sieber, The Legal Aspects of Computer Crime. Report at The Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders Havana, Cuba August 27–September 7, 1990, p.16.

[9] Ustawa z 18 marca 2004 r. o zmianie ustawy - Kodeks karny, ustawy - Kodeks postępowania karnego oraz ustawy - Kodeks wykroczeń (Dz. U. Nr 69, poz.626) [The Penal Code Amendment of 18 March 2004].

Europe Convention on Cybercrime (hereinafter the CoC). In effect, three new CIA offences: *system interference* (Article 269a), *misuse of devices* (Article 269b), and (once again) *data interference* (Article 268a) were introduced to the Penal Code. Simultaneously, the possession of child pornography was prohibited (Article 202) and a wording of some already existing provisions on computer-related offences was slightly modified by inserting the term "computer data" instead of "information", or "the record on an electronic information carrier".[10] Intended implementation of the CoC has also affected procedural regulations. Some specific procedural measures envisaged by the CoC were adopted to the Code of Criminal Procedure.[11]

The most recent legal change of cyber criminal law took place in 2008 in order to implement the regulations contained in two Framework Decisions to the legal system of Poland[12]. This goal was accomplished in the case of criminalisation of *hacking* (Article 267 § 2) and the so-called *virtual child pornography* (Article 202 § 5) in the Penal Code.

3. Ratification of the CoE Convention on Cybercrime

The Council of Europe Convention on Cybercrime is still awaiting ratification in Poland. Poland signed this international treaty on 23 November 2001 in Budapest and subsequently took steps to implement its provisions in 2004, though has not ratified it. The ratification procedure commenced by the Ministry of Justice in May 2008 is still pending due to not fully solved implementation problems. According to a memorandum obtained from the Department of International Cooperation and European Law of the Ministry of Justice, the only inconsistency concerns the child pornography regulation.[13] Article 202 § 4a of the Penal Code sets a lower age-limit of a child protection against exploitation for pornography than it is required (as a minimum) under Article 9 (3) of the Convention.

[10] Articles 165§ 1 point 4 and 287 § 1 of the Penal Code.

[11] See infra, part III.

[12] Ustawa z dnia 24 października 2008 r. o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw (Dz. U. Nr 214, poz. 1344) [The Penal Code Amendment of 24 October 2008].

[13] Ministerstwo Sprawiedliwości, Departament Współpracy Międzynarodowej i Prawa Europejskiego, Notatka w sprawie zgodności prawa polskiego z Konwencją Rady Europy o Cyberprzestępczości z dnia 12 sierpnia 2009 r., DWM V 025-5/08 [Memorandum of the Department of International Cooperation and European Law of the Ministry of Justice on the Consistency of Polish Law with the Council of Europe Convention on Cybercrime]

However, in the opinion of the present author, there are some other, more significant gaps in the domestic law of Poland with regard to the CoC. These discrepancies, which concern in particular the criminal procedure law regulations, ought to be removed before ratification of the CoC.

4 . General development of cybercrime

Since 1 September 1998, Polish criminal law allows the prosecution of certain specific violations of computer security, as well as a number of computer-related offences. However, the effect this has had in practice is difficult to gauge on the basis of the criminal statistics. As commonly known, these statistics provide rather unreliable record of criminal acts that have actually been committed. Furthermore, criminal statistics are often inaccurate measure of the recorded crime for a number of reasons. One of them must be mentioned in the present context.

The police and court statistics are based on the classifications of the Penal Code, which does not distinguish specific types of cybercrime, such as internet auction fraud, in a separate provision. As a result, crime statistics often fail to provide an accurate number of cybercrimes recorded under a given provision, which may also cover other, IT-unrelated behaviours. This is particularly true with regard do such offences as the illegal access (Article 267 § 1), illegal interception (Article 267 § 3), data interception (Article 268§ 2), racism and xenophobia (Article 256 of the Penal Code) and copyrights and related rights infringements (Articles 116-118 of the Law of February 4, 1994, on Copyright and Neighbouring Rights). Thus, not all the figures provided in table no. 1 correspond to cybercrimes and some of their categories (e.g., unauthorised access and interception, data interference or copyright offrnces) are only partly reflected by the statistics given below. Therefore, statistics presented below are of limited value as a reliable indicator of the official reaction to cybercrime and should be treated in this respect with caution.

Table no. 1. Cybercrimes known to the Police (1999–2012[14])

Year	Unauthorized access to the system and/or interception of information[15]	Data interference[16]	Computer sabotage[17]	System interference[18]	Misuses of devices[19]	Computer fraud[20]	Copyright offences[21]	Pornography[22]
2012	1513	884	5	30	27	n.a.	10481	1886
2011	948	629	5	30	29	n.a.	10551	2265
2010	1102	479	0	18	71	n.a.	20983	939
2009	645	1115	2	243	18	n.a.	18516	1967
2008	505	249	2	13	12	404	9748	1209
2007	384	168	0	11	4	492	12422	697
2006	370	136	4	19	9	444	10504	719
2005	260	98	3	1	6	568	9735	366
2004	248	89	0	-	-	220	13976	178
2003	232	138	2	-	-	168	11270	147
2002	215	167	12	-	-	368	11991	112
2001	175	118	5	-	-	279	9590	90
2000	240	48	5	-	-	323	4064	79
1999	113	49	3	-	-	217	2322	68

Nevertheless, even a cursory glance at the figures presented above allows for one general observation concerning the way a cybercrime is being handled by the law enforcement and criminal justice authorities in Poland.

Two basic categories of cybercrime: those against traditional legal interests (e.g. property) and the modern one (e.g. confidentiality, integrity and availability of data/system) are differently perceived and reacted hereupon by their victims and the law enfocement

[14] Statistical data were updated in February 2014.
[15] Article 267§ 1-3 PC
[16] Article 268 § 1-3, and Article 268a PC
[17] Article 269 § 1-2 PC
[18] Article 269a PC
[19] Article 269b PC
[20] Article 287 § 1-2 PC
[21] Articles 116-118 of the Law of February 4, 1994, on Copyright and Neighbouring Rights
[22] Article 202 § 1-4 PC

authorities. It is rather not a coincidence that Internet-related frauds are more eagerly prosecuted in Poland than computer security offences.

Table no. 2 Internet- related offences (N= 658) prosecuted in Poland (2001-2002) [23]

OFFENCES AGAINST SECURITY OF DATA AND SYSTEMS		OTHER INTERNET-RELATED OFFENCES	
Type of offence	Number of cases	Type of offence	Number of cases
Hacking and interception	11	Internet auction fraud	524 (79%)
Data interference	11	Copyright infringments	31 (4,7%)
Computer sabotage	1	Defamation	17 (2,5%)
		Pornography	16 (2,4%)
		Threats	13 (1,9%)
		Other offences	34 (5,1%)
Total:	**23 (3,4%)**	Total:	**635 (96,6%)**

As the research shows (table no.2) out of 658 cybercrime cases prosecuted in Poland in 2001-2002, most of them (79 %) were frauds related with Internet auctions. CIA offences have constituted only a small part (3,4 %) of all Internet-related cases under prosecution. However, in reality, computer security incidents emerging from the Polish domain of the Internet are counted in tens of thousands, as the yearly reports of the Polish Telecom Security Incident Response Team show it.[24]

An increase in the Internet auction frauds is a visible tendency in the last years. A survey carried out by the National Prosecution Service in 2007 has disclosed that 8920 cases of fraud committed on the Internet auction sites were prosecuted in Poland during the 2006 and the first half of 2007. Approximately - 1700% rate of increase since 2001-2002.

[23] Ryszard Stefański, Barbara Świątkiewicz, Internet Offences in Poland: Analysis of the practice (in:) J.C. Ferré Olive, E.Musco, B.Kunicka-Michalska, J.A.Cabral at al., Grotius II Penal Programme. Penal Legislation in the Fight Against Financial Crimes, Fraud and Corruption, Computer Fraud and Internet Crimes, Universidad de Salamanca, 2004.

[24] Incident handling, statistics and procedures, Warsaw, May 2003, http://www.terena.nl/tech/task-forces/tf-csirt/meeting9/nazar-polish-telecom.pdf

II. Substantive criminal law

1. Offences against the confidentiality, integrity, and availability of a computer system

All offences against computer security are within chapter XXXIII of the Penal Code, ("Offences Against the Protection of Information"). This chapter includes eight basic provisions (Articles 265-269b) protecting the main features of information security, i.e., confidentiality, integrity and availability. Besides traditional offences against secrecy of the State (Article 265) and other official secrecy (Article 266) there are penal provisions related to offences defined in the Council of Europe Convention on Cybercrime (Chapter II, Section 1 Title 1) as the crimes of illegal access (Article 2), illegal interception (Article 3), data and system interference (Articles 4 and 5) and misuse of devices (Article 6).

Polish Penal Code provides a wide range of offences that specifically relate to a computer system and data as the objects of offending. The following offences against confidentiality, integrity and availability of computer data and systems can be distinguished:

- illegal access to a computer system (article 267 § 1 and 2),
- illegal interception (article 267 § 3)
- data interference (articles 268 and 268a)
- system interference (articles 269 and 269a)
- misuse of devices (article 269b)

Most of CIA offences are prosecuted upon the complaint of the injured person. So the criminal proceedings cannot be initiated without the injured person lodging a complaint with a state prosecution office. Since that moment these offences are prosecuted *ex officio*. However, the injured person has a right to change his/her decision and can withdraw a complaint before a trial begins, provided that the public prosecutor consents.

Only computer sabotage – article 269, and misuse of devices – article 269b are the offences prosecuted *ex officio*, i.e. pursuant public accusation. Under the legality principle, to which

the Polish criminal justice system formally adheres, the police and prosecutors have a duty to investigate and prosecute all known offences and offenders. One should note that the Penal Code defines an offence as "a socially harmful act" prohibited by the criminal law. This definition allows the police and the public prosecutor to have de facto discretion on the decision of whether a minor act is considered a formal violation of the law, to be labelled an offence and prosecuted.

1.1. Illegal access to a computer system

The article 2 of the CoC is based on the assumption that '*the mere unauthorised intrusion, i.e. "hacking", "cracking" or "computer trespass" should in principle be illegal in itself*'.

Initially this approach was not adopted in Poland. Instead, a traditional concept of the secrecy of correspondence was used as a general basis for the protection of various kinds of information, including data stored on computers. Thus, confidentiality of digitalized information rather than integrity of a computer system was at stake, as reflected by the provision of Article 267 § 1 of the Penal Code in its original version.[25] In principle, under this regulation an unauthorised access to a computer system *per se* did not lead to criminal liability. A hacker was subject to such liability only if after a successful infringement of security measures he had obtained information to which he was not entitled. In other words, the offence was committed when the information stored in the system and not the system itself was compromised. In effect, such violations of integrity of a computer system, as taking control over the compromised system for further attacks on other systems, or just for fun, remain beyond the scope of penal sanction of Article 267 § 1 of the Penal Code.

This legal loophole was patched in 2008, so at present a "pure" hacking or an unauthorised access to a computer system is subject to penalty in Poland. There are even two legal grounds for that in the Penal Code. Under amended Article 267 § 1 of the Penal Code, it is now a criminal offence to get an unauthorised access to information stored on a

[25] Article 267 § 1 of the Penal Code before the amendment of 2008: Whoever, without being authorised to do so, acquires information not destined for him, by opening a sealed letter, or connecting to a wire that transmits information or by breaching electronic, magnetic or other special protection for that information, shall be subject to a fine, the penalty of restriction of liberty or the penalty of deprivation of liberty for up to 2 years.

computer system following breaking or circumventing its security measures.[26] On the other hand, a newly established provision (Article 267§ 2) penalizes anyone who, without authorisation obtains access to the whole or any part of an information system.[27] A wording of this latter provision is very close to that of Article 2 of the 2005 Framework decision and in fact implements it literally. However, an official justification for this legislative change has emphasised pragmatic rather then political reasons, stressing the usefulness of punishability of "pure access" as a legal weapon against distributors of spyware and other malicious software used for taking control over infected computers.[28] Because such purpose of penalisation has not explicitly been reflected in the law, there are doubts whether a legislative technique used complies with the principle of legality or not[29].

The concept of "unauthorised access to a computer system" is an ambiguous one, and as experience based on comparative law shows, it gives a great deal of flexibility in the application of penal law, particularly if the notion of "unauthorised access" is not legally defined.[30] Such omission of the legislator opens a gate for various legal interpretations in judicial practice. Some of them might be very "innovative" in the context of rapidly changing technology. For instance, the said regulation may be used for the prosecution of "piggybacking" in a wireless environment and a number of other minor infringements of computer security that do not deserve punishment, nor intervention of the criminal justice authorities. A foggy language of criminal law is unacceptable in view of its fundamental guarantees with the principle *nullum crimen sine lege certa* in the forefront. Therefore a

---

[26] Article 267 § 1 of the Penal Code as amended in 2008: Whoever, without being authorised to do so, acquires access to information not destined for him, by opening a sealed letter, or connecting to a telecommunication network or by breaching or circumventing electronic, magnetic, computer or other special protection for that information, shall be subject to a fine, the penalty of restriction of liberty or the penalty of deprivation of liberty for up to 2 years.
A similar approach has been employed in Germany with Law No. 1786/2007 (*Strafrechtsänderungsgesets zur Bekämpfung der Computerkriminalität in Kraft*) in order to harmonise § 202a of the German Penal Code with the CoC (Article 2).

[27] Article 267 § 2. The same punishment shall be imposed on anyone, who, without authorisation, obtains access to the whole or any part of an information system.

[28] Reasoning of the draft amendment of the Penal Code of 28 October 2008.

[29] Andrzej Adamski, Opinia do projektu ustawy z druku nr 458 Rządowy projekt ustawy o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw (Opinion on the bill amendment of the Penal Code for the Office of Legal Analyses of the Sejm) http://orka.sejm.gov.pl/rexdomk6.nsf/Opdodr?OpenPage&nr=458

[30] See: O.Kerr, Cybercrime's Scope: Interpreting 'Access' and 'Authorization' in Computer Misuse Statutes, *New York University Law Review*, Vol. 78, No. 5, November 2003.

recent over-criminalisation of hacking under the Polish Penal Code face criticism in the literature.[31]

1.2. Illegal interception

According to Article 3 CoC, the interception of computer data should be punished only if committed without right and by using technical means. Article 267 §3 of the Penal Code goes beyond the provision of CoC, criminalising the installation or use of a device or computer software in order to intercept information to which the perpetrator is not authorised. Furthermore, it refers to "information", not to computer data, and gives a more general description of the illegal act than Article 3 CoC. In particular there is no reference to "non-public transmissions of data" or "electromagnetic emissions". Nevertheless, all forms of usage of technical means to intercept passwords, keystrokes, or information send by e-mail and through other channels of electronic communication are covered by Article 267 § 3, provided that it is done without authorisation. An interpretation of this provision based on *argumentum a minori ad maius* would lead to the conclusion that interception of data flows, including its non-public transmissions are penalised as well. [32]

Before the 2008 amendment of the Penal Code, this provision did not mention computer programme as an instrument of offending. As a result, there were different interpretations of this issue in the literature.[33] The present wording of Article 267 § 3 brought these controversies to an end, making a prosecution of malware-based attacks on data confidentiality possible. These may include not only the use of password-sniffers, but any piece of software placed or injected into the victim's system or a publicly accessible website in order to enable the perpetrator to acquire information not intended for him.

---

[31] Andrzej Adamski, Nowe ujęcie cyberprzestępstw w kodeksie karnym – ale czy lepsze? [New frame of cybercrime in the Penal Code –is it better?], *Prawo Teleinformatyczne*, 2007, 3(5), pp. 4-8.

[32] Article 267 § 3**.** The same punishment shall be imposed on anyone, who, in order to acquire information to which he is not authorised to access, installs or uses tapping, visual detection or other equipment or computer software.

[33] See: Włodzimierz Wróbel, [in:] Andrzej Zoll (ed.) Kodeks karny. Część szczególna. Komentarz [The Penal Code. Special Part. Commentary], vol.2, Kraków, Zakamycze 1999, p. 1009; Andrzej Adamski, Prawo karne komputerowe [Criminal Law and Computers], C. H. Beck, Warszawa 2000, p. 58.

One of the side effects of the 2008 amendment is an overlap of paragraphs 1 and 3 of Article 267. For instance, the one who installs a tapping device in order to intercept a conversation (§ 2), immediately acquires access to it, especially while connecting to a telecommunication network (§ 1). On the other hand, a description of the offence in question is broad enough to cover trivial or anecdotal incidents, including those which are not computer-related, such as for instance a binocular assisted voyeurism.

The penal sanctions for illegal access and illegal interception are the same. The perpetrator of these offences faces an alternative sanction of a fine, the penalty of restriction of liberty or the penalty of deprivation of liberty up to 2 years. Such penalties apply also for a disclosure to the other person of the information unlawfully obtained in a way prohibited in paragraphs 1-3 of the Article 267.

1.3. Data interference

Intentional manipulation of computer data is subject to extensive penalisation in Poland. Two penal provisions directly address this issue (Articles 268 § 2 and 268a). Additionally, unauthorized changing, deleting, impairing and adding of computer data constitute legal elements of some other offences, like system interference offence (article 269a), computer sabotage (article 269) and computer fraud (article 287).

The original function of article 268 § 2 of the Penal Code was the protection of an "essential" information against rendering its retrieval impossible, or very difficult one, due to the data destruction or manipulation.[34] Under this legal construction, the criminal liability of the perpetrator was dependent on the victim's assiduousness in keeping back-up copies of his data. Such limitation is not known to Article 4 of the CoE convention, which implies that data interference offence shall be deemed as completed whenever data is altered or destroyed, regardless of whether there are back-up copies or not. An effort to implement

[34] Article 268 § 1. Whoever, being unauthorised, destroys, impairs, deletes or alters a record of essential information or otherwise prevents or makes it significantly difficult for an authorised person to obtain knowledge of that information, shall be subject to a fine, the penalty of restriction of liberty or the penalty of deprivation of liberty for up to 2 years.
§ 2. If the act specified in § 1 concerns the record on an electronic information carrier, the perpetrator shall be subject to the penalty of deprivation of liberty for up to 3 years.
§ 3. Whoever, by committing an act specified in § 1 or 2, causes a significant loss of property, shall be subject to the penalty of deprivation of liberty for a term of between 3 months and 5 years.

article 4 of the CoC to the Penal Code was not, however, successful. The new provision of article 268a has, for unknown reasons, been tailored by the legislator in a way which does not fully correspond to the Article 4 CoC. Instead of protecting data against manipulations, the wording of article 268a puts emphasis on the protection of access to the data itself.[35] Therefore, some authors are of the opinion that the primary function of this provision is to safeguard access to databases[36], and not the protection of data integrity. Nevertheless, the interpretation of article 268a may allow for prosecution of attacks against data integrity, including incidents of malicious code infections and website defacements, even if they result only in slight modifications of data.

1.4. System interference

System interference aims at criminalizing acts of computer sabotage and the resultant loss of availability of the information service. The offence covers intentional hindering of a lawful use of computer systems, including telecommunication facilities, by using or influencing computer data. Such legal regulations may criminalize various forms of denial of service attacks (DoS, DDoS) that may stop, for instance, a website from communication with other computers.

In Poland the system interference is penalised in various provisions of the Penal Code, depending on the character of the data and on the interference. The strongest protection of data and systems availability is provided by Article 269 § 1 which concerns data of particular significance for national defence, transport safety, operation of the government, or other state authority or local government. The maximum penalty for the intentional hindering of processing or transmission of such data is 8 years of imprisonment.[37] Under this provision, a denial of service attack can be considered criminal

[35] Art. 268a. § 1. Whoever, without being authorized to do so, destroys, damages, removes, changes or makes an access to computer data difficult, or in a significant degree disrupts or prevents automatic processing, gathering or transmission of such data, shall be subject to the penalty of deprivation of liberty for up to 3 years.
§ 2. Whoever, by committing an act specified in §1, causes a significant loss of property
shall be subject to the penalty of deprivation of liberty for a term of between 3 months and 5 years.

[36] Andrzej Marek, Kodeks karny. Komentarz [The Penal Code. Commentary], Warszawa 2005, p. 556.

[37] 269. § 1. Whoever destroys, deletes or changes a record on an electronic information carrier, having a particular significance for national defence, transport safety, operation of the government or other state authority or local government, or interferes with or prevents automatic collection and transmission of such information, shall be subject to the penalty of deprivation of liberty for a term of between 6 months and 8 years.

offence mostly when directed at servers in the government domain (*gov*). However, the legal requirements concerning the sensitive nature of data that are protected under Article 269 make the commission of this offence against a government website hardly possible.

System interference is also penalised by two other provisions, inserted in the Penal Code in 2004 in order to implement articles 4 and 5 of the CoE convention. Article 269a criminalises serious hindering of functioning of a computer system or computer network under the penalty of deprivation of liberty of up to 5 years. [38] A very similar prohibition is provided by Article 268a (*in fine*) with the penalty of deprivation of liberty of up to 3 years for anyone who seriously hinders core functions of computer systems like processing, gathering or transmission of computer data. The penalty increases up to 5 years if the offence results in a significant loss of property.

This double protection of computer data and systems availability is a classic superfluousness of legal regulation. Therefore a proposal was made to remove one of this provision from the Penal Code.[39]

1.5. Misuses of devices (Article 269b)

In 2004 a controversial "hacker's tools" provision of Article 6 of the CoE Convention was implemented with considerable modifications to the Penal Code (Article 269b). From the very beginning a main dilemma related with this regulation was how to distinguish the use, import, production, etc. of such devices for both legitimate and illegitimate purposes. During the drafting process of the CoE Convention a clause excluding criminal liability for this offence was added to Article 6 in order to make clear that tools created for the authorised testing or the protection of a computer system are not covered by the provision. A similar exclusionary rule was not adopted by the Polish legislator.

---

§ 2. The same penalty should apply to a person who commits offences mentioned in § 1, by destroying or replacing the information carrier or by destroying or damaging a device serving for automatic processing, gathering or transferring of information data.

[38] Art. 269a. Whoever, without being authorized to do so, through transmitting, destroying, deleting, impairing or changing computer data, causes significant interference with functioning of a computer system or network, shall be subject to the penalty of deprivation of liberty for a term of between 3 months to 5 years.

[39] Andrzej Adamski , Opinia do projektu ustawy ..(Opinion on the bill amendment..), *supra* note 18 at 5.

Article 269b (1) of the Penal Code which seeks to implement the paragraph 1(a) of Article 6 of CoE convention consists of two parts. The first part of this provision criminalises the production, acquiring, sale and making available devices, including computer programmes, adapted for the purpose of commission of offences against computer security (267 § 3, 268a § 1 or § 2 in connection with § 1, 269 § 2 or 269a) and public safety (articles 165§ 1 point 4)[40]. This part of the provision makes no reference to the unauthorised access offence (Article 267 § 1 and § 2), thus it is not consistent with the Convention.

The second part of Article 269b §1 tends to reflect the paragraph 1(b) of Article 6 of CoE Convention, but this effort is not successful. In fact, in a description of prohibited act an important normative element is missing. There is no requirement that conducts related with computer passwords or access codes have to be performed for illegal purposes, i.e. with the intent of a commission of offences indicated above. Deficient construction of Article 269b leads to over-criminalisation of internet users. Literal interpretation of this provision, in particular a phrase "acquires of other data that allow for the access to information stored in a computer system" cover such "innocent" internet activity as googling [use of a web browser].

Misuse of devices is largely based on the concept of a preparatory offence. As such it extends the scope of criminal liability to a stage preceding an attempt of the commission of CIA offence. It also requires an offender who prepares the commission of an offence to act purposefully, i.e., with a specific intent.

All conducts that are specified in paragraph 1 (a) of Article 6 of the CoE convention concern various items which have to be designed, adapted or used for the purpose of committing CIA offences. As opposed to the CoE convention (article 6), Polish Penal Code (article 269b) does not require the specific (i.e. direct) intent for the commission of the act. Since indirect intent (*dolus eventualis*) is sufficient, theoretically any publication of exploits or other dual-use software on the web page by the one who does this "exclusively for educational purposes" would bring the author of such disclaimer before the court under the charge of violation of

[40] Article 165 § 1 point 4 of the Penal Code prohibits intentional causing of general hazard to the life or health of many persons or property of a considerable value by interference with automatic data processing.

article 269b. For the same reason, computer security experts (e.g. virus analysts) or network administrators run the risk of prosecution for dealing with "hacker tools", unless they are able to prove their *bona fide*. Unfortunately, the wording of article 269b is not precise enough to challenge such interpretations definitely.[41]

2. Computer-related traditional offences

2.1. Computer-related forgery

There is no specific provision on computer-related forgery in the special part of the 1997 Penal Code. Polish legislator did not consider the idea of computer forgery a separate type of offence protecting legal interests of security and reliability of electronic data that have relevance for legal and economic relations. Another, more general approach has been adopted in Poland in order to provide criminal law protection of electronic documents against forgery. A legal definition of "document", included in the general part of the Code (article 115 § 14), was amended to enable application of traditional legal provisions on offences against documents for prosecution of their modern, electronic or digital forms. Initially, the document was defined in the Penal Code as "any object or record on a computer data carrier…". In 2004 this definition was replaced by another one ("any object or other recorded information carrier"… [42]) which provides a fertile ground for various interpretations. Generally speaking, there is no consensus among authors as how to construe a core part of this definition, however majority of them share the opinion that under the Penal Code a document by virtue of its nature is a tangible item.[43] Since a document must have a physical substrate, computer data is not recognised as a carrier of the information, and, in

[41] Krzysztof Gienas, Hak na hakera [Catch on a Hacker], „*Rzeczpospolita*" (29.07.2005); Andrzej Adamski, Cyberprzestępczość - aspekty prawne i kryminologiczne [Cybercime – Legal and Criminological Aspects], *Studia Prawnicze* 2005 nr 4 (167), pp. 60-61.

[42] A provision of paragraph 14 of Article 115 reads: A document is any object or other recorded information carrier to which is attached a specific right, or which in connection with the subject of its content, constitutes evidence of a right, a legal relationship or a circumstance, which may have legal significance.

[43] Joanna Piórkowska-Flieger, Fałsz dokumentu w polskim prawie karnym [Forgery of Documents in the Polish Criminal Law], Zakamycze, Kraków 2004, pp. 193-194; Beata Mik, Karnomaterialna ochrona dokumentów (zagadnienia wybrane*)* [Criminal Law Protection of Documents (Selected issues), *Prokuratura i Prawo* 2001, nr 4, p. 57, Jarosław Majewski, (in:) Andrzej Zoll (ed.) Kodeks Karny, Część ogólna. Komentarz [The Penal Code. General Part. Commentary] , tom I, Zakamycze, Kraków 2004, p. 1461; Magdalena Budyn-Kulik i inn., Kodeks karny. Praktyczny komentarz [The Penal Code. Practical Commentary], Zakamycze, Kraków 2004.; Andrzej Marek, Kodeks karny. Komentarz [The Peal Code.Commentary], LEX, Warszawa 2007.

consequence, is excluded from the legal definition of the document. So only electronic documents recorded on a floppy disk, CD-rom or hard drive are legally protected against forgery. Such an interpretation implies that unauthorised alteration of an electronic document during its transmission shall not be prosecuted as an offence of forgery.[44] Arguably, any other provision does not apply to this situation, including data interference offence (Article 268a) due to its inadequate definition (see above). In this context the present regulation of computer-related forgery can hardly be find as reasonable and consistent with the international standards.

2.2. Computer related-fraud

A specific provision against computer fraud was introduced to the Penal Code of 1997. A definition of this offence provided in Article 287 is more flexible than the model offence proposed in Article 8 of the CoE Convention. While the latter provision puts an emphasis on the effect caused by an offender (loss of property), there is no such a requirement under the Polish law. According to Article 287, an offence is accomplished at the moment of interference into the data processing by the perpetrator who wants to achieve a financial gain in this way. The actus reus consists in any inputting, altering, deleting of computer data or other unauthorised interference with its processing. The mental element requires specific intent (dolus directus) directed at acquiring a material benefit or causing damage to another party.[45] However, it is not required that the intended effects have to materialize, because they do not belong to elements of this offence. For that reason a completion of computer fraud offence takes place at the moment of interfering with the data integrity or processing, irrespective of the occurrence of economic consequences of these manipulations. It was

[44] Andrzej Adamski, Buszujący w sieci. Cybernowelizacja prawa karnego [Scouring over the Net. Cyber-amendment to the Penal Code], „Rzeczpospolita" (27.10.2003); Piotr Ochman, Spór o pojęcie dokumentu w prawie karnym [Controversy over the Definition of Document in Criminal Law] , *Prokuratura i Prawo* 2009, no. 1 , p. 34.

[45] Article 287. § 1. Whoever, in order to gain material benefits or cause the other person material damage, affects automatic processing, gathering or transmitting computer data , or changes or deletes record or introduces a new record of computer data, without being authorised to do so, shall be subject to the penalty of deprivation of liberty for a term of between 3 months and 5 years.
§ 2**.** In the event that the act is of a lesser significance, the perpetrator shall be subject to a fine, the penalty of restriction of liberty or the penalty of deprivation of liberty for up to one year.
§ 3**.** If the fraud has been committed to the detriment of a next of kin, the prosecution shall occur on a motion of the injured person.

believed that such construction of the offence will facilitate prosecution of computer frauds.[46] Current research of prosecutorial practice has shown, however, that this is not the case.[47] Article 287 constitutes the so-called conduct crime.[48] As such its provision is applied by prosecutors not as a sole but mostly ancillary legal basis of qualification of an offender's act. A factor which triggers the reaction of a victim of computer-related fraud and has an influence on the decision to prosecute this offence is an occurrence of economic loss caused by the offender. The legal provision of Article 287 in its current shape would only reflect a *modus operandi* of the offender, not a whole criminal content of the act he has committed. For that reason one may conclude that the goal of criminalisation of computer-related fraud has not been fully achieved.[49]

3. Illegal content

3.1. Child pornography

In Poland the list of illicit acts related to child pornography is quite extensive and it includes its production, dissemination, public presentation, procuring, recording as well as storing and possession (Article 202 § 3-5 of the Penal Code).[50] In addition, the law makes a

[46] Kazimierz Buchała, Przestępstwa przeciwko ochronie informacji i oszustwo komputerowe[Offences Against the Protection of Information and Computer Fraud] , (w:) Materiały z konferencji naukowej [Legal Aspects of Computer-Related Abuse, Proceedings of the International Conference], Poznań, 20-22 kwietnia 1994, Towarzystwo Naukowe Organizacji i Kierownictwa „Dom Organizatora", Toruń 1994 , p. 136.

[47] Ryszard A. Stefański, Oszustwa komputerowe w praktyce polskich organów ścigania [Computer Fraud in the Practice of the Polish Investigation Organs], *Studia Prawnicze* 2006 nr 4 (170), p. 130-132.

[48] Some authors disagree with this view and argue that Article 287 constitutes a result crime, see for instance: Piotr Kardas, Oszustwo komputerowe w kodeksie karnym [Computer Fraud in the Penal Code], *Przegląd Sądowy* 2000, No. 11-12, pp. 71-73.

[49] Andrzej Adamski, Oszustwo komputerowe a oszustwo internetowe [Computer Fraud and Internet Fraud] (w:) Przestępczość teleinformatyczna. Materiały seminaryjne pod red. J.Kosińskiego Wyższa Szkoła Policji, Szczytno 2005, p. 21; Rafał Korczyński, Robert Koszut, „Oszustwo" komputerowe [Computer „Fraud"], *Prokuratura i Prawo* 2002, No.2, pp.32-35.

[50] Article 202 of the Penal Code (child pornography offences)
§ 3. Whoever, for the purpose of dissemination, produces, records, imports or disseminates or presents publicly pornographic material in which a minor is presented, or pornographic material associated with the use of violence or the use of an animal, shall be subject to the penalty of deprivation of liberty for from 6 months to 8 years.
§ 4. Whoever records pornographic content with the participation of a minor under age of 15, shall be subject to the penalty of deprivation of liberty from one to 10 years.
§ 4a.Whoever imports, stores or possesses pornographic content in which a minor under 15 years of age is presented, shall be subject to the penalty of deprivation of liberty for a term of between 3 months to 5 years.
§ 4b.Whoever produces, disseminates, presents, stores or possesses a pornographic content featuring a created or processed image of a minor taking part in a sexual activity, shall be subject to the penalty of fine, limitation of liberty or deprivation of liberty up to 2 years.

distinction between acts committed for the purpose of dissemination of child pornography and for other undefined purposes, including one's own use. The first category of illegal conducts is subject to more severe punishment (imprisonment for 6 months to 8 years) than the other (imprisonment for 3 months to 5 years), however, not without exceptions.[51]

Polish law does not provide any legal definition of pornography in general, and consequently, child pornography is also undefined. The objective of child pornography offences is described in the Penal Code as "pornographic content with the participation of minor". This is a broad concept, not confined only to "visual depiction" (as determined in the CoE Convention and the EU Framework Decision) but encompassing all forms of expression, including literary works and oral presentations.[52] The only exception is a newly established provision of paragraph 4b of Article 202 of the Penal Code which directly refers to an "image" as an object of the offence.

Despite three legislative amendments of child pornography offences in the years of 2004-2008, Polish criminal law does not fully comply with international and European legal standards in this field. The most critical issue, also for the ongoing process of ratification the CoE Budapest Convention, is the age-limit to which the ban on child pornography applies.

In accordance with the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography, and the Council of Europe Convention on Cybercrime, in most countries, legislation on child pornography protects children under the age of 18, regardless of the age of consent to sexual activity, which is normally lower. In Poland, the age of consent is 15 and the law on child pornography protects children under 18. However, this concerns only dissemination or public presentation of child pornography and acts committed for the purpose of its dissemination, including production, recording, acquisition, storing and possessing of pornographic

---

[51] Paragraph 4 of Article 202 of the Penal Code penalises recording of pornographic content with the participation of a minor under age of 15 with imprisonment from 1 to 10 years, whereas the same conduct undertaken for the purpose of dissemination of child pornography is subject to imprisonment from 6 months to 8 years.

[52] In the official Polish translation of the EU Framework Decision of 2004, the definition of child pornography differs from the original English text. The latter reads: '*child pornography' shall mean pornographic material that visually depicts or represents*..., while the former points out that '*child pornography' shall mean pornographic material that contain pornographic content, which depicts or represents*...(„pornografia dziecięca" oznacza materiał zawierający treści pornograficzne, które przedstawia lub prezentuje ..).

content with the participation of a minor. The age-limit is lower in case of recording, procuring, storing and possessing child pornography for a purpose other than dissemination (e.g. for personal use), and amounts to 15 years, which is not in compliance with the CoE Budapest Convention of 2001 (article 9 paragraph 3), the EU Framework Decision of 2004 (article 1) and CoE Lanzarote Convention of 2007 (article 1).[53]

At the first glance, there are considerable differences between the scope of criminalisation of conducts related to child pornography under the CoE Conventions and the EU Framework Decision of 2004 on the one hand, and Polish criminal law on the other. Transmission, offering, supplying and making available are not explicitly criminalised in Poland, as opposed to recording, public presentation and storing which are, in turn, not covered by the European legal instruments of child protection from being sexually abused through production and proliferation of child pornography (table no. 3).

Table no. 3
Comparison of conducts consisting of child pornography offences in the European legal instruments and the Polish Penal Code

CoC 2001	FD 2004	Polish Penal Code of 1997
production	production	production
offering[54]		
	supplying	
		recording
		public presentation
making available[55]	making available	
distribution[56]	distribution, dissemination	dissemination
transmission[57]	transmission	

[53] The CoE Convention on Cybercrime of 2001 and the CoE Convention on the protection of children against sexual abuse of 2007 give the Parties the possibility to lower age-limit protection of children to 16 years or less. The EU Framework Decision of 2004 does not allow MS in child pornography offences to lower the age of protection under 18 years.

[54] "Offering" is intended to cover soliciting others to obtain child pornography. It implies that the person offering the material can actually provide it.

[55] "Making available" is intended to cover the placing of child pornography online for the use of others, e.g. by means of creating child pornography sites. It also covers the creation or compilation of hyperlinks to child pornography sites in order to facilitate access to child pornography

[56] "Distribution" is the active dissemination of the material.

[57] "Transmitting" is sending child pornography through a computer system to another person.

procuring for onself or for another[58]	acquisition	procurment, acquisition
possession	possession	possession
		storage

A closer examination of this issue would reveal that these differences are not semantically significant. For instance, making child pornography available on the Internet by uploading a file with such content to a website results in its public presentation. Making available this same file by means of an ftp server or a hard disk of a computer connected to an e-donkey file sharing system, would be recognised by a Polish judge as its dissemination in view of the Supreme Court interpretation of this term.[59] Some terms used by Polish legislator to define forbidden conducts overlap (e.g. producing and recording, possessing and storing) and one of them ("transmission"), specified in the European legal instruments is missing in Article 202 of the Penal Code.

The mere possession of "real" child pornography was criminalized in Poland in 2004.[60] Initially, this prohibition concerned only pornographic content with the participation of children under the age of 15. In 2005 the ban on possession was extended to the pornographic content with the participation of all minors, regardless of their age, provided that the possessor acts for the purpose of dissemination.[61] In effect**,** recording, procuring, possessing and storing pornographic material with the participation of children between 15 and 18 are legal if the perpetrator acts without the aim of public distribution.

Since the end of 2008 the so-called pseudo[62] and virtual[63] child pornography has been forbidden in Poland.[64] The ban concerns not only production, dissemination, storage and

[58] The term "procuring for oneself or for another" means actively obtaining child pornography, e.g. by downloading it (All definitions after Explanatory Memorandum, 95-97).

[59] The Supreme Court in a ruling dated 16 February 1987 held that dissemination of pornographic materials is meant as making them commonly available. Wyrok Sądu Najwyższego z dnia 16 lutego 1987 r. (WR 28/87), OSNKW 1987 Nr 9-10, poz. 85.

[60] Ustawa z 18 marca 2004 r. o zmianie ustawy - Kodeks karny, ustawy - Kodeks postępowania karnego oraz ustawy - Kodeks wykroczeń (Dz. U. Nr 69, poz.626) [The Penal Code Amendment of 18 March 2004].

[61] Ustawa z 27 lipca 2005 r. o zmianie ustawy –Kodeks karny, ustawy- Kodeks postępowania karnego i ustawy – Kodeks karny wykonawczy (Dz.U. Nr 163, poz. 1363) [The Penal Code Amendment of 27 July 2005].

[62] Pseudo child pornography takes an innocent image of a child and manipulates it (by computer or otherwise) to place the child in a sexual context. This is also known as 'morphing'. Real harm is done by pseudo child pornography because a real child's image was used in the creation process. The morphed image violates

possession but also presentation of pornographic content. The newly adopted provision of paragraph 4b of Article 202 of the Penal Code reads:

> Whoever produces, disseminates, presents, stores or possesses pornographic content featuring of a created or processed image of a minor taking part in a sexual activity, shall be subject to the penalty of fine, limitation of liberty or deprivation of liberty up to 2 years.

As opposed to the European legal instruments, there are no requirements that the image should be "realistic" and concern "non-existent child". Thus, the law allows for an extensive interpretation of this provision, including both images that appear to reflect reality as well as cartoons.

Polish criminal law regulation on child pornography is rather strict in a sense that it does not exclude criminal responsibility under circumstances making it possible according to exclusionary clauses provided for by Article 3 point 2 of the 2004 Framework Decision and Article 9 point 4 of the CoE Convention.

3.2. Racism and xenophobia

Poland have signed the Additional Protocol to the Convention on Cybercrime, concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed Through Computer systems (28 January 2003), but did not ratified it. Four types of offences considered by the Additional Protocol are covered, at least partly, by the Polish legislation.

Dissemination of racist and xenophobic material through computer systems is partly covered by Article 256 of the Penal Code, which foresees criminal responsibility for the public incitement to hatred on the basis of national, ethnic, race or religious differences or

---

the child's dignity, reputation and right to privacy. [after: Michael Walton, Possession of Child Pornography. Background Paper, New South Wales Council for Civil Liberties, January 2005, p.6 http://www.nswccl.org.au/docs/pdf/bp2%202005%20Possess%20Child%20Porn.pdf

[63] Virtual child pornography depicts fictitious children. A 'fictitious child' can be either a pure figment of its creator's imagination or an adult actor playing the part of a child.[Id.]

[64] Ustawa z dnia 24 października 2008 r. o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw (Dz. U. Nr 214, poz. 1344) [The Penal Code Amendment of 24 October 2008]

praising of a fascist or other totalitarian system of the state.[65] This offence can be committed through both conventional an electronic means, including web sites, chat rooms, newsgroups or discussion fora.

Threats for racist and xenophobic motives are criminalized under Article 119 § 1 of the Penal Code with imprisonment for 3 months to 5 years.[66]

An insult for racist and xenophobic motives, if committed publicly, is condemned by the Penal Code as a specific offence (Article 257) and sanctioned by imprisonment of up to three years.[67]

As to the last punishable conduct under the Additional Protocol (Denial, gross minimisation, approval or justification of genocide or crimes against humanity) it is partly covered by Article 55 of the Law on the Institute of National Remembrance – Commission for the Prosecution of Crimes against the Polish Nation.[68] Under this provision, anyone who publicly and contrary to facts denies crimes which occurred in particular during the second World War (in particular the Holocaust) is subject to criminal responsibility under a penalty of a fine or the deprivation of liberty of up to three years.

4. Infringements of copyright and related rights

In Poland two basic legal acts do criminalise infringements of copyright and related rights. These are respectively the Copyright and Neighbouring Rights Act of 4 February 1994[69] (further: the Copyright Act), and the 1997 Penal Code. Criminal law protection of legitimate interests of copyright holders in the Penal Code is limited only to computer programmes and

[65] Article 256. Whoever publicly promotes a fascist or other totalitarian system of state or incites hatred based on national, ethnic, race or religious differences or for reason of lack of any religious denomination, shall be subject to a fine, the penalty of restriction of liberty or the penalty of deprivation of liberty for up to 2 years.

[66] Article 119. § 1. Whoever uses violence or makes unlawful threat towards a group of person or a particular individual because or their national, ethnic, political or religious affiliation, or because of their lack of religious beliefs, shall be subject to the penalty of the deprivation of liberty for a term of between 3 months and 5 years.

§ 2. The same punishment shall be imposed on anyone, who incites commission of the offence specified under § 1.

[67] Article 257. Whoever publicly insults a group within the population or a particular person because of his national, ethnic, race or religious affiliation or because of his lack of any religious denomination or for these reasons breaches the personal inviolability of another individual shall be subject to the penalty of deprivation of liberty for up to 3 years.

[68] The Law of December 18, 1998 on the Institute of National Remembrance - Commission for the Prosecution of Crimes against the Polish Nation (Journal of Laws, December 19, 1998) http://www.ipn.gov.pl/portal/en/32/46/Act_on_the_Institute.html

[69] English translation: http://www.mkidn.gov.pl/cps/rde/xbcr/mkid/act_on_copyright.pdf

covers two kinds of infringements: illegal copying of software (article 278 § 2)[70], and handling of "stolen" software (article 293)[71]. These are *ex officio* prosecuted offences what may partly explain relatively high rates of such crimes recorded by the police statistics.[72] The scope of criminalisation of the Copyright Act is broader and encompasses all kinds of protected works and artistic performance against plagiarism, illegal reproduction, dissemination and even purchase of illegal copies of literary, photographic, musical, audio-visual and other protected works (Articles 116-118).

Although none of these provisions employ the exact wording of the TRIPS agreement ("piracy on a commercial scale"), most of them take economic dimension into account. This usually takes form of the aggravation of penalty if a criminal act is committed for the purpose of a financial gain. For example, the Copyright Act makes unauthorised dissemination of another's work an offence (Article 116), but whereas simple dissemination is punishable by two years' imprisonment, the penalty is raised to three years "if the perpetrator commits the act … in order to gain material benefits", and to five years if he has made the offence "a regular source of income".[73]

Under the Copyright Act (Article 50 sec.3)[74], terms "dissemination" and "making available" have similar meaning and can be used interchangeably as far as spreading of protected

[70] Article 278. § 1. Whoever, with the purpose of appropriating, wilfully takes someone else's movable property shall be subject to the penalty of deprivation of liberty for a term of between 3 months and 5 years.

§ 2. The same punishment shall be imposed on anyone, who without the permission of the authorised person acquires someone else's computer software, with the purpose of gaining material benefit.

§ 3. In the event that the act is of a lesser significance, the perpetrator shall be subject to a fine, the penalty of restriction of liberty or the penalty of deprivation of liberty for up to one year.

[71] Article 293. § 1. The provisions of Article 291 and 292 shall be applied accordingly to computer software.

§ 2. The court may decide on the forfeiture of the item specified in § 1 and in Articles 291 and 292, even though it may not be the property of the perpetrator.

[72] In the year 2007 the police statistics recorded over 20.000 incidents of illegal copying and handling of "stolen" software.

[73] Article 116 of the Copyright Act: 1. Whoever, without authorization or against its terms and conditions, disseminates someone else's work, in the original or derivative version, performance, phonogram, videogram or broadcast shall be liable to a fine, restriction of liberty or imprisonment for the period of up to 2 years.

2. If the perpetrator commits the act specified in paragraph 1 above in order to gain material benefits, he shall be liable to imprisonment for the period of up to 3 years.

3. If the perpetrator makes the offence specified in paragraph 1 above a regular source of income or organizes or manages a criminal activity, as specified in paragraph 1, he shall be liable to imprisonment from 6 months up to 5 years.

4. If the perpetrator of the act specified in paragraph 1 above acts unintentionally, he shall be liable to a fine, restriction of liberty or imprisonment for the period of up to one year

[74] Article 50 of the Copyright Act: The separate fields of exploitation shall be, in particular:
/…/

works over the Internet is concerned. A criminal law aspect of this consideration is associated with peer-to-peer file sharing. Uploading files for their exchange or sale on the website, or making them available to other users of file sharing system may lead those who are involved in such activities to criminal responsibility under Article 116 of the Copyright Act. It depends not only on the content of files but also on the technical features and functionality of the file-share programme used.

Each Party to the CoC is obliged to criminalise wilful infringements of copyright and related rights (article 10). Against this background it must be noted that Polish law penalises also some unintentional copyright infringements. This refers to the offence of unlawful dissemination of the work of another (Article 116 sec. 1 of the Copyright Act) as well as the offence of unintentional handling of "stolen" software and other work (Article 293 of the Penal Code, Article 118 sec. 3 of the Copyright Act). In this connection, it can be pointed out that the level of criminal law protection of copyright and related rights in Poland surpasses those which has been set out by the international standards in this field.

5. Privacy (or "data protection") offences

The right to privacy and the right to personal data protection were recognised by Polish Constitution of 1997.[75] The Law on the Protection of Personal Data was adopted in 1997 and came into force in 1998.[76] Respect for privacy and personal data protection is also guaranteed with penal sanctions. Unlike in France or Germany, offences against privacy do not compose a separate chapter in the Polish Penal Code. The criminal law provisions protecting various facets of privacy are dispersed over a special part of the Code and can be found among offences against liberty (chapter XXIII), honour and personal inviolability (chapter XXVII) and the protection of information (chapter XXXIII). The secrecy of

---

3) within the scope of dissemination of the work in a manner other than as specified in Subparagraph 2 -public performance, exhibition, presentation, communication, broadcasting and re-broadcasting, as well as making the work available to the public in a manner allowing every person to have access to such work in a place and at a time of his own choice.

[75] Respectively - Articles 47 and 51 of the Constitution of the Republic of Poland of 2nd April , see: http://www.sejm.gov.pl/prawo/konst/angielski/kon1.htm

[76] The Law of August 29, 1997 on the Protection of Personal Data, http://www.giodo.gov.pl/144/id_art/171/j/en/

correspondence, bodily integrity or inviolability of home are legal goods traditionally protected under penal sanctions long before the concept of the right to privacy has emerged as a fundamental human right. Expansion of information technology, particularly in the area of personal data processing, gave rise to new legal developments and reforms. In the early 90', members of the Criminal Law Reform Commission decided to exclude a regulation on privacy and personal data protection from the draft Penal Code to a new comprehensive legislation.[77] Such legislation, however, has only been enacted with regard to the protection of personal data. The criminal law protection of intimacy of the private life of natural persons, which would resemble those adopted in French and German penal codes, is still missing in Poland. A legal lacuna of this kind is undesirable, particularly in the Information Age. A proof of that is a recent draft amendment to the Penal Code concerning penalisation of a willful "dissemination of pictures of a naked person without consent of the person concerned". This legislative initiative was a response to a high profile Internet-related incident. A countermeasure, initially proposed as an offence against sexual liberty and decency, has finally been placed among offences against liberty as Article 191a of the Penal Code.[78]

On the other hand, the Law on the Protection of Personal Data of 1997 includes a comprehensive catalogue of punishable conducts. Among them, one may distinguish four main categories of "crimes against privacy"[79] :

(a) infringements of substantive privacy rights – articles 49[80], 50[81] and 51[82];

---

[77] Kazimierz Buchała, Przestępstwa..*supra* note 37 at 131.

[78] Ustawa z dnia 5 listopada 2009 r. o zmianie ustawy – Kodeks karny, ustawy – Kodeks postępowania karnego, ustawy – Kodeks karny wykonawczy, ustawy – Kodeks karny skarbowy oraz niektórych innych ustaw (not in force at the time of writing).

Art. 191a. § 1. Kto utrwala wizerunek nagiej osoby lub osoby w trakcie czynności seksualnej, używając w tym celu wobec niej przemocy, groźby bezprawnej lub podstępu, albo wizerunek nagiej osoby lub osoby w trakcie czynności seksualnej bez jej zgody rozpowszechnia, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

§ 2. Ściganie następuje na wniosek pokrzywdzonego

Article 191a of the Penal Code: § 1. Whoever records of an image of a naked person or a person involved in a sexual activity, with the use of violence, illegal threat or deceit, or an image of a naked person or a person involved in a sexual activity disseminates without consent of the person concerned, shall be subject to the penalty of the deprivation of liberty for a term of between 3 months and 5 years.

§ 2. The prosecution shall occur on a motion of the injured person.

[79] After Ulrich Sieber, Legal Aspects of Computer-Related Crime in the Information Society (COMCRIME –Study) p. 65.

[80] Article 49 of the Data Protection Act reads: 1. A person, who processes personal data in a data filing system where such processing is forbidden or where he/she is not authorised to carry out such processing, shall be liable to a fine, the penalty of limitation of liberty or the penalty of deprivation of liberty up to two years.

(b) infringements against formal requirements – article 53[83];

(c) infringements of access rights – article 54[84];

(d) neglect of security measures – article 52[85].

The Polish Data Protection Act (DPA) of 1997 has originated already in the "Internet era" and is based on the Directive 95/46/EC [86], a fundamental EU instrument of the protection of data subjects vis-a-vis centralised data banks. This may partly explain why most of penal provisions of the DPA criminalise infringements that are related to "data filing system" and make liable for such infringements its administrators. Application of criminal sanctions for privacy offences has proved to be ineffective in practice. As the Inspector General complained in her 2004 annual report:

> Public prosecutors, as well as Police officers, many times showed lack of basic legal knowledge and understanding of the Act, and even conscious disrespect for its provisions. {…} the prosecution authorities often reacted by discontinuing the cases addressed to them, e.g. by stating that the act does

---

2. Where the offence mentioned in point 1 of this article relates to information on racial or ethnic origin, political opinions, religious or philosophical beliefs, religious, party or trade union membership, health records, genetic code, addictions or sexual life, the person who processes the data shall be liable to a fine, the penalty of limitation of liberty or the penalty of deprivation of liberty up to three years.

[81] Article 50 of the Data Protection Act reads: A person who, being the controller of a data filing system, stores personal data incompatibly with the intended purpose for which the system has been created, shall be liable to a fine, the penalty of limitation of liberty or the penalty of deprivation of liberty up to one year.

[82] Article 51 of the Data Protection Act reads: 1. A person who, being the controller of a data filing system or being obliged to protect the personal data, discloses them or provides access to unauthorised persons, shall be liable to a fine, the penalty of limitation of liberty or the penalty of deprivation of liberty up to two years.
2. In case of unintentional character of the above offence, the offender shall be liable to a fine, the penalty of limitation of liberty or the penalty of deprivation of liberty up to one year.

[83] Article 53 of the Data Protection Act reads: A person who, regardless of the obligation, fails to notify the data filing system for registration, shall be liable to a fine, the penalty of limitation of liberty or the penalty of deprivation of up to one year.

[84] Article 54 of the Data Protection Act reads: A person who, being the controller, fails to inform the data subject of its rights or to provide him/her with the information which would enable that person to benefit from the provisions of this Act, shall be liable to a fine, the penalty of limitation of liberty or the penalty of deprivation of liberty of up to one year.

[85] Article 52 of the Data Protection Act reads: A person who, being the controller of a data filing system violates, whether intentionally or unintentionally, the obligation to protect the data against unauthorised takeover, damage or destruction, shall be liable to a fine, the penalty of limitation of liberty or the penalty of deprivation of liberty up to one year.

[86] Directive 95/46/EC of the European parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ No. L 281, 23.11.1995.

not bear attributes of a prohibited act or due to the fact that an offender has not been identified. At the same time, the laconic presentation of reasons for decisions on discontinuity, revealing in particular defects in explaining basic factual circumstances, showed that it was an attempt to quickly "get rid of" a case.[87]

Out of 462 notifications on the commission of crime against personal data protection which were addressed by the Inspector General to the prosecution authorities (1999-2006) only in 58 cases (12.5%) an indictment was brought to the court. [88]

In view of a declared failure of the criminal law model of sanctions in personal data protection, in 2007 a draft amendment of the DPA was submitted to Parliament in order to supplement the present system with another one, based on administrative liability with heavy fines (up to 100 000 Euros) imposed by the Inspector General on subjects who did not execute his decisions. This proposal faced criticism of the business sector and was stuck in Sejm.

The "second generation" of data protection laws based on the right to informational self-determination was fairly adequate in the world of centralized databanks. As an instrument oriented mostly towards prevention of privacy infringements related to uncontrolled flows of personal data, in principle it is still useful and valid. However, it becomes hardly applicable to the massive and decentralised processing of personal information over the Internet[89], a largely uncontrollable environment, where ID-theft and trafficking in personal data flourish. In this context, a role of control mechanisms based on repression and criminal law increases.

6. Liability of Internet service providers

[87] Inspector General for Personal Data Protection, Activity Report for 2004, p.20.

[88] Explanatory statement to a draft amendment of the Law on Personal Data Protection (Print No. 488) presented by the President of the Republic of Poland on 21 December 2007. http://orka.sejm.gov.pl/Druki6ka.nsf/wgdruku/488

[89] *Electronic storage and transmission of data, particularly via the Internet, has thrown the privacy principles (…) into sharp relief* – see: Neil Robinson, Hans Graux, Maarten Botterman, Lorenzo Valeri, Review of the European Data Protection Directive, Published 2009 by the RAND Corporation, http://www.rand.org/pubs/technical_reports/TR710/

In Poland the position of ISPs is governed by the Law of 18 July 2002 on Providing Services by Electronic Means (LPSEM) [90] which has been adopted in order to harmonise Polish legal regulations with those of the European Union, in particular Directive 2000/31/EC of June 8, 2000 (Directive on electronic commerce), and the Directive 2002/58/EC (Directive on privacy and electronic communications).[91]

Regarding the liability of intermediaries or ISPs, the E-Commerce Directive[92] provides that Member States be required to ensure that ISPs are not liable for the information transmitted or stored by them, so the Member States cannot impose a general obligation on ISPs to monitor the information they transmit or store.

Article 14, paragraph 1 of the E-Commerce Directive exempts the Host Provider from liability for any hosted content if the provider has no actual knowledge of illegal activity or information or upon obtaining such knowledge or awareness, acts expeditiously to remove the information or to prevent access to it. The Host Provider is therefore not obliged to actively monitor all the content transmitted or stored by his service. This privilege does not affect the possibility of requiring the service provider to terminate or prevent an infringement, or of establishing procedures governing the removal or disabling of access to information (Article 14, paragraph 3).

The Law of 18 July 2002 provides for a similar legal regime of ISPs liability based on the principle of guilt. Under this statute, ISPs are liable, under Polish civil or criminal law, for the illegal content of the websites to which they provide access only if they have not promptly undertaken the appropriate measures to block access to such content in response to the official notification or reliable message on such content or activity related to it.

---

[90] The Law of 18 July 2002 on Providing Services by Electronic Means (English translation) http://www.itu.int/osg/spu/spam/legislation/Ustawa%20SUDE-eng_ver.pdf

[91] The Directive 2000/31/EC of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), Official Journal of the European Communities No. L 178/1 from 17.7.2000; The Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). In case of the latter instrument, the Law of 18 July 2002 was based on its draft.

[92] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), OJ L 178, 17.7.2000, p. 1–16.

In contrast to the French and the UK regulations, which were obviously inspired by the US Digital Millennium Copyright, the Polish legislature did not implement a paragraph on the 'notice and take down' procedure. As a result, the Law of 18 July 2002 does not stipulate how the notification should be drafted and in what manner the provider should react to the notification.

At present, the Internet Access Providers are not obliged to blocking access to foreign sites with illegal content or services. This appears to be, however, a transitory situation. In Poland, like in some other European countries, the works on legal changes in this area are under development, but unlike other countries (e.g. Germany, Italy or the UK) they have their incentive in a recent political scandal and are aimed primarily at banning online gambling. [93] The new regulations envisage that Internet Access Providers would have to block access to internet sites that would be indicated by officials from the tax offices, Internal Security Agency (ABW) or the police. A government agency (The Electronic Communication Office) will run a central register of forbidden sites, which will also include pedophile and fascist related websites.

[93] Robert Zieliński, Sylwia Czubkowska, Koniec internetowej wolności w Polsce, *Dziennik Gazeta Prawna* (6-8. 11.2009) http://biznes.gazetaprawna.pl/artykuly/368235,koniec_internetowej_wolnosci_w_polsce.html; Poland Proposes Online Casino Ban http://www.onlinecasinoreports.com/news/industrycoverage/2009/11/10/poland-proposes-online-casino-ban.php ; Gov't Cracks Down on Gambling, *The Warsaw Voice*, 17 Nov. 2009 http://www.warsawvoice.pl/articleX.php/21304

III. Criminal procedure

Investigations of cybercrime require specific procedural instruments that enable law enforcement authorities to identify the offenders and collect the evidence of committed crimes. Relying on this assumption the Council of Europe Convention on Cybercrime has introduced some new procedural measures for the purpose of improving both the criminal investigations and international co-operation in computer crime cases. By virtue of this international treaty, each Party to the CoC is obliged to adopt these measures and establish in its domestic law the powers and procedures for the purpose of "specific criminal investigations or proceedings", relevant for an electronic environment. [94]

As reports on implementation of the CoC indicate, a number of the CoE member states have some problems with fulfillment of this obligation.[95] Poland is not an exception in this regard, however against a comparative background, its advances in implementation of the CoC procedural provisions are relatively modest, and in some areas even non-existent.

The clear example is the position taken by the Polish lawmaker with regard to the core idea of the CoC, i.e. "to adapt traditional procedural measures, such as search and seizure, to the new technological environment".[96] A legal reform consistent with the CoE Recommendation No. R (95) 13 on problems of criminal procedural law connected with information technology, was strongly recommended to the Polish legislator by some authors in the late 90'.[97] This proposal has not been taken into account by the then Criminal Law Reform Commission.[98] Instead, an opposite approach of "according application" of already in force provisions on the coercive powers (search of premises and seizure of objects[99]) to

---

[94] Explanatory Memorandum, 140.

[95] L.Picotti, I.Salvadori, National legislation implementing the Convention on Cybercrime – Comparative analysis and good practices, Dissusion paper (draft), Version 12 march 2008, Council of Europe, Project on Cybercrime http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/T-CY/DOC%20567%20study2-d-version8%20provisional%20(12%20march%2008).PDF

[96] Explanatory Memorandum, 134

[97] Andrzej Adamski, Prawo... *supra* note 20 at 216. A similar proposal has been put under consideration of the Polish legislature in connection with Article 19 of the draft CoC – see: Andrzej Adamski, Przestępczość w cyberprzestrzeni. Prawne środki przeciwdziałania zjawisku w Polsce na tle projektu konwencji Rady Europy (Crime in Cyberspace. Legal countermeasures in Poland and the Council of Europe Draft Convention), Toruń 2001, pp. 81-90.

[98] See also: Arkadiusz Lach, Poland (in:) S.Mason (ed.) International Electronic Evidence, British Institute of International and Comparative Law, BIICL 2008, p. 695.

[99] Article 219. § 1 of the CCP: A search may be made of premises and other places in order to detect or arrest a person or to ensure his compulsory appearance, as well as to locate objects which might serve as

electronic evidence was adopted in the Code of Criminal Procedure (CPP) amended in 2003. A newly established provision of Article 236a of the CPP provided that the regulations contained in chapter 25 of the CCP (search and seizure) "shall be applied *mutatis mutandis*" to information systems and data, including correspondence send by electronic mail[100].

In pursuant of this legal provision, the search and seizure of stored computer data may concern only tangible objects like computers and data carriers (e.g. hard –drives, CD-Roms, memory sticks), and can be executed by securing the data medium upon which this data is stored. As a routine, the seizure of electronic evidence takes place in the course of the search of premises or persons, and, as a rule, is carried out by the police on the basis of a warrant issued by a court or a public prosecutor. Where there is a risk of loss of evidence and immediate action is required, a warrantless search is allowed, however it must subsequently be approved by the court or prosecutor (Article 220 § 3 of the CCP)[101]. Moreover, if there is a reasonable suspicion that a crime has been committed, subsequent approval by the prosecutor is not required for the search of a body, clothes and luggage of a given person as well as to the checking of a cargo stored at terminals or carried by means of transportation (Article 15.1.5. of the Police Act).[102]

Adopted approach of "*mutatis mutandis* application" of traditional regulations like Article 219 of the CCP [103] to information technology is deficient in many respects and can hardly be recognised as an attempt of transposition of Article 19 of the CoC to the Polish legal system. Clearly, as some authors argue, such transposition was not intended by the

---

evidence in criminal proceedings, if there is a good reason to suppose that the suspected person or the objects sought are to be located there.

[100] Article 236a of the CCP: The provisions of this Chapter shall be applied accordingly, to those exercising control over or using information technology systems with respect to data stored in this system or on a storage medium being at his disposal or being used, including correspondence send by electronic mail.

[101] Article 220 § 3 of the CCP: In cases not amenable to delay, if the court's or state prosecutor's order cannot be issued, the agency conducting the search shall produce a warrant from the chief of the unit or an official identity card, and then apply without delay to the court or the state prosecutor for approval of the search. The person on whose premises the search was conducted should be served, within seven days of the date of the action, upon a demand from such person made for the record, an order of the court or the state prosecutor authorizing the action. The person should be instructed about his right to make such a demand.

[102] Ustawa z 19 kwietnia 1990 r. o Policji (Dz.U.2007.43.277) http://www.ifp.pl/html/ustawa/ustawa.html

[103] Article 219. § 1. A search may be made of premises and other places in order to detect or arrest a person or to ensure his compulsory appearance, as well as to locate objects, which might serve as evidence in criminal proceedings, if there is good reason to suppose that the suspected person or the objects sought are to be located there.

drafters and legislature at all.[104] Undesirable consequences of this omission are threefold. On the one hand, such imprecise regulation, based on analogous application of law, provides vast opportunities for arbitrary interpretation, and hence improper application of the criminal procedure provisions. On the other hand, the lack of clarity on how to carry out computer searches and data seizures in a lawful manner would diminish the effectiveness of investigating authorities. Last but not least, uncertainty surrounding interpretation of Article 236a of the CCP may also negatively affect the situation of computer users, including respect for their right to privacy. This is particularly true as far as technically advanced methods of evidence collection, including "extended" search of computer systems are concerned.

1. Extended search of information systems

So far, the Supreme Court had no opportunity to pronounce any ruling on admissibility of an online computer search. Opinions on this subject differ. Officials from the Ministry of Justice subscribe to the interpretation that Articles 219 and 236a of the CPP provide sufficient basis for the application of such a measure.[105] On the other hand, there is a wide agreement among authors who deal with this issue that the above provisions do not constitute a legal basis for the extended search of networked information systems located outside premises named in a search warrant.[106] The major argument raised against such a possibility on the grounds of legality points out the inadmissibility of an analogous application of the criminal procedural law *in malam partem*, especially with regard to the use of coercive measures. A reference is made in this context to Article 50 of the Constitution which recognizes the right

[104] See: Lach *supra* note 62 at 695, who speculates that "it is possible that the Polish lawmaker was of the opinion that it is not necessary to create separate coercive measures for the electronic environment".

[105] Uzasadnienie wniosku o udzielenie zgody na ratyfikację Konwencji Rady Europy z 23 listopada 2001 r. o cyberprzestepczości [Reasoning of the motion for authorisation on ratification of the Council of Europe Convention on Cybercrime], p. 7.

[106] Andrzej Adamski, Rządowy projekt dostosowania polskiego kodeksu karnego do Konwencji Rady Europy o cyberprzestępczości [Government's bill on implementation of the CoE Convention on Cybercime, paper presented at the conference SECURE 2003 Warsaw, 5-6 November 2003r.] http://www.cert.pl/PDF/secure2003/adamski.pdf; Arkadiusz Lach, Gromadzenie dowodów elektronicznych po nowelizacji kodeksu postępowania karnego [Collecting Electronic Evidence after Amendment of the Code of Criminal Procedure], *Prokuratura i Prawo* 2003, nr 10, p. 23; A. Nowak, Przeszukanie i zatrzymanie sprzętu komputerowego jako procesowa forma uzyskiwania materiału dowodowego [Search and Seizure of Computer Hardware as a Procedural Measure of Evidence Collection] , *Dodatek do Monitora Prawniczego* 2005 nr 3, p. 42.

to inviolability of the home , and stipulates that the search is allowed only in cases and in a manner specified by the statute.[107] In connection with this, it can be mentioned about the recent draft amendment of the Police Act of 1990 which proposes to include into the police surveillance measures a remote search of computer hard drives.[108]

2. Seizure of data

Although the CCP does not explicitly provide so, the computer data of evidential value may be seized by making its copy. Securing electronic evidence in this way is regarded to be legally permissible as a less intensive measure of evidence collection than the seizure of data carriers or complete computer installations. Such *in bonam partem* interpretation of law is based on Article 236c of the CCP. Additionally, it also corresponds to the legal principle of proportionality (Article 227 of the CCP), which requires coercive measures to be applied with moderation and respect for the dignity of the persons involved, and without unnecessary damage or hardship.[109] The fact that the CCP does not directly allows the investigating authorities to seize data through making its copy has various consequences. It implies, for instance, that the confiscation of data and its subsequent removal from the suspect's computer system have little chance to be applied in result of "*mutatis mutandis* application" of the existing legal provisions.[110] A conservative approach to handling of electronic evidence, adopted in the CCP, may also account for the lack of regulations governing the search and seizure of computer data in a manner compatible with computer forensic standards.[111] This, in turn, may explain why top-rank officials from the Ministry of Justice call into question the usefulness of this sort of regulations and find the current state of legislation in the field of electronic evidence fairly satisfying.[112] In view of considerable differences between expected and actual compliance of the Polish criminal procedure with

[107] Article 50 of the Constitution: The inviolability of the home shall be ensured. Any search of a home, premises or vehicles may be made only in cases and in a manner specified by statute.

[108] Communication presented at the 13th Conference on Network and ICT Systems Security - SECURE 2009 (Warsaw, 20-21 October 2009) by the representative of the Headquarters of the Police.

[109] Arkadiusz Lach, *supra* note 70 at 22.

[110] Id., p.25.

[111] Respective recommendations are included in the Explanatory Memorandum, 197.

[112] Odpowiedź sekretarza stanu w Ministerstwie Sprawiedliwości - z upoważnienia ministra - na interpelację nr 7857 w sprawie postępowania z dowodami elektronicznymi [Response of the Secretaty of State in the Ministry of Justice – on authorisation of the Minister - to the interpellation no. 7857 on handling of the electronic evidence], http://orka2.sejm.gov.pl/IZ6.nsf

the procedural provisions of the CoC, it is not easy to share this opinion. On the other hand, it should be borne in mind that from the point of view of criminal justice practitioners, simple techniques of gathering electronic evidence (e.g., seizure of hardware instead of data) have some advantages over more complex one, and are perceived as a speedy and efficient way of securing evidence material for future forensic examination. Observation of judicial practice allows for generalisation that in computer-related cases not the digital evidence itself, but the expert witness report is the key piece of evidence presented to the court.

3. Preservation of data

Preservation of stored computer data is a legal measure of crucial importance for a successful prosecution of cybercrime, because it authorises investigating authorities to prevent the deletion of specific data that are under control of other subjects and could be of relevance for a given criminal investigation. Such data, upon the request of appropriate authorities, could be ordered to be preserved for possible later access following a further disclosure order. According to Article 16 of the CoC, the legal power of preservation of data applies both to content data (e.g. business records) and traffic data (e.g. server logs).[113] Preservation of data order was adopted in Poland in 2004, however to a limited extent. It can only be applied in relation with conducted criminal investigations to the traffic data kept by telecommunication service providers in their computer systems.

Under Article 218a of the CCP[114], the court or public prosecutor, depending on the phase of the criminal proceedings, may issue a data preservation order addressing it to any telecom operator or service provider with the request to preserve the specified data. This measure is effective for a period not longer than 90 days and can not be extended. Apparently, time constrains prescribed for the preservation of data are becoming obsolete under the regime of data retention.

4. Retention of data

[113] Explanatory Memorandum, 161

[114] Article 218a § 1 of the CCP: Offices, institutions and entities running their activity in the telecommunication sector shall be obligated, upon the court or public prosecutor demand included in their order, to secure immediately, for a specified period not exceeding 90 days, computer data stored in a equipment that contains this data on a data carrier or computer system (unofficial translation).

A legal regime of mandatory telephone traffic data retention for the purposes of law enforcement and national security agencies dates back in Poland to 2003. Both the regulation of the Ministry of Infrastructure from 2003[115] and the Telecommunication Act from 2004[116] provided 12 month period of retention of data concerning on-line interactions of subscribers and users of telecommunication services. This period has been extended to 2 years in 2005[117], however its further extension (up to 5 years), supported by the group of MPs in order to increase "efficiency in combating crime and terrorism"[118], was not accepted by the parliamentary commission in 2006.[119] This legislative proposal was rejected by the commission as not compatible with the Directive 2006/24/EC.[120]

The Directive has been transposed into the Polish legal system in two steps in 2009. In April 2009 the obligation of telephone data retention was imposed on telecommunication operators and service providers in pursuant to the amended Law on Telecommunication of 2004[121]. The term of application of the retention of "communications data relating to Internet access, Internet telephony and Internet e-mail'' was postponed until 15 March 2009[122]. Even so, works on the legal framework for this measure have started in June 2009, when the Criminal Bureau of the National Police Headquarters submitted a draft proposal on this subject to the Ministry of Interior and Administration. The police proposed to include into the scope of data retention regime providers of information society services to enable law enforcement authorities access to traffic data generated by providers of VoIP telephony,

---

[115] Rozporządzenie Ministra Infrastruktury z dnia 28 stycznia 2003 r. w sprawie wykonywania przez operatorów zadań na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego, (Dz. U. Nr 19, poz. 166), zob. http://www.abc.com.pl/serwis/du/2003/0166.htm

[116] The Act of 16 July 2004 Telecommunication Law (Dz.U. No.174, item 1800, with amendments).

[117] Ustawa z dnia 29 grudnia 2005 r. o zmianie ustawy - Prawo telekomunikacyjne oraz ustawy - Kodeks postępowania cywilnego (Dz. U. z dnia 25 stycznia 2006 r.)

[118] Poselski projekt ustawy o zmianie ustawy - Prawo telekomunikacyjne – druk nr 681 (18.05.2006) http://orka.sejm.gov.pl/Druki5ka.nsf/0/D552595FC549A3C5C1257194003EBF4F/$file/681.pdf Draft amendment of the Law on Telecommunication – print no.681; Prokurator: Posłowie, zmieńcie prawo, *Rzeczpospolita* 08.09.2006 http://new-arch.rp.pl/artykul/637261.html

[119] Commission minutes http://orka.sejm.gov.pl/Biuletyn.nsf/wgskrnr5/INF-63

[120] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

[121] Ustawa z dnia 24 kwietnia 2009 r. o zmianie ustawy - Prawo telekomunikacyjne oraz niektórych innych ustaw (Dz.U.2009.85.716). [Law of 24 April 2009 amending the Telecommunication Act and some other laws]

[122] Poland, like most of the EU member states, choose to take advantage of Article 15 (3) of the Directive in this respect.

Internet communicators and electronic mail.[123] A "trial balloon" on the government's plans to impose strict control on the Internet traffic was released by the press in August 2009 and has aroused a strong critical reaction among ISPs and civil-liberties advocates.[124] In view of expected high costs of data retention some webmail providers have considered the possibility of moving their servers abroad to find there more business-friendly legal environment for their activity.[125] On the other hand, there have appeared speculations on the possibility of massive migration of e-mail accounts of regular Internet users on foreign servers to avoid monitoring.[126]

Whether such "warnings" have had any impact on the shape of legal regulations or not, it is difficult to ascertain. The fact remains, however, that in contrast to the police requirements, the supplementary regulation of 28 December 2009, concerning *inter alia* Internet traffic data retention, does not cover providers of information society services.[127] As a delegated regulation based on the Telecommunication Act (Article 180c sec. 2) it refers directly to "operators of public telecommunication networks" and "providers of publicly accessible telecommunication services", leaving aside other entities that would fall under the definition of ''providers of publicly available electronic communications services or of public communications networks'' (Article 1 data retention directive).[128]

It seems that under the present regulations of 2009 not all categories of Internet traffic data are subject to mandatory retention required by the Directive. For instance, the personal data, including the user ID of the sender or intended recipient of e-mail correspondence are beyond the reach of telecom providers. In general they are responsible

---

[123] From the police perspective, retention of Internet data must be regulated by the Law on Providing Services by Electronic Means of 2002, which concerns information society services.

[124] M. Lemańska, Internet pod ścisłą kontrolą, *Rzeczpospolita* 20.08.2009 http://www.rp.pl/artykul/67344,351363_Internet_pod_scisla_kontrola.html

[125] U. Zielińska, Polski matrix, czyli inwigilacja na żądanie, *Rzeczpospolita* 20.08.2009 http://www.rp.pl/artykul/132583,351364_Polski_matrix__czyli_inwigilacja_na_zadanie_.html

[126] I. Janke, Pielęgnujmy wolność Internetu, *Rzeczpospolita* 24.08.2009 http://www.rp.pl/artykul/9157,353405_Janke__Pielegnujmy_wolnosc_Internetu_.html

[127] Rozporządzenie Ministra Infrastruktury z dnia 28 grudnia 2009 r. w sprawie szczegółowego wykazu danych oraz rodzajów operatorów publicznej sieci telekomunikacyjnej lub dostawców publicznie dostępnych usług telekomunikacyjnych obowiązanych do ich zatrzymywania i przechowywania (Dz. U. Nr 226. poz.1828)

[The Regulation of the Minister of Infrastructure of 28 December 2009 on a detailed specification of data and types of operators of public telecommunications networks or providers of publicly available telecommunications services obliged for its retention and storage, *Journal of Laws of 2009, No 226 item 1828*, went into force on 1 January 2010].

[128] As rightly pointed out in literature, the term '*providers of publicly available communications services or public communication networks'* is vague and "the directive missed the opportunity to provide its detailed definition in order to prevent deviating interpretations among the Member States" (E. Kosta, P. Valcke, Retaining the data retention directive, *Computer Law and Security Report* 2006, vol.22, issue 3 , p. 374).

for the transmission of data packets and have no reasons nor technical capabilities for processing of data flowing through networks they operate. [129]

The retention period is equal for both the telephone and Internet traffic data and amounts to 24 months from the date of the communication.[130] Access to retained data is restricted to the police, national security agencies, and judicial authorities.[131] All the authorities designated under the relevant laws have the right of access to traffic, subscribers and localisation data in the case of any crime, however, trivial. There is no legal threshold of seriousness of crime nor independent oversight of the disclosure of data by telecom providers to the applicants.

5. Production order

According to Article 18 CoC, the aim of production order is to give the competent authority the power to compel a person in its territory to provide specific stored data, or to compel an ISP to furnish the subscriber with information necessary for the criminal investigation that are in those persons' possession or control. There are similar procedural measures in the Polish legal system, however a scope of their applicability is relatively narrow and covers only telecommunication service providers. According to Article 180d of the Law on Telecommunication, they are obliged to submit on their own expense the traffic, location and subscriber's data to the police, state prosecutor and court in compliance with the rules and procedures prescribed by other legal provisions. Respectively, corresponding regulations are to be found in the Police Act (Article 20c) and the CCP (Article 218). Article 20c of the Police Act allows the duly authorised police officer to obtain from the telecom operator for the purposes of detection and prevention of crime the stored traffic, location and subscriber's data. This can be done either on an oral demand of a policeman or by means of

[129] A reference can be made in this context to the present discussion on "transit providers" where it is indicated that : "*Entities that simply carry Internet data across networks but that neither provide access to the Internet, nor to e-mail or VoIP services ("transit providers"), are not required to retain data under the Directive, since they do not have the data necessary to correlate logs to a specific user.*" – see: European Commission, Directorate General Justice, Freedom and Security, Summary Report – Informal Data Retention Experts Meeting - 2 April 2008, p.6.
http://ec.europa.eu/justice_home/news/events/data_retention/meeting_report_05_04_07.pdf

[130] This period has been reduced to 12 months by an amendment of the Telecommunications Law Act of 16th November 2012.

[131] The Police, Military Police, Military Counter-Intelligence Service, Fiscal Intelligence, Border Guard, Internal Security Agency, Central Anticorruption Bureau, courts and prosecutors.

transmission of data through a telecommunication network (written application is not required). A production order addressed to the telecommunication service provider may also be issued by the prosecutor in the course of preparatory proceedings or the court during court proceedings. On the basis of a recently amended Article 218 of the CCP, all entities operating in the telecommunication sector are obligated to surrender to the court or state prosecutor upon demand included in their order, any correspondence and data specified in Article 180c and Article 180d of the Law on Telecommunication, when the above are significant to the pending proceedings. The indicated provisions of telecommunication law do not apply to the Internet service providers. Obviously, they have a legal duty to cooperate with the state authorities by disclosing their subscribers' data to them. This obligation, however, has been defined in a very general way.[132] Furthermore, neither the Police Act nor the CCP make any direct reference to ISPs, hence the law does not unequivocally mandate police officers, state prosecutors and courts to order ISPs to submit data that have already been stored in their computer systems.

Despite this legal ambiguity and its critical assessment in the literature[133], subscriber information is communicated by the ISPs to the law enforcement and criminal justice authorities on their demand.

6. Real-time collection of traffic data

Until presently, the Polish legislation does not provide a measure consistent with Article 20 of the CoC.[134] An opposite view contained in the Explanatory memorandum to the motion for authorisation on ratification of the Council of Europe Convention on Cybercrime[135] cannot be accepted. Its reasoning refers to the executive regulation of the Council of Ministers from 13

[132] Article 18 (6) of the Law on Providing Services by Electronic Means of 2002 states that "the service providers provide the information on data referred to in paragraphs 1-5 to the state authorities for the needs of legal proceedings carried on by them." These are mostly personal data of the subscribers, including their electronic addresses and some categories of traffic data.

[133] Andrzej Adamski, Przestępczość, *supra* note 61 at 75; Arkadiusz Lach, Dowody elektroniczne w procesie karnym , Toruń 2004, p. 126.

[134] Arkadiusz Lach, Dowody elektroniczne , p.124.

[135] Uzasadnienie wniosku o udzielenie zgody na ratyfikację Konwencji Rady Europy z 23 listopada 2001 r. o cyberprzestępczości [Reasoning of the motion for authorisation on ratification of the Council of Europe Convention on Cybercrime], p. 8.

September 2005[136] which is inadequate in this context, both technically and legally. In the latter aspect – as a legal basis for the criminal law procedural measure.

7. Interception of content data

Interception of communications is regulated by the provisions of Chapter 26 of the CCP which apply not only to telephone conversations but also other forms of communications, including electronic mail (Article 241)[137].
It can be argued that this provision enables lawful interception of all kinds of Internet-related communications, including Skype conversations, of course, as soon as such possibility becomes technically feasible.

IV. Evaluation and Summary

The focus of this report was upon the current developments in the Polish criminal law legislation aimed at its harmonisation with the European normative standards in the field of combating cybercrime, mostly – the 2001 CoE Convention on Cybercrime. The report has covered two main subject areas of cyber crime laws: substantive criminal law and criminal procedure.

The general observation that can be made on the basis on the foregoing analysis is not very flattering for the legislator. Despite substantial efforts undertook in order to implement the CoE Convention on cybercrime to the Polish legal system, their results appear to be far from expectations. Paradoxically, they are partly below and partly above the expectations concerning comprehensive and adequate alignment of the national legislation with international law instruments.

[136] Rozporządzenie Rady Ministrów z dnia 13.09.2005 r. w sprawie wypełniania przez przedsiębiorców telekomunikacyjnych zadań i obowiązków na rzecz obronności , bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego (Dz.U. Nr 187, poz.1568). [Regulation of the Council of Ministers of 13 September 2005 on the execution of tasks and duties related to the defence and security of the state and the security and public order by the telecommunication entities, *Journal of Laws 2005, No.187, item 1568*]

[137] Article 241 of the CCP: The provisions of this chapter shall apply respectively to surveillance and recording by technical means, of the content of other conversations or information transmissions, including correspondence transmitted by electronic mail.

The transposition of procedural measures provided by the CoC to the domestic law has been selective and incomplete. Such IT-specific measures as extended search of computer and data seizure were not incorporated into the CCP. The same concerns the real time interception of traffic data and preservation of computer data not related with traffic. The legislator can also be blamed for oversights that call into question the legality of co-operation between ISPs and law enforcement authorities in the realm of production orders.

The implementation of the substantial criminal law provisions was more successful, at least in quantitative terms. It brought to the Penal Code a number of new provisions that increased considerably, sometimes excessively, the scope of criminal law protection of some legal goods, while leaving the others poorly protected.

The present regulation of CIA-offences is redundant. Before 2008 a "pure" hacking, or unauthorised access to a computer system, has not been criminalised in Poland. At the moment, there are two hacking offence provisions and a triple ban on the system interference. Even so, not all normative standards established by the Council of Europe and the European Union instruments are fully covered by the Penal Code. The most notable examples concern the protection of data integrity and authenticity of e-documents. An erroneous design of the Penal Code provisions (Article 268a, Article 115 § 14) undermines legal protection of computer data and electronic documents against unauthorised manipulations. On the other hand, the vague wording of the hacking offence (Article 267 § 2) allows for a wide application of this provision, including trivial situations that do not deserve intervention of the criminal law.
A faulty definition of "hacker's tools" offence (Article 269b of the Penal Code) leads to ridiculous interpretations of this provision, lowering the prestige of the law in the eyes of its addressees.

As the overview of main findings of the present report indicates, the correlation between the number of penal provisions and the quality of cybercrime legislation seems to be weak, if not negative. An examination of factors that may account for such result goes beyond the

scope of the present analysis. It would be reasonable to conclude that as long as the ratification of the CoC is an ongoing process in Poland, it is still possible to fill the gaps and make improvements in the binding regulations.

Annex

Bibliography

Andrzej Adamski, Buszujący w sieci. Cybernowelizacja prawa karnego, „*Rzeczpospolita*" (27.10.2003)

Andrzej Adamski, Cyberprzestępczość - aspekty prawne i kryminologiczne, *Studia Prawnicze* 2005 nr 4 (167)

Andrzej Adamski, Nowe ujęcie cyberprzestępstw w kodeksie karnym – ale czy lepsze?, *Prawo Teleinformatyczne*, 2007, 3(5)

Andrzej Adamski , Opinia do projektu ustawy z druku nr 458 Rządowy projekt ustawy o zmianie ustawy - Kodeks karny oraz niektórych innych ustaw (Legal opinion on the bill amendment of the Penal Code prepared for the Office of Legal Analyses of Sejm on 8 July 2008) http://orka.sejm.gov.pl/rexdomk6.nsf/Opdodr?OpenPage&nr=458

Andrzej Adamski, Oszustwo komputerowe a oszustwo internetowe (w:) Przestępczość teleinformatyczna. Materiały seminaryjne pod red. J.Kosińskiego Wyższa Szkoła Policji, Szczytno 2005

Andrzej Adamski (ed.), Prawne aspekty nadużyć popełnianych z wykorzystaniem nowoczesnych technologii przetwarzania informacji, Materiały z konferencji naukowej [Legal Aspects of Computer-Related Abuse, Proceedings of the International Conference], Poznań, 20-22 kwietnia 1994, Towarzystwo Naukowe Organizacji i Kierownictwa „Dom Organizatora", Toruń 1994

Andrzej Adamski, Prawo karne komputerowe, C.H.Beck, Warszawa 2000

Andrzej Adamski, Przestępczość w cyberprzestrzeni. Prawne środki przeciwdziałania zjawisku w Polsce na tle projektu konwencji Rady Europy, Wydawnictwo „Dom Organizatora", Toruń 2001

Andrzej Adamski, Rządowy projekt dostosowania polskiego kodeksu karnego do Konwencji Rady Europy o cyberprzestępczości, paper presented at the conference SECURE 2003 (Warsaw, 5-6 November 2003 r.) http://www.cert.pl/PDF/secure2003/adamski.pdf

Kazimierz Buchala, Poland, (in:) Ulrich Sieber (ed.) Information Technology Crime. National Legislations and International Initiatives, Carl Heymans Verlag KG, Köln,Berlin,Bonn, München 1994

Kazimierz Buchała, Przestępstwa przeciwko ochronie informacji i oszustwo komputerowe, (w:) Materiały z konferencji naukowej [Legal Aspects of Computer-Related Abuse, Proceedings of the International Conference], Poznań, 20-22 kwietnia 1994, Towarzystwo Naukowe Organizacji i Kierownictwa „Dom Organizatora", Toruń 1994

Magdalena Budyn-Kulik i inn., Kodeks karny. Praktyczny komentarz, Kantor Wydawniczy Zakamycze, Kraków 2004

European Commission, Directorate General Justice, Freedom and Security, Summary Report - Informal Data Retention Experts Meeting - 2 April 2008 http://ec.europa.eu/justice_home/news/events/data_retention/meeting_report_05_04_07.pdf

Krzysztof Gienas, Hak na hakera, *Rzeczpospolita* (29.07.2005)

Incident handling, statistics and procedures, Warsaw, May 2003, http://www.terena.nl/tech/task-forces/tf-csirt/meeting9/nazar-polish-telecom.pdf

Igor Janke, Pielęgnujmy wolność Internetu, *Rzeczpospolita* (24.08.2009) http://www.rp.pl/artykul/9157,353405_Janke__Pielegnujmy_wolnosc_Internetu_.html

Piotr Kardas, Oszustwo komputerowe w kodeksie karnym, *Przegląd Sądowy* 2000, No. 11-12

Orin Kerr, Cybercrime's Scope: Interpreting 'Access' and 'Authorization' in Computer Misuse Statutes, *New York University Law Review*, Vol. 78, No. 5, November 2003. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=399740

Rafał Korczyński, Robert Koszut, „Oszustwo" komputerowe, *Prokuratura i Prawo* 2002, No.2

Eleni Kosta, Peggy Valcke, Retaining the data retention directive, *Computer Law and Security Report* 2006, vol.22, issue 3

Arkadiusz Lach, Dowody elektroniczne w procesie karnym, Wydawnictwo „Dom Organizatora", Toruń 2004

Arkadiusz Lach, Gromadzenie dowodów elektronicznych po nowelizacji kodeksu postępowania karnego, *Prokuratura i Prawo* 2003, nr 10

Arkadiusz Lach, Poland (in:) S.Mason (ed.) International Electronic Evidence, British Institute of International and Comparative Law, BIICL 2008

Magdalena Lemańska, Internet pod ścisłą kontrolą, *Rzeczpospolita* (20.08.2009) http://www.rp.pl/artykul/67344,351363_Internet_pod_scisla_kontrola.html

Jarosław Majewski, Rozdział XVI. Objaśnienie wyrażeń ustawowych (w:) Andrzej Zoll (red.)Kodeks Karny, Część ogólna. Komentarz, tom I, Kantor Wydawniczy Zakamycze, Kraków 2004

Andrzej Marek, Kodeks karny. Komentarz, Warszawa 2005

Andrzej Marek, Kodeks karny. Komentarz. Wydawnictwo LEX, Warszawa 2007

Beata Mik, Karnomaterialna. ochrona dokumentów (zagadnienia wybrane*), Prokuratura i Prawo* 2001, nr 4

Andrzej Nowak, Przeszukanie i zatrzymanie sprzętu komputerowego jako procesowa forma uzyskiwania materiału dowodowego, Dodatek do *Monitora Prawniczego* 2005 nr 3

Piotr Ochman, Spór o pojęcie dokumentu w prawie karnym, *Prokuratura i Prawo* 2009, nr 1

Lorenzo Picotti, Ivan Salvadori, National legislation implementing the Convention on Cybercrime – Comparative analysis and good practices, Dissusion paper (draft), Version 12 March 2008, Council of Europe, Project on Cybercrime
http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/T-CY/DOC%20567%20study2-d-version8%20provisional%20(12%20march%2008).PDF

Joanna Piórkowska-Flieger, Fałsz dokumentu w polskim prawie karnym, Kantor Wydawniczy Zakamycze, Kraków 2004

Neil Robinson, Hans Graux, Maarten Botterman, Lorenzo Valeri, Review of the European Data Protection Directive, Published 2009 by the RAND Corporation, http://www.rand.org/pubs/technical_reports/TR710/

Ryszard A. Stefański, Barbara Świątkiewicz, Internet Offences in Poland: Analysis of the practice (in:) J. C. Ferré Olive, E. Musco, B. Kunicka-Michalska, J. A. Cabral at al., Grotius II Penal Programme. Penal Legislation in the Fight Against Financial Crimes, Fraud and Corruption, Computer Fraud and Internet Crimes, Universidad de Salamanca 2004.

Ryszard A. Stefański, Oszustwa komputerowe w praktyce polskich organów ścigania, *Studia Prawnicze* 2006 nr 4 (170)

Michael Walton, Possession of Child Pornography. Background Paper, New South Wales Council for Civil Liberties, January 2005, p.6
http://www.nswccl.org.au/docs/pdf/bp2%202005%20Possess%20Child%20Porn.pdf

Włodzimierz Wróbel, Komentarz do rozdziału XXXIII Kodeksu karnego – Przestępstwa przeciwko ochronie informacji [w:] A.Zoll (red.) Kodeks karny. Część szczególna. Komentarz, t.2, Kraków, Wydawnictwo Prawnicze Zakamycze 1999

Ulrich Sieber, The Legal Aspects of Computer Crime Raport at The Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders Havana, Cuba August 27-September 7, 1990

Ulrich Sieber, Legal Aspects of Computer-Related Crime in the Information Society (COMCRIME -Study)

Urszula Zielińska, Polski matrix, czyli inwigilacja na żądanie, *Rzeczpospolita* (20.08.2009) http://www.rp.pl/artykul/132583,351364_Polski_matrix__czyli_inwigilacja_na_zadanie_.html

Robert Zieliński, Sylwia Czubkowska, Koniec internetowej wolności w Polsce, *Dziennik Gazeta Prawna* (6-8.11.2009) http://biznes.gazetaprawna.pl/artykuly/368235,koniec_internetowej_wolnosci_w_polsce.html

Criminal Law Provisions

Penal Code

Hacking

Article 267 § 1 before the 2008 amendment: Whoever, without being authorised to do so, acquires information not destined for him, by opening a sealed letter, or connecting to a wire that transmits information or by breaching electronic, magnetic or other special protection for that information shall be subject to a fine, the penalty of restriction of liberty or the penalty of deprivation of liberty for up to 2 years.

Article 267 § 1 in force: Whoever, without being authorised to do so, acquires access to information not destined for him, by opening a sealed letter, or connecting to a telecommunication network or by breaching or circumventing electronic, magnetic, computer or other special protection for that information shall be subject to a fine, the penalty of restriction of liberty or the penalty of deprivation of liberty for up to 2 years.

Article 267 § 2. The same punishment shall be imposed on anyone, who, without authorisation, obtains access to the whole or any part of an information system.

Illegal interception

Article 267 § 3. The same punishment shall be imposed on anyone, who, in order to acquire information to which he is not authorised to access, installs or uses tapping, visual detection or other equipment or computer software.

Data interference

Article 268 § 1. Whoever, being unauthorised, destroys, impairs, deletes or alters a record of essential information or otherwise prevents or makes it significantly difficult for an authorised person to obtain knowledge of that information, shall be subject to a fine, the penalty of restriction of liberty or the penalty of deprivation of liberty for up to 2 years.

§ 2. If the act specified in § 1 concerns the record on an electronic information carrier, the perpetrator shall be subject to the penalty of deprivation of liberty for up to 3 years.
§ 3. Whoever, by committing an act specified in § 1 or 2, causes a significant loss of property, shall be subject to the penalty of deprivation of liberty for a term of between 3 months and 5 years.

Article 268a. § 1. Whoever, without being authorized to do so, destroys, damages, removes, changes or makes an access to computer data difficult, or in a significant degree disrupts or prevents automatic processing, gathering or transmission of such data, shall be subject to the penalty of deprivation of liberty for up to 3 years.

§ 2. Whoever, by committing an act specified in §1, causes a significant loss of property shall be subject to the penalty of deprivation of liberty for a term of between 3 months and 5 years.

System interference

Article 269. § 1. Whoever destroys, deletes or changes a record on an electronic information carrier, having a particular significance for national defence, transport safety, operation of the government or other state authority or local government, or interferes with or prevents automatic collection and transmission of such information, shall be subject to the penalty of deprivation of liberty for a term of between 6 months and 8 years.

§ 2. The same penalty should apply to a person who commits offences mentioned in § 1, by destroying or replacing the information carrier or by destroying or damaging a device serving for automatic processing, gathering or transferring of information data.

Article 269a. Whoever, without being authorized to do so, through transmitting, destroying, deleting, impairing or changing computer data, causes significant interference with functioning of a computer system or network, shall be subject to the penalty of deprivation of liberty for from 3 months to 5 years.

Article 268a. § 1. Whoever, without being authorized to do so, destroys, damages, removes, changes or makes an access to computer data difficult, or in a significant degree disrupts or prevents automatic processing, gathering or transmission of such data, shall be subject to the penalty of deprivation of liberty for up to 3 years.

§ 2. Whoever, by committing an act specified in §1, causes a significant loss of property shall be subject to the penalty of deprivation of liberty for a term of between 3 months and 5 years.

Misuse of devices

Art. 269b. § 1. Whoever, produces, acquires, sells off or makes available to other persons devices or computer software adapted to the commission of an offence mentioned in Article 165 § 1 pt 4, Article 267 §3, Article 268a § 1 or § 2 in

connection with § 1 or § 2, Article 269 § 2 or Article 269a, and computer passwords, access codes or other data that make possible the access to information stored in a computer system or network,
shall be subject to the penalty of deprivation of liberty for up to 3 years.

§ 2 In case of a conviction for an offense referred to in § 1, the court rules the forfeiture of items, and may decide their forfeiture if they were not the property of the perpetrator.

Computer related-fraud

Article 287. § 1. Whoever, in order to gain material benefits or cause the other person material damage, affects automatic processing, gathering or transmitting computer data , or changes or deletes record or introduces a new record of computer data, without being authorised to do so,

shall be subject to the penalty of deprivation of liberty for a term of between 3 months and 5 years.

§ 2. In the event that the act is of a lesser significance, the perpetrator

shall be subject to a fine, the penalty of restriction of liberty or the penalty of deprivation of liberty for up to one year.

§ 3. If the fraud has been committed to the detriment of a next of kin, the prosecution shall occur on a motion of the injured person.

Child pornography

Article 202 § 3. Whoever, for the purpose of dissemination, produces, records, imports or disseminates or presents publicly pornographic material in which a minor is presented, or pornographic material associated with the use of violence or the use of an animal, shall be subject to the penalty of deprivation of liberty for from 6 months to 8 years.

§ 4. Whoever records pornographic content with the participation of a minor under age of 15, shall be subject to the penalty of deprivation of liberty from from one to 10 years.

§ 4a.Whoever imports, stores or possesses pornographic content in which a minor under 15 years of age is presented, shall be subject to the penalty of deprivation of liberty for from 3 months to 5 years.

§ 4b.Whoever produces, disseminates, presents, stores or possesses a pronographic content featuring a created or processed image of a minor taking part in a sexual activity, shall be subject to the penalty of fine, limitation of liberty or deprivation of liberty up to 2 years.

Racism and xenophobia

Article 119. § 1. Whoever uses violence or makes unlawful threat towards a group of person or a particular individual because or their national, ethnic, political or religious affiliation, or because of their lack of religious beliefs, shall be subject to the penalty of the deprivation of liberty for a term of between 3 months and 5 years.

§ 2. The same punishment shall be imposed on anyone, who incites commission of the offence specified under § 1.

Article 256. Whoever publicly promotes a fascist or other totalitarian system of state or incites hatred based on national, ethnic, race or religious differences or for reason of lack of any religious denomination,

shall be subject to a fine, the penalty of restriction of liberty or the penalty of deprivation of liberty for up to 2 years.

Article 257. Whoever publicly insults a group within the population or a particular person because of his national, ethnic, race or religious affiliation or because of his lack of any religious denomination or for these reasons breaches the personal inviolability of another individual, shall be subject to the penalty of deprivation of liberty for up to 3 years.

Theft of computer programme

Article 278. § 1. Whoever, with the purpose of appropriating, wilfully takes someone else's movable property, shall be subject to the penalty of deprivation of liberty for a term of between 3 months and 5 years.

§ 2. The same punishment shall be imposed on anyone, who without the permission of the authorised person, acquires someone else's computer software, with the purpose of gaining material benefit.

§ 3. In the event that the act is of a lesser significance, the perpetrator shall be subject to a fine, the penalty of restriction of liberty or the penalty of deprivation of liberty for up to one year.

Handling of "stolen" software

Article 293. § 1. The provisions of Article 291 and 292 shall be applied accordingly to computer software.

§ 2. The court may decide on the forfeiture of the item specified in § 1 and in Articles 291 and 292, even though it may not be the property of the perpetrator.

Data Protection Act

Article 49 (1). A person, who processes personal data in a data filing system where such processing is forbidden or where he/she is not authorised to carry out such processing, shall be liable to a fine, the penalty of limitation of liberty or the penalty of deprivation of liberty up to two years.

2. Where the offence mentioned in point 1 of this article relates to information on racial or ethnic origin, political opinions, religious or philosophical beliefs, religious, party or tradeunion membership, health records, genetic code, addictions or sexual life, the person who processes the data shall be liable to a fine, the penalty of limitation of liberty or the penalty of deprivation of liberty up to three years.

Article 50.1. A person who, being the controller of a data filing system, stores personal data incompatibly with the intended purpose for which the system has been created, shall be liable to a fine, the penalty of limitation of liberty or the penalty of deprivation of liberty up to one year.

Article 51.1. A person who, being the controller of a data filing system or being obliged to protect the personal data, discloses them or provides access to unauthorised persons, shall be liable to a fine, the penalty of limitation of liberty or the penalty of deprivation of liberty up to two years.
2. In case of unintentional character of the above offence, the offender shall be liable to a fine, the penalty of limitation of liberty or the penalty of deprivation of liberty up to one year.

Article 52. A person who, being the controller of a data filing system violates, whether intentionally or unintentionally, the obligation to protect the data against unauthorised takeover, damage or destruction, shall be liable to a fine, the penalty of limitation of liberty or the penalty of deprivation of liberty up to one year.

Article 53. A person who, regardless of the obligation, fails to notify the data filing system for registration, shall be liable to a fine, the penalty of limitation of liberty or the penalty of deprivation of up to one year.

Article 54. A person who, being the controller, fails to inform the data subject of its rights or to provide him/her with the information which would enable that person to benefit from the provisions of this Act, shall be liable to a fine, the penalty of limitation of liberty or the penalty of deprivation of liberty of up to one year.

The Copyrigh Act

Article 116.

1. Whoever, without authorization or against its terms and conditions, disseminates someone else's work, in the original or derivative version, performance, phonogram, videogram or broadcast shall be liable to a fine, restriction of liberty or imprisonment for the period of up to 2 years.
2. If the perpetrator commits the act specified in paragraph 1 above in order to gain material benefits, he shall be liable to imprisonment for the period of up to 3 years.
3. If the perpetrator makes the offence specified in paragraph 1 above a regular source of income or organizes or manages a criminal activity, as specified in paragraph 1, he shall be liable to imprisonment from 6 months up to 5 years.
4. If the perpetrator of the act specified in paragraph 1 above acts unintentionally, he shall be liable to a fine, restriction of liberty or imprisonment for the period of up to one year

Article 117.

1. Whoever, without authorization or against its conditions, fixes or reproduces another person's work in the original or derivative version, performance, phonogram, videogram or broadcast, for the purpose of its dissemination, shall be liable to a fine, restriction of liberty or imprisonment for the period of up to 2 years.
2. If the perpetrator makes the offence specified in paragraph 1 a regular source of income or organizes or manages a criminal activity, as specified in paragraph 1 above, he shall be liable to imprisonment for the period of up to 3 years.

Article 118.

1. Whoever, in order to gain material benefits, purchases or assists in selling or accepts or assists in concealing objects, which are carriers of a work, performance, phonogram or videogram being disseminated or reproduced without authorization or against its conditions, shall be liable to imprisonment for the period from 3 months to 5 years.
2. If the perpetrator makes the offence specified in paragraph 1 a regular source of income or organizes or manages criminal activity, as specified in paragraph 1, shall be liable imprisonment from 1 to 5 years.
3. Where on the basis of circumstances the perpetrator of the act specified in paragraph 1 or 2 should and could presume that the object has been obtained through an illegal act, he shall be liable to a fine, restriction of liberty or imprisonment for the period of up to 2 years.

Article 118[1]

1. Whoever produces devices or their components intended for an illegal removal or circumvention of effective technical protection measures against communication, recording or reproducing works or objects of related rights, or carries on trade in such devices or their components or advertises them for the purpose of sale or rental, shall be liable to a fine, restriction of liberty, or imprisonment for the period up to 3 years.
2. Whoever owns, keeps or uses devices or their components referred to in paragraph 1, shall be liable to a fine, restriction of liberty or imprisonment for the period up to one year.

Article 119. Whoever prevents or hinders the exercise of the right to supervise the use of a work, performance, phonogram or videogram or refuses to provide information stipulated in Article 47, shall be liable to a fine, restriction of liberty or imprisonment up to 1 year.

Article 120.
[Article 120 has been deleted.]

Article 121.
1. In the event of sentencing for the offence specified in Articles 115, 116, 117, 118 or 1181, the court shall order the seizure of objects coming from the offence, even if they were not owned by the perpetrator.
2. In the event of sentencing for the offence specified in Articles 115, 116, 117 or 118, the court may order seizure of objects used to commit the offence, even if they were not owned by the perpetrator.

Article 122.
Offences specified in Articles 115, 116, paragraphs 1, 2 and 4, Article 117, paragraph 1, Article 118, paragraph 1, Article 1181 and Article 119 shall be prosecuted upon a motion of the injured person.

Article 122[1].
In the cases conducted with respect to offences specified in Articles 115 to 119, the injured person shall also be the competent organization for collective management of copyright or related rights.

The Code of Criminal Procedure

Article 219. § 1. A search may be made of premises and other places in order to detect or arrest a person or to ensure his compulsory appearance, as well as to locate objects which might serve as evidence in criminal proceedings, if there is good reason to suppose that the suspected person or the objects sought are to be located there.

Article 218a § 1. Offices, institutions and entities running their activity in the telecommunication sector shall be obligated, upon the court or public prosecutor demand included in their order, to secure immediately, for a specified period not exceeding 90 days, computer data stored in a equipment that contains this data on a data carrier or computer system.

Article 236a. The provisions of this Chapter shall be applied accordingly, to those exercising control over or using information technology systems with respect to data stored in this system or on a storage medium being at his disposal or being used, including correspondence send by electronic mail.

Article 220 § 3. In cases not amenable to delay, if the court's or state prosecutor's order cannot be issued, the agency conducting the search shall produce a warrant from the chief of the unit or an official identity card, and then apply without delay to the court or the state prosecutor for approval of the search. The person on whose premises the search was conducted should be served, within seven days of the date of the action, upon a demand from such person made for the record, an order of the court or the state prosecutor authorizing the action. The person should be instructed about his right to make such a demand.