„Krytyka Prawa", tom 8, nr 2/2016, s. 126–156, ISSN: 2080-1084 Copyright by Akademia Leona Koźmińskiego

MAŁGORZATA SKÓRZEWSKA-AMBERG[1]

Criminal-law protection against cybercrime in Poland: Successful harmonisation or unachieved task?

Abstract

The aim of this paper is to address the issue of implementation of international legal instruments regarding cybercrime into the Polish criminal law.

Effective protection against cybercrime requires, among other things, the establishment of an appropriate legal framework. Criminal prohibitions of a deterrent effect, which are a part of this framework, seem of particular importance. In Europe such a set of rules is provided for in the instruments of the Council of Europe as well as in the European Union instruments. As a member of both these international organisations, Poland is obliged to implement their standards.

The author's aim is to analyse whether and, if so, to what extent the current Polish criminal legislation is in line with European requirements. The process of implementation of these norms has expanded in the span of over 10 years and was initiated even before Poland accessed the European Union. Polish criminal law, however, is not yet fully compliant with international requirements on cybercrime. This paper is an attempt to identify some areas of the criminal law which are still to be amended as well as to submit some solutions *de lege ferenda*.

Keywords: cybercrime, cyberspace, integrity, confidentiality, computer forgery, identity theft, computer fraud, child pornography, child abuse, grooming

[1] PhD Małgorzata Skórzewska-Amberg – Department of Theory and Philosophy of Law; e-mail: mskorzewska@kozminski.edu.pl.

„Krytyka Prawa", tom 8, nr 2/2016, s. 126–156, ISSN: 2080-1084 Copyright by Akademia Leona Koźmińskiego

MAŁGORZATA SKÓRZEWSKA-AMBERG

Prawnokarne regulacje cyberprzestępczości w Polsce: udana harmonizacja czy niewykonalne zadanie?

Streszczenie

Celem opracowania jest analiza polskiego prawa karnego dotyczącego cyberprzestępczości, a w szczególności analiza ich zgodności z regulacjami przyjętymi przez Radę Europy i Unię Europejską.

Proces wdrażania norm ustanowionych na forum europejskim został w Polsce zainicjowany jeszcze przed wstąpieniem do UE i trwa już od ponad dekady. Polskie prawo karne nie jest jednak jeszcze w pełni zgodne z międzynarodowymi wymogami dotyczącymi cyberprzestępczości. Niniejszy artykuł jest próbą identyfikacji pewnych obszarów prawa karnego, które powinny zostać zmienione, a także przedstawienia rozwiązań *de lege ferenda*.

Słowa kluczowe: cyberprzestępczość, cyberprzestrzeń, integralność, poufność, fałszerstwo komputerowe, kradzież tożsamości, oszustwo komputerowe, pornografia dziecięca, wykorzystywanie dzieci, grooming

 DOI: 10.7206/kp.2080-1084.113

Introduction

Along with the development and globalisation of computer networks, in particular the Internet, we have seen quick prevalence of types of conduct regulated by the law but committed in the new environment, such as fraud, as well as completely new types of conduct, strictly related to the digital form of data, such as hacking.

Because of the profound dependence of the information society on information and communication systems, and primarily on access to reliable information, the issue of cybercrime will continue to rise. If we consider that various estimates show that in the early 21st century profits from computer crime exceeded profits from drug trafficking and currently reach the level of income from both legal and illegal weapons trade[2], we can see how big a problem it is.

Criminal law, whose primary task is to protect the rights of individuals, both by protecting goods which are essential for the development of individuals, as well as by mending the wrongdoing which the victim has suffered – in so far as this is possible, must make an effort to meet the needs of the technological revolution that is taking place before our eyes every day.

The correlation of criminal law with reality of the digital world is not easy. On one hand we have a collection of repressive standards, which should be shaped most precisely; on the other hand there is a rapidly changing reality, which can immediately adapt to the variables which define it. In addition, the language of cyberspace is not always easily translatable into the language of law. Consequently, in many cases the law, in particular criminal law, which is quite self-contained, must develop a new way to depict reality. This description should remain highly precise on one hand, and on the other support a much wider description of unwanted conduct, including various types of conduct which do not exist today. Is it a paradox or a necessity? Or perhaps a paradoxical necessity...

Undoubtedly, one of the key issues relating to cybercrime is the vast nature of the global network, and thus different territorial affiliation of network nodes. In the second half of the 20th century, two opposing concepts of the legal system in cyberspace were shaped. According to one of those concepts, an autonomous and

[2] B. Mejssner, *Niezbite cyfrowe dowody*, http://cio.cxo.pl/artykuly/55536/Niezbite.cyfrowe.dowody.html (12.01.2016).

sovereign legal system in cyberspace should be established[3], whereas the other concept argues that legal activities performed in the virtual reality apply to physical entities and consequently are subject to the legal power of the place of residence.[4]

It should be stressed that these concepts mainly pertained to the issues related to commercial transactions online. Today, one of the most urgent issues of the global network are violations which belong to the domain of criminal law – and criminal law should not remain outside the control of the machinery of the state.

It seems that the only effective solution is the convergence of legal systems and standardisation of law in strict international cooperation. A certain example in this scope is provided by international conventions or legislation of the European Union, which establishes a legal framework for the internal laws of the Member States.

The purpose of this article is to make an attempt at analysing the compliance of the Polish criminal law with European regulations and an attempt at choosing *de lege ferenda* solutions in those fields which need adapting. Due the vast scope of the subject, the deliberations are limited to the substantive criminal law incorporated in the provisions of the Penal Code.

Offences against the confidentiality, integrity and availability of computer data and systems

The existence of information in a digital form, their processing, storage, and sharing in such form is one of the fundamental features of the information society.

Confidence in the information and communication systems, the documents and data stored in such systems, possibility of a free and exclusive disposal of the information possessed, freedom to decide on the scope and nature of the data to be disclosed, and the right to protect the confidentiality of the data, belong to the catalogue of protected rights of the individual and more specifically concern the sphere of his freedom and security, upheld by the criminal law.

The protection of the security of computer systems and computer data on a European level is governed by two basic acts: Council of Europe Convention on Cybercrime (Budapest Convention, CETS No. 185) and Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against

---

3 I.T. Hardy, *The Proper Legal Regime for Cyberspace*, "University of Pittsburgh Law Review" 1994, 55; D.R. Johnson, D. Post, *Law and Borders – the Rise of Law in Cyberspace*, "Stanford Law Review" 1996, 48(5).

4 J.L. Goldsmith, *Against Cyberanarchy*, "University of Chicago Law Review" 1998, 65(4); C. Reed, *Internet Law: Text and Materials*, Cambridge 2004.

 DOI: 10.7206/kp.2080-1084.113

information systems and replacing Council Framework Decision 2005/222/JHA (OJ L 218, 14.08.2013, pp. 8–14).

Both of these acts accordingly define a catalogue of crimes, which includes:

1) illegal access to a computer system, i.e. intentional and unauthorised access to the whole or any part of a computer (Article 2 of the Convention, Article 3 of the Directive);
2) illegal interception of data, i.e. intentional and unauthorised interception – by technical means – of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data (Article 3 of the Convention, Article 6 of the Directive);
3) illegal data interference, i.e. intentional and unauthorised modification of computer data, including their deletion, deterioration, concealment, alteration or suppression (Article 4 of the Convention, Article 5 of the Directive);
4) illegal system interference, i.e. intentional and unauthorised seriously hindering or interrupting the functioning of a computer system by data transmission or modification, including their input, deletion, deterioration, alteration and suppression (Article 5 of the Convention, Article 4 of the Directive);
5) misuse of devices, i.e. possession, production, sale, procurement for use, import, distribution or otherwise making available of the devices, including computer software, passwords and access codes or similar data, that allow the breaches of confidentiality, integrity and availability of data and computer systems (Article 3 of the Convention, Article 6 of the Directive).

For the purposes of the Convention, a computer system is any device or group of interconnected devices, one or more of which, pursuant to a programme, performs automatic processing of data (Article 1(a)), while computer data means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a programme suitable to cause a computer system to perform a function (Article 1(b)) The Directive defines these terms in similar way (Article 2(a) and 2(b)). In addition, the directive clarifies the term illegal (without right) – recognising that such conduct is not authorised by the owner or by another right holder of the system or of part of it, or not permitted under national law (Article 2(d)).

In Polish law, in Article 3(3) of the Act on Informatisation of Operations of Entities Executing Public Tasks of 17 February 2005 (consolidated text: Journal of Laws of 2014 item 1114), an electronic system is defined as a set of cooperating devices and software ensuring processing, storing, sending and receiving of data in telecom-

munication networks.[5] However, there is no legal definition of computer data, so it seems that the definition of this concept proposed by the Convention on Cybercrime and the directive on attacks against information systems should be used.

Polish criminal law aims to protect the integrity of and access to information, stored and processed in data communication networks and the integrity and security of computer systems. The broad subjective right to dispose of such information[6] is also protected by law, in particular through the constitutionally guaranteed right to privacy and secrecy of communication.[7]

Article 267 of the Penal Code, in § 1 imposes penalties on illegal opening of a sealed document, unlawful connecting to telecommunication networks, or breaching or by-passing electronic, magnetic or other special protection of the information, in § 2 – violation of the integrity of information system, and in § 3 – unauthorised installing, or handling any tapping, visual or any other device, software or technology.

Unauthorised destroying, damaging, removing or altering the recording of the relevant information or in other ways foiling or obstructing an authorised person's access to the content of such information is penalised in Article 268 § 1 of the Penal Code. The liability of the perpetrator is enhanced in case the action is linked to computer information carrier[8] (Article 268 § 2 of the Penal Code) or causes considerable economic loss (Article 268 § 3 of the Penal Code).

Article 268a of the Penal Code imposes penalties on unauthorised access to computer data and disrupting to a significant degree or preventing the automatic collection, processing or transmission of such data. It seems that this provision, which concerns matters governed by Article 4 of the Convention and Article 5 of the Directive does not fully comply with the requirements of these regulations. Article 268a § 1 of the Penal Code „Whoever, without being authorised to do so, destroys, damages, removes, alters or impedes the access to IT data (...)" suggests that only the access to such data is protected and not the integrity of the data themselves, which seems to be the goal of Article 4 of the Convention and Article 5

---

5 Processing takes place with the use of an end device, appropriate for a given type of network, destined to be plugged directly or indirectly to the ending of the network (so called telecommunication end device), pursuant to Art. 2(43) of the Act of 16 July 2004 – Telecommunication Law (consolidated text: Journal of Laws of 2014 item 243 as amended).

6 W. Wróbel [in:] A. Zoll (ed.) *Kodeks karny. Część szczególna. Tom II, Komentarz do art. 117–277 k.k.*, Warszawa 2008, p. 1287.

7 A. Marek, *Kodeks karny. Komentarz*, Warszawa 2010, p. 570; J. Piórkowska-Flieger [in:] T. Bojarski (ed.) *Kodeks karny. Komentarz*, Warszawa 2012, p. 701.

8 Defined in Article 3(1) of the Act on Informatisation of Operations of Entities Executing Public Tasks of 17 February 2005 (consolidated text: Journal of Laws of 2014 item 1114) – as a material or a device used to record, store and read data in digital format.

 DOI: 10.7206/kp.2080-1084.113

of the Directive. Therefore, the scope of criminalisation introduced by that regulation is not clear. The protection covered by Article 268a § 1 of the Penal Code should be augmented by the protection of the actual information and not merely of the access to the information. When it comes to the case of Article 267 § 1 of the Penal Code, the criminalisation of acquiring access to information seems adequate (since it is not significant whether the perpetrator is able to read the particular information or not, being able to do so when it comes to secured information is what is really important). However, in the case of Article 268a § 1 of the Penal Code it appears that actions such as „destroying, damaging, removing, altering" should refer to the actual data, while „impeding" – should concern the access to data of this kind.

Article 269 of the Penal Code protects the computer data of particular importance for national defence, safety and security of transport and functioning of governmental administration, other state authority organs, or state or local government.

Seriously disturbing the functioning of a computer system or data communication network through unauthorised violation of its integrity or transmission of computer data is criminalised in Article 269a of the Penal Code.

Consecutively, Article 269b § 1 of the Penal Code lays down penalties on the construction, disposal or sharing with others of any devices or computer software modified in order to perpetrate enumerated offences (such as i.a. compromising the integrity, tapping or impeding access to certain data, notably preventing the operation of a computer system). The punishment is also applicable to actions concerning computer passwords, access codes or data which facilitate prohibited access to information saved in computer systems or in communication networks. The absence of an unambiguous definition of what sort of information gathered in a computer system or in an IT network to be guarded leads to a provision that places penalties on any kind of behaviour which involves admittance to any information in a data communication network (for example links to certain Web pages). A mere straightforward amendment to the provision may entirely change its applicability in practice. This still being in accordance with the expected intention of the legislator. Hence, instead of „access to information stored on a computer system or a data communication network", the following wording is proposed „access to secured information stored on a computer system or a data communication network".

Although offences against the confidentiality, integrity and availability of computer data and computer systems in the Polish Penal Code are governed primarily in the chapter concerning offences against the protection of information, also the provisions related to offences against documents can be applied to this

sphere. More specifically, Article 276 of the Penal Code prescribes criminal sanctions against a person who destroys, damages, hides, eliminates or makes a document unusable, withouth holding the rights to exercise exclusive control over the document.

The destruction of a document could take the form of destroying the carrier of the document or destroying the data recorded on the carrier.[9]

Hiding the document storage place meets the criteria of concealing a document, while preventing access to the document, e.g. by locking it in an armoured closet, meets the criteria of removal of the document.[10] Thus preventing or hindering the access to the document referred to in Article 276 of the Penal Code also meets the criteria of concealing a document.[11] Concealing a document within the meaning of Article 276 of the Penal Code may also include „the denial of possession of a document, keeping the possession of the document and failure to give the document, in spite of the request, to the entitled person".[12]

Hence, it may be concluded that preventing access to an electronic document, for example by changing the access codes, can also be seen as a form of concealment of the actual document.

Computer related crimes

Criminal law distinguishes two types of attacks related to computer crime: attacks against computer systems (offenses against the confidentiality, integrity and availability of data and computer systems) and computer related crime, where the computer systems are used as a tool to violate the legal rights traditionally protected by criminal law.[13]

There are two computer related crimes indicated in the Convention on Cybercrime: computer related forgery (Article 7), i.e. intentional and unauthorised modification of computer data – their input, alteration, deletion or suppression –

---

9 W. Wróbel [in:] G. Bogdan, K. Buchała et al. (eds.), *Kodeks karny. Część szczególna. Komentarz do k.k.*, t. 2, Kraków 1999, 1059.

10 Ibidem, p. 1060.

11 See the judgment of the Supreme Court of 23 May 2002 (V KKN 404/99, OSNKW 2002, Vol. 9–10, item 72): „A person may be accused of the crime provided under Article 276 of the Penal Code, consisting of concealing a document specified therein, only when it is indicated that he/she himself/herself took an action to conceal a document, to which he/she had no exclusive right of disposition, from a person authorised to dispose of the same i.e. the document was put in a place such person is not aware of or has no or difficult access to (...)".

12 The judgment of the Supreme Court of 9 August 2000 (V KKN 208/00, OSNKW 2000, Vol. 9–10, item 84).

13 A. Adamski, *Prawo karne komputerowe*, Warszawa 2000, pp. 30–31.

 DOI: 10.7206/kp.2080-1084.113

made in order to use the revised data as authentic (regardless whether or not the data is directly readable and intelligible), and computer related fraud (Article 8), i.e. the intentional and unlawful causing of a loss of property to another person by modifying (input, alteration, deletion or suppression) computer data or other interference with the functioning of a computer system with the intent of procuring, without right, an economic benefit for oneself or for another person.

Spoofing, i.e. tampering with network services and protocols in order to hide the identity (i.a. IP spoofing[14], e-mail spoofing – including phishing, web spoofing – including pharming), is an example of fraud carried out in a computer system.

From the point of view of cybercrime, nearly two decades have passed since the drafting of the Convention on Cybercrme, which is an extremely long period. During that time, new methods of committing crimes with the use of ICT systems have been developed. At least one of those requires special attention. Despite the fact that international regulation, referred to in this article, does not, *expressis verbis*, indicate identity theft, the growing threat of this phenomenon is the reason why identity theft appears in this analysis.

Computer related forgery

Computer forgery can be employed in connection to both forgery of traditional documents, produced by computer hardware and software (for example counterfeiting of official forms using a scanner and software for the processing of graphic documents), as well as forgery of a document originated, stored or transmitted in electronic form (for example changes in electronic trade books).

The objective of legal document protection is not merely to protect the information as such, but also, and above all, to ensure trustworthiness of documents, and hence maintain confidence in legal transactions.

An electronic document has been defined in Article 3(2) of the Act on Informatisation of Operations of Entities Executing Public Tasks of 17 February 2005 (consolidated text: Journal of Laws of 2014 item 1114) as a set of data constituting a separate meaningful whole, organised within a defined internal structure and

[14] Used e.g. in connection to *network weaving*, also called *connection laundering*; it occurs when somebody with the purpose of making it difficult to disclose his or her identity reaches the host through several servers, each time changing identity (e.g. by altering the source address in the Internet protocol – *IP spoofing*), Garfinkel S., Spafford G., *Bezpieczeństwo w Unixie i Internecie*, Warszawa 1997, p. 436.

recorded on an IT data carrier[15], where an IT data carrier is a material or a device used to record, store and read data in digital or analogue format (Article 3(1)).

In accordance with Article 115 § 14 of the Penal Code, a document is any object or any other carrier of recorded information to which a specified right is attached or which, due to its content, evidences a right, legal relationship or legally relevant circumstances.

In the literature, one can also come across the view that, according to Article 115 § 14 of the Penal Code, „all documents are purely material", because a „recorded carrier" is a document, and the definition of a computer carrier of information indicates that it is a carrier on which the content was recorded in the manner specified for the appropriate carrier.[16]

However, it seems that it should not be prejudged that a document carrier is a physical object. Since, within the meaning of the Penal Code, the substance of a document is determined solely by whether a specific right is attached to the same or whether it includes a legally relevant content[17], a recorded intangible information carrier should be considered as a document as well. It is clear that a document must be submitted in a physically available format. It is therefore considered that both tangible and intangible carriers of the collected, processed or transmitted IT data are protected by criminal law.

The provisions with regard to offenses against credibility of documents preserve the confidence in legal transactions. Such confidence is based on trust with regard to the content of the document. On account of the content of the document, the document is considered proof of a right, but to be considered as such, the registered information carrier, either tangible or intangible, must emerge in visible form.

Legally protected interests connected with a document may be compromised by physical falsification – Article 270 § 1 of the Penal Code: "whoever, in order to use it as authentic, forges or alters a document or uses such forged or altered document"[18]

---

15 Besides, the definition of a document is also included in Article 2(5) of the Act on Protection of Classified Information of 5 August 2010 (Journal of Laws No. 182 item 1228, as amended), which provides that recorded classified information is also to be considered a document; Article 5(2) of the Act on Electronic Signature of 18 September 2001 (consolidated text: Journal of Laws of 2013 item 262 as amended) considers the data in electronic form bearing a secure electronic signature verified by a valid qualified certificate to be equivalent in terms of legal effects to the documents bearing handwritten signatures, if separate provisions do not state otherwise.

16 A. Wąsek [in:] O. Górniok et al. (eds.), *Kodeks karny. Komentarz. Tom I*, Gdańsk 2005, p. 856.

17 J. Piórkowska-Flieger, *Fałsz dokumentu w polskim prawie karnym*, Lublin 2003, cited after A. Wąsek [in:] O. Górniok et al. (eds.), op. cit., pp. 855–856.

18 R. Zakrzewski, *Ochrona wiarygodności dokumentów w nowym kodeksie karnym*, "Przegląd Ustawodawstwa Gospodarczego" 1999, 7–8, p. 6.

 DOI: 10.7206/kp.2080-1084.113

or intellectual falsification of such document: whether direct – Article 271 or indirect – Article 273 of the Penal Code.

Direct intellectual falsification of a document, i.e. giving false testimony regarding circumstances with legal significance by a person authorised to issue a document (Article 271 § 1 of the Penal Code), as well as indirect intellectual falsification of a document, i.e. using a document containing false testimony (Article 273 of the Penal Code) are omitted, as irrelevant from the point of view of the present subject.

Article 270 § 1 of the Penal Code provides for two forms of document falsification – forgery and alternation, not only of an entire document but also the alternation or forgery of any part of the same[19], e.g. a signature or a date.[20] The Supreme Court, in the judgment of 27 November 2000 (III KKN 233/98) ruled, that „a document is forged when it does not come from the person in the name of whom it has been prepared and it is altered when an unauthorised person makes changes to an authentic document".[21]

A person who makes preparations for the offenses referred to in Article 270 § 1 and 2 of the Penal Code is also subject to criminal sanctions.

Despite some claims in the literature that electronic documents may cause unclear qualification of an act of manipulating the content of such documents (in particular alteration of the same), some concerns may be raised as to whether manipulating the content of a digital document meets the criteria of an act prohibited under Article 270 § 1 of the Penal Code or whether such activity should be treated as a computer fraud prosecuted under Article 287 § 1 of the Penal Code. According to Grzegorz Kopczyński[22], the problem of such differentiation arises as the falsification of electronic documents is not identified in the Penal Code. It seems that the alteration of the content of an electronic document – i.e. giving it a different content than the original one – should always be treated, in accordance with Article 115 § 14 of the Penal Code, as document forgery, therefore an offense referred

---

19 See the decision of the Supreme Court of 8 April 2002 (IV KKN 421/98): „Alteration of the document, within the meaning of (...) Article 270 § 1 of the Penal Code, may also consist in writing something in addition, without the consent of the victim".

20 J. Piórkowska-Flieger, *Przestępstwa przeciwko wiarygodności dokumentów w nowym kodeksie karnym*, "Przegląd Sądowy" 1997, 10, p. 11.

21 Similarly, in the judgment of 5 September 2000 (II KKN 569/97), the Supreme Court ruled that: „The crime provided in Article 265 of the Penal Code of 1969 (identical to the one under Article 270 the Penal Code of 1997) may be committed in two ways. One is making a letter to appear as a document to create an impression that the content of the same comes from the issuer mentioned therein, while in fact this is not the case (forgery). The other is changing the content of an existing authentic document by the perpetrator (alteration)".

22 Cf. G. Kopczyński, *Pojęcie dokumentu i fałszu materialnego w nowym kodeksie karnym*, [in:] L. Bogunia (ed.), *Nowa Kodyfikacja Prawa Karnego*, Vol. II, Wrocław 1998.

to in Article 270 § 1 of the Penal Code. A situation in which an electronic record is modified in order to obtain financial gains or to cause harm to a person should be considered as a concurrence of regulations.[23]

Article 310 § 1 of the Penal Code provides for penal sanctions i.a. for forging or altering money or other means of payment and documents entitling to a sum of money. In accordance with the doctrine, this regulation also protects plastic money and electronic money, among other things, as both aforesaid types of money „are accepted as means of payment in trade and used to discharge payment obligations"[24] and thus, „they may appear as designations of "other means of payment" referred to under Article 310 § 1 of the Penal Code".[25]

Electronic money is defined in Article 2.21a of the Act of Payment Services (consolidated text: Journal of Laws of 2014 item 873 as amended) as monetary value kept in an electronic (including magnetic) format, issued – with an obligation to redeem the same – for the purpose of payment transactions and accepted by entities other than the sole issuer of such electronic money. Besides, the same act defines a payment instrument as a personalised device or a set of procedures agreed upon by the user and the provider, used by the user to place a payment order[26] (Article 2(10)) and a payment card as a card that authorises cash withdrawals or allows to place a payment order (Article 2(15a), as well as a debit card – Article 2(15aa) and a credit card – Article 2(15ab)).

The concept of „other means of payment", as expressed in Article 310 § 1 of the Penal Code permits to extend the protection provided by the provision also to payment instruments, payment cards, as well as electronic money. This is exceedingly important, particularly in cases where a financial transaction is accomplished by means of electronic communication, as well as with regard to the recurrent replacement of a tangible security carrier by a digital one.

Making preparations for the offense under Article 310 § 1 of the Penal Code, e.g. through the creation or distribution of programmes which can generate credit card numbers, is punishable under Article 310 § 4 of the Penal Code.

---

23 See the judgment of the Court of Appeal in Lublin of 30 March 2000 (II Aka 41/00): „In the case where the offender forged or altered a document, and then made use of it (...) to bring another person to an unfavorable disposition of property, it must be concluded that he is guilty of two offenses: forgery of a document (Article 270 § 1 of the Penal Code) and fraud (Article 286 § 1 of the Penal Code)".

24 J. Skorupka, *Przedmiot ochrony przestępstwa z art. 310 k.*, "Palestra" 2002, 7–8, p. 68.

25 Ibidem.

26 Statement made by the payer or recipient addressed to his supplier, containing an instruction to execute a payment transaction – Article 2(36) of the Act on Payment Services.

 DOI: 10.7206/kp.2080-1084.113

Computer related fraud

In the Polish Penal Code, the legislator distinguishes two types of fraud: „normal" – defined in Article 286 § 1 of the Penal Code and „computer fraud" – defined in Article 287 § 1 of the Penal Code.

Fraud, in the light of Article 286 § 1 of the Penal Code, means bringing another person to unfavourable disposition of his own or someone else's property by misleading this person or making use of any mistake, as well as taking advantage of this person's inability to assess properly the actions taken. Misleading describes behaviour intended to cause a false perception of reality. Taking advantage of a person's inability to assess properly the actions taken, means persuading this person to dispose of any property, at a moment when he or she is not in a position to properly assess the significance and consequences of their actions.[27] Such inability may be permanent or temporary, or even momentary.

The criminal character referred to in Article 286 of the Penal Code concerns an offence directed towards a person – a subject, who can make a misstep, or be in a situation lacking an appropriate understanding of the actions in question. The problem emanates in connection to the economic benefits procured by the offender, or the wrong induced through the offender's action or a consequence of a data processing system. In such circumstances the apparatus can not be blamed, for the way of its action is directed by a human who has control over it. From the perspective of the topics here discussed, two issues are of significant interest: firstly, mistake of the person responsible for the software; secondly, human action with the aim of causing damage or gaining a benefit. Such actions can consist in changing the software, submitting incorrect data or manipulating the outcome of data processing.

Criminal liability for computer fraud is described in Article 287 of the Penal Code as fraud committed with the use of devices for automatic processing, storing or transferring of data and comprises no element of the offender's misleading another person or making use of his or her mistake. To exhaust the constituent elements of the offence, the fact of technological influence on data processing is essential. The activity of the offender who acts in order to obtain a financial benefit or to cause damage to another person, is not aimed directly at the wronged person.[28] Not only the activity consisting in changing (or erasing) data stored in the

---

27 J. Skorupka, *Wady oświadczenia woli w wybranych przestępstwach gospodarczych*, "Przegląd Sądowy" 2000, 4, p. 45.

28 B. Michalski [in:] *Kodeks karny. Część szczególna. Tom II. Komentarz pod redakcją Andrzeja Wąska*, Warszawa 2010, p. 1174.

computer system, modifying or interfering with data processing software operation or changing the information as a result of processing, but also mechanical interference with data processing devices or connecting to the system of data transmission, meet the criteria of the offence described in Article 287 § 1 of the Penal Code. Change, deletion or entry of data, i.e. modification of information on a data storage device, meet the criteria of the offence set out in Article 287 § 1 of the Penal Code. Such modifications can be made both to the actual data storage device and to the computer system. The criminal offence may imply for example diverting bank transfers or an equivalent modification of a financial operation which produces additional interest in the bank account of an unauthorised person. A different illustration of computer fraud is the so called carding, which involves the use of money from a credit card where the number has been stolen, for example while executing financial activity on the Internet.

Article 287 of the Penal Code protects the property, i.e. all the proprietary rights confirmed by the record in the system storing, processing or automatically transmitting the data or the record on a computer data carrier, or property which refers to such record.[29] Thus if IT data are not connected with proprietary rights, violation of their integrity is not subject to the provisions of property protection but is subject to the provisions described in the chapter referring to the offences against protection of the information.

The condition for being liable under Article 287 of the Penal Code is that the activity intended to obtain a financial benefit or cause damage to another person.

Identity theft

Identity theft is a form of misappropriation of somebody's identity, impersonation of another individual by taking on another person's identity. This is generally done with the aim to cause harm or to gain an unjust advantage. Identity theