INFORMATION TECHNOLOGY TERMINOLOGY IN CHAPTER XXXIII OF THE POLISH PENAL CODE OF 1997

Filip Radoniewicz, PhD student
Maria Curie-Skłodowska University in Lublin
Faculty of Law and Administration
Institute of Criminal Law
Department of Comparative Criminal Law
ul. Pana Balcera 8/43
20-631 Lublin, Poland
filip.radoniewicz@gmail.com

Abstract: In the introductory part of the article, the distinction between two frequently confused concepts - "data" and "information" was made and their definitions were given, to describe afterwards the basic classifications - "computer data" and "information system". For that purpose international legal statutes were recalled, including the OECD Guidelines for the Security of Information Systems of the 26th of November 1992 and the Council Framework Decision 2005/222/JHA of the 24th of February 2005 on attacks against information systems. In the main part of the article, the author focuses on the information concepts, which are used by the Polish legislator in the Chapter XXXIII of the Penal Code, in which computer crimes are enumerated. Attention is paid to inconsistency in terminology, conceptual overlaps between certain specifications, and lack of definition of the relevant concepts. As the conclusion it is stated that the measures so far undertaken by the legislator, to standardise the terminology, are inadequate. Therefore, further efforts regarding that issue are essential. What is more, introduction of definitions of the most relevant classifications - especially "information system" and "computer data" to the Penal Code is advisable.

TERMINOLOGIA INFORMATYCZNA W PRZEPISACH ROZDZIAŁU XXXIII POLSKIEGO KODEKSU KARNEGO Z 1997 ROKU

Abstrakt: W części wstępnej referatu dokonano rozróżnienia i zdefiniowania dwóch często mylonych ze sobą pojęć – „danych" oraz „informacji", by następnie scharakteryzować podstawowe terminy – „danych komputerowych" i „systemu informatycznego". Odwołano się w tym celu do aktów prawa międzynarodowego, w tym do Wytycznych OECD w sprawie Bezpieczeństwa Systemów Informatycznych z 26 listopada 1992 roku oraz Decyzji Ramowej Rady 222/2005/WSiSW z dnia 24 lutego 2005 roku w sprawie ataków na systemy informatyczne. Główna część referatu poświęcona jest omówieniu pojęć informatycznych, którymi posługuje się polski ustawodawca w rozdziale XXXIII Kodeksu karnego, w którym umieszczono przestępstwa komputerowe. Zwrócona zostaje uwaga na niespójność terminologiczną, nakładanie się zakresów pojęciowych niektórych terminów oraz brak definicji istotnych pojęć. W konkluzji wskazano, iż podjęte dotychczas przez ustawodawcę próby ujednolicenia terminologii okazały się niewystarczające. W związku z tym konieczne są dalsze prace w tym kierunku. Ponadto wskazane.jest wprowadzenie do Kodeksu karnego definicji najważniejszych terminów - przede wszystkim „systemu informatycznego" i „danych komputerowych".

In the Penal Code of 1997 the Polish legislator uses terms of the information technology science provenance. As he actually does not give their definitions it seems indispensable to refer to other statutes. Information technology terms are included mainly in provisions regarding so called "cyber offences"[17] which are enumerated in Chapter XXXIII of the Penal Code titled "Offences against the Protection of Information", in regulations of articles 267 – 296b. Therefore the terminology used in this chapter is the issue of this publication.

First of all the meaning of two essential concepts should be discussed, which are information (computer) data and information system. Simultaneously it is necessary to specify relationship between data and information.

Concepts of "information" and "data" are often regarded as one and the same or synonyms in spite of the differences between them. The Polish Language Dictionary defines the meaning of information as: "a notification of something, an announcement, a message, a clue or an instruction" (Szymczak 1995, 739).

Włodzimierz Wróbel defines "information" on the basis of the colloquial meaning of this word as "a sign, a sound, a record, a code hiding sensitive content" (Wróbel 2006, 1235). Similarly Barbara Kunicka-Michalska intentionally does not differentiate terms of "information" and "data" using them interchangeably (Kunicka-Michalska 2000, 246-247).

The difference between the two concepts in question is not actually noticed by Katarzyna Napierała, according to whom distinguishing between them is almost impossible as: "First of all *information and data* are abstract concepts despite their expression them in tangible, real form (…); secondly, they are also a means of communication, its essential and indispensable elements. As a consequence, the terms of reference of both concepts, in some measure, overlap (Napierała 1997, 13).

In Europe several years ago attention was paid to the importance of differentiating both terms. The first document in which the effort to find a solution was made was the Report of the Dutch Committee on Computer Crime compiled in 1988. The committee was appointed to define some basic concepts necessary to create regulations regarding questions related to automatic information processing (Adamski 2000, 38). According to the document "As data is regarded presentation of facts, notions or orders in the established way, which enables their transmission, interpretation or processing by both human beings and automatic means. A computer program is

[17] Generally there are distinguished "computer offences" (cybercrime in the strict sense), as violations in which information system and computer data are the object of a crime (as examples can be given hacking or breaching integrity of data) and "computer - related offences", in which the object of violation are legal interests whereas computer, information network, data processing systems, electronic devices are used as tools. Computer – related offences are either common offences as fraud, handling stolen goods, forgery or less conventional as money laundering.

a special category of data in the meaning of this definition. (…) Information is an effect caused by data – intentional or experienced by their users."

The definitions of both terms are included in the Recommendation of the OECD concerning Guidelines for the Security of Information (Recommendation, OECD/GD (92) 10):

a) **Data** – a representation of facts, concepts or instructions in a formalised manner suitable for communication, interpretation or processing by human beings or by automatic means;
b) **Information** – the meaning assigned to data by means of conventions applied to that data.

According to the above definitions the significance of the terms "information" and "data" differs from their colloquial meaning. It is nearer to the technical meaning of information which defines "information" as an abstract object, which in coded form (data) can be stored (on data carrier), transmitted (e.g. by voice, electromagnetic wave, electric current), processed during algorithm performance and used to control (e.g. a computer is controlled by program being coded information)" (Kalisiewicz 1997, vol 3, 54); although "data" are objects on which programs operate (Kalisiewicz 1997, vol 2, 15).

Consequently it should be assumed that information has no material quality and what is more is not an item. It is a kind of "abstract object", immaterial. Only in the form of data can be transmitted, processed, stored. Data are information emanations, its self-expressions. Simultaneously data can have many forms, records: literal, sound, digital etc. Therefore they are information carriers (media). It may be assumed that they have material form but are not items. As information is regarded that which can be expounded, decoded from data. For that reason it is possible to possess computer data but be unable to use information contained e.g. because of no acquaintance with the algorithm according to which they are coded. Distinction between terms is important from the legal point of view. Data damaging not always means information damaging, as data acquisition does not have to be information appropriation (compare with: Adamski 2000, 39-40). Computer data have material form but are not items – they are energy impulses (usually electric). Whereas such items as hard discs, floppy discs, CDs and DVDs are data carriers.

Three information attributes are distinguished and protected: availability, integrity and confidentiality (More in: Górski 1994, 283-285).

a) **Availability** is the ability of using information by an authorised person whenever necessary. According to the Recommendation of the Council of the OECD – the characteristic of data, information and information systems being accessible and usable on a timely basis in the required manner (Recommendation, OECD/GD (92) 10). As examples of violations of availability are quoted sabotage, viruses introduction to system, system or network overload of data in excess.

b) **Integrity** according to the OECD definition means the characteristic of data and information being accurate and complete and the preservation of accuracy and completeness (Recommendation, OECD/GD (92) 10). It refers to inviolability of both data and computer systems. In the case of information processed in computer network this means transmitted data is identical to that received. Unauthorised access in order to destroy or modify data or viruses introduction for the purpose of deleting data are among to the most common attacks against integrity.

c) **Confidentiality** assumes access to data only for entitled persons, excluding third parties. It is connected with protection against their being read and copied by unauthorised persons. The OECD Regulation defines confidentiality as: the characteristic of data and information being disclosed only to authorised persons, entities and processes at authorised times and in the authorised manner (*Recommendation,* OECD/GD (92) 10). Forms of infringements of confidentiality are for example unauthorised access to view information, copying data, obtain information during transmission trough the network or eavesdropping.

In the European Community legal definitions of the above mentioned terms may be found in the Regulation (EC) No 460/2004 of the European Parliament and of the Council of the 10th of March 2004 establishing the European Network and Information Security Agency (Official Journal L 77, 13/03/2004 p. 1 – 11).

The first effort to regulate the question of network security in European Community Law was the Council Framework Decision 2005/222/JHA of the 24th of February 2005 on attacks against information systems (Official Journal L 69, 16/03/2005 p. 67 – 71)[18]. Which refers to the term of ”computer data” alike above-mentioned definitions. According to its article 1 they are regarded as ”any representation of facts, information or concepts in a form suitable for processing in an information system, including a program suitable for causing an information system to perform a function”[19]. The definitions result in understanding computer data as information (facts or concepts) emanation, carrier or medium. Information becomes readable for an information system only in the form of computer data. For this purpose it must be ”coded” in binary language – changed into the “0” and “1” sequence and then recorded on a carrier (e.g. CD, DVD or hard disc) or transmitted by network as energy impulses. By this definition as computer data are meant also programs suitable for causing an information system to perform a function: an operating system and applications. In the Penal Code the term of

[18] Poland implemented its regulations with the Act of 24.10.2008 on Amendment to a Law – the Penal Code and Some Other Acts (Journal of Laws 2008 No. 214 entry1344).

[19] The similar definition is included in the Convention on Cybercrime (Convention No. 185 of the Council of Europe on Cybercrime). Poland has signed it but not ratified yet.

"information data" was used, which is identical to the term of "computer data" used in the Framework Decision.

To explain the concept of "information system" it is necessary to refer to the provisions of the Framework Decisions 2005/222 as well. According to it an **information system** means any device or group of inter-connected or related devices, one or more of which, pursuant to a program, performs automatic processing of computer data, as well as computer data stored, processed, retrieved or transmitted by them for the purposes of their operation, use, protection and maintenance[20]. Consequently, in the Framework Decision as an information system is regarded both a single device (e.g. a computer) and group of connected devices, as a network either small (e.g. local area), containing a few computers or a large one, for instance a municipal area. By the expression of "inter-connected or related" the lack of necessity of physical connection (wires) of devices is indicated. Data transmission may occur through another carrier (for example electromagnetic waves). The term of "automatic processing of data" was inter alia defined by the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention No. 108 of the Council of Europe for the Protection of Individuals with regard to Automatic Processing of Personal Data). According to the definition formulated for the purpose of the Convention, as automatic processing of data are regarded actions as follow: storage of data, carrying out of logical and/or arithmetical operations on those data, their alteration, erasure, retrieval or dissemination if carried out in whole or in part by automated means (article 2 of Convention). Automated means refer to actions implemented partially or completely without the involvement of a human being. In passing, it is worth mentioning, that in the Penal Code amendment of the 24th of October 2008 Act, to article 267 point § 2 the term of an "information system" was added without changing the term of a "computer system" [21] in articles 269a and 269b. In

[20] The Convention on Cybercrime includes the concept of a "computer system". Its definition is similar to an "information system", but the scope of the former system is narrower. "A computer system under the Convention is a device consisting of hardware and software developed for automatic processing of digital data. It may include input, output, and storage facilities. It may stand alone or be connected in a network with other similar devices" (Explanatory Report to Convention on Cybercrime, § 23). Therefore a "computer system" is for example a personal computer or a mobile phone, but not a network. A network under the Convention on Cybercrime is an interconnection between two or more computer systems.

[21] The concept of "computer system" was introduced to the Penal Code with the Act of the 18th of March 2004 on Amendment to a Law – the Penal Code, the Code of Criminal Procedure, and the Code of Petty Offences (Journal of Laws. 2004 no. 69 entry 626), which was connected the adaptation of Polish Law to the Convention on Cybercrime regulations. I think that "computer system" should be replaced by "information system".

my opinion the presence of the latter is only an oversight. It should be replaced by an "information system".

In the regulation of article. 267 § 1 the term of **"telecommunications network"** is used, in regulation of art. 269a though the term seemingly with similar meaning – **"data communications network"** appears**.** For the purpose of regulation and unification of the conceptual system the Act of the 4th of September 2008 on Amendment to a Law in Order to Unify Information Terminology was enacted (Dz. U. 2008 no. 171, entry 1056). In case of the term of „data communications system" being used in one of acts mentioned in its contents it refers to the Act of 17 February 2005 on Implementation of the IT Solutions to Entities Executing Public Assignments Activity (Journal of Laws 2005 no. 64, entry 656). According to the definition included in article 3 point 3 of this act, data communications system means: "group of cooperating computer devices and software providing data processing, storage as well as transmitting and receiving through telecommunications networks through appropriate for the network in question final device in the meaning of the Act of the 16th of July 2004 Telecommunications Law (Journal of Laws 2004 no. 171 entry 1800 with amendments)". The term of "telecommunications network", according to this Act (article 2 point 35) means "transmission systems, commutation or redirecting devices and other resources enabling signals sending, reception or transmission through wires, radio waves, optical waves or other means, using electromagnetic energy, regardless of their kind" (More in: Radoniewicz 2011, in press).

To summarise: as information system should be regarded a device or group of related devices processing data, a telecommunications system though, according to Xawery Konarski, means group of cooperating devices, programs and procedures used in order to process data for any distance (Konarski 2004, 62). Telecommunications system therefore is a structure used for processing data and also their transmission between processing data systems, especially an information system connected to telecommunication network for the purpose of data transmission (Konarski 2004, 62).

According to the above mentioned it should be assumed that "data communications network" (that is a group of data communication systems connected to each other) means a telecommunications network in which both computer data processing and their transmission occur. The structure came into existence in connection with a convergence of extensive computer and telecommunication networks (Konarski 2004, 64). In my opinion "data communications network" is a type of "an information system". If in articles 268a and 269b a "computer system" were replaced by "information system" (as I suggest in the earlier part of this paper), "data communications network" would be unnecessary. I therefore suggest that it should cease to be used.

In the regulation of article 267 § 1 breaching electronic, magnetic or other special protection is mentioned. As protection should be regarded any form of impediment in access to information, the elimination of which requires specialised

knowledge, particular device or a code (Wróbel 2006, 1282-1283). Information may be protected directly – e.g. in cipher or an access protection by a password or, in some measure, indirectly - because of computer system protection (as examples firewalls and users accreditation procedure may be referred to). As "breaching" should be regarded action directed to diminish a protective function; it need not mean its destruction (Kardas 2000, 71-72; Kozłowska-Kalisz 2007, 518; Wróbel 2006, 1283).

Taking into consideration the opinions of doctrinal antagonists and the provisions of the Framework Decision, it was assumed that for a perpetrator to commit an offence of hacking the infringement of a protection is not needed, it is enough when it is omitted (an expression "or evading" after the "breaching" was added in § 1). Such "evading" may consist in:

a) human deception (En. *social engineering* that is socio-technique based for example on pretending to be somebody else to wheedle a password);
b) system deception – among methods based on protection evasion in that way is spoofing of IP, ARP or DNS addresses[22];
c) taking advantage of holes (errors) in operating systems, applications, or protocols[23] (for that purpose programs called *exploits* are used).

Provisions of article 267 § 3 penalise installation or using – for the purpose of acquiring information - tapping, visual detection device or other special software. Usage of the last term as a tool of invigilation[24] means without doubt that computer program is considered as such tool. It could be a program such as a Trojan horse or a "back door" (Adamski 2000, 59; Wróbel 2006, 1287).

In the provision of article 268 § 2 the concept of electronic information carrier was used which should not be questionable[25]. Its content consists all data carriers in

[22] *Spoofing* (*masquerade*), that is addresses deception, means action for the purpose of misleading as to the place of communication dispatch. Most frequent is the deception of IP addresses (a logical address of a computer assigned by network administrator) but possible also is deception of ARP, DNS and www addresses (See: Littlejohn Schinder 2005, 284-286).

[23] It is a group of rules describing communication processes. Protocols are responsible for computer identification in a network. To enable data exchange between computers they must use the same network protocol. Two or more protocols functioning in different network layers become a suite. The most popular presently is a suit of TCP/IP (See for instance: Littlejohn Schinder 2005, 234-268; Mandia and Prosise 2002, 147-155).

[24] In the first version of the amendment of the legal project "the special software". was mentioned. During Parliamentary work though the adjective "special" was rightly removed as it could suggest computer programs created only to commit an offence. Whereas in many cases we deal with "double nature" programs, having many functions but which can also be used by criminals (often even against the will and intentions of their authors).

[25] The Act of the 4th of September 2008 on Amendment to a Law for the Purpose of Information Terminology Standardisation (Journal of Laws 2008 no. 171, entry 1056), which in the provision in question changed the ambiguous expression of "the computer information carrier" to "the

"information sense", such as floppy and hard discs (magnetic carriers), CDs, DVDs (optical carriers), semiconductor memories etc.

The article 269b criminalises preparing, obtaining, selling and making available the computer devices and software tailored to the purposes of committing one or more of the offences described in article 165 § 1 point 4, article 267 § 3, article 268a§ 1 or § 2 in connection with § 1, articles 269 § 2 or 269a and preparing computer passwords, entry codes or other data that makes information stored in a computer system or data communications network available. The meaning of the concepts used in the regulation is beyond doubt. However it is puzzling why the legislator did not take into consideration in this article the provisions of art. 267 § 1 § 2 penalising hacking when he quoted other regulations.

Finally, I would like to raise two other questions. Firstly, I would like to pay attention to the expression "without being authorised", which is used by the legislator in article 267 as it has a wider meaning than is usually considered. It should be interpreted taking into account the sense, which is given to it in the Framework Decision 2005/222. According to its article 1: "without right means access or interference not authorised by the owner, other right holder of the system or part of it, or not permitted under national legislation".

The issues of access to the sources of an information system and ability to interfere in data processing, in most cases, are regulated by provisions of "soft law" – internal networks statutes. Whereas the system administrator decides about rights given to a user. In consequence, the expression "without being authorised", means primarily, lack of rights considered in this way and not contravention of the law in force, which rarely regulates this question. Simultaneously, the European Union's legislator gives member states the opportunity of more precise regulation in this subject.

Secondly, in the provision of article 268a, describing features of criminal offence, the expression was used of significant interference or hindering automatic processing, storing or transmitting information data. It is indubitable that the expression is identical to the significant interference with functioning of a computer system or data communications network used in the above-mentioned article 269a (functioning of a computer system or data communications network means exactly processing, storing or transmitting data). Andrzej Adamski (Adamski 2005, 58-59) and Włodzimierz Wróbel (Wróbel 2006, 1309) rightly remark that the provisions of articles 268a and 269a overlap to a certain extent.

---

information data carrier" at the same time indicates that it should be referred to according to the regulation of article 3 point 1 of the Act of the 17th of February 2005 on Implementation of the IT Solutions to Entities Executing Public Assignments Activity. In this regulation "the information data carrier" means "material or a device used for recording and replaying digital or analog data".

I consider it is clearly visible that there is a certain legal "disorder" in the field of information terminology. Undoubtedly it should be standardised and adapted to the system of concepts used in European Community statutes. Defining basic terms (computer data, information system) is indispensable. It seems advisable to add the above-mentioned concepts to the provision of article 115 of the Penal Code (to the definitions of the most important terms)[26]. The rest of them may be defined in other legal acts like as for instance in case of the "telecommunications network", definition of which is found in the Telecommunications Law. In case of some others we may refer to European Union acts binding Poland directly (as for example Regulation (EC) No 460/2004 of the 10th of March 2004 establishing the European Network and Information Security Agency in which in article 4 the concepts of computer data accessibility, integrity and confidentiality were defined). The condition of the situation in question is obviously standardisation of the terminology (More in: Radoniewicz 2009, 68-69).

Bibliography

Adamski, Andrzej. 2005. Cyberprzestępczość - aspekty prawne i kryminologiczne. *Studia Prawnicze* 4: 51-76.

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

Górski, Janusz. 1994. Ocena poufności i bezpieczeństwa systemów informatycznych. In *Prawne aspekty nadużyć popełnianych z wykorzystaniem nowoczesnych technologii przetwarzania informacji. Materiały z konferencji naukowej pod redakcją dr Andrzeja Adamskiego*, ed. A. Adamski, 283-307. Toruń: Wydawnictwo „Dom Organizatora" TNOiK.

Kalisiewicz, Dariusz, ed.1997. *Nowa encyklopedia powszechna PWN. Vol. 2*. Warszawa: Wydawnictwo Naukowe PWN.

Kalisiewicz, Dariusz, ed.1997. *Nowa encyklopedia powszechna PWN. Vol. 3*. Warszawa: Wydawnictwo Naukowe PWN.

Kardas, Piotr. 2000. Prawnokarna ochrona informacji z perspektywy przestępstw komputerowych. Analiza dogmatyczna i strukturalna w świetle obowiązującego stanu prawnego. *Czasopismo Prawa Karnego i Nauk Penalnych* 1: 25-120.

Konarski, Xawery. 2004. *Komentarz do ustawy o świadczeniu usług drogą elektroniczną,* Warszawa: Wydawnictwo Diffin.

Kozłowska-Kalisz, Patrycja. 2007. Rozdział XXXIII. Przestępstwa przeciwko ochronie informacji. In *Kodeks Karny. Praktyczny komentarz,* Marek Mozgawa (ed.), Magdalena Budyn-Kulik, Patrycja Kozłowska-Kalisz, Marek Kulik, 488-509 . Warszawa: Wolters Kluwer Polska.

[26] At least in reference to computer data this is the claim of: Barbara Kunicka-Michalska (Kunicka-Michalska 2005, 581) and Andrzej Marek (Marek 2007, 484).

Kunicka-Michalska, Barbara. 2000. *Przestępstwa przeciwko ochronie informacji i wymiarowi sprawiedliwości. Rozdział XXX i XXXIII Kodeksu karnego. Komentarz*, Warszawa: Wydawnictwo C.H. Beck.

Kunicka-Michalska, Barbara.2005. Rozdział XXXIII. Przestępstwa przeciwko ochronie informacji. In , *Kodeks karny. Część szczególna. Komentarz. Tom II,* Andrzej Wąsek (ed.), Oktawia Górniok, Wiesław Kozielewicz, Emil Pływaczewski, Barbara Kunicka-Michalska, R. Zawłocki, Bogusław Michalski, Jerzy Skorupka*,* 433-614. Warszawa: Wydawnictwo C.H. Beck.

Littlejohn Schinder, Debra. 2005. *Cyberprzestępczość. Jak walczyć z łamaniem prawa w sieci,* Gliwice: Wydawnictwo Helion.

Mandia, Kevin and Chris Prosise. 2002. *Hakerom śmierć!* Warszawa: Wydawnictwo Read Me

Marek, Andrzej.2007. *Kodeks karny. Komentarz*. Warszawa: Wolters Kluwer Polska.

Napierała, Katarzyna. 1997. *Prawne aspekty ochrony danych osobowych przetwarzanych w systemach informatycznych*. Warszawa: Wydawnictwo ABC.

Radoniewicz, Filip. 2009. Postanowienia decyzji ramowej Rady w sprawie ataków na systemy informatyczne a ujęcie cyberprzestępstw w kodeksie karnym. *Ius Novum* 1: 48-69.

Radoniewicz, Filip. 2011. Unification of information terminology in the Polish law – selected issues. *Comparative Legilinguistics (International Journal for Legal Communication)*, in press

Szymczak, Mieczysław, ed. 1995. *Słownik Języka Polskiego*. *Vol. 1.* Warszawa: Wydawnictwo Naukowe PWN.

Wróbel, Włodzimierz. 2006. Rozdział XXXIII. Przestępstwa przeciwko ochronie informacji .In *Kodeks karny*. *Część szczególna. Komentarz do art. 117-277 k.k.,* Andrzej Zoll (ed.), Agnieszka Barczak-Oplustil, Grzegorz Bogdan, Zbigniew Ćwiąkalski, Małgorzata Dąbrowska-Kardas , Piotr Kardas, Jarosław Majewski, Janusz Raglewski, Mateusz Rodzynkiewicz, Maria Szewczyk, Włodzimierz Wróbel, 1234-1314. Kraków: Kantor Wydawniczy Zakamycze.

Convention No. 108 of the Council of Europe for the Protection of Individuals with regard to Automatic Processing of Personal Data, 28 January 1981 http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=108&CM=8&DF=11/08/2009&CL=ENG, Accessed March 15, 2011.

Convention No. 185 of the Council of Europe on Cybercrime, 23 November 2001 http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=8&DF=22/08/2009&CL=ENG. Accessed March 15, 2011.

Explanatory Report to Convention No. 185 of the Council of Europe on Cybercrime, http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=8&DF=22/08/2009&CL=ENG., Accessed March 15, 2011.

Recommendation of the Council of the OECD concerning Guidelines for Security of Information Systems, OECD/GD (92) 10, Paris, 1992. http://www.oecd.org/document/19/0,3343,en_2649_34255_1815059_1_1_1_37441,00.html . Accessed March 15, 2011.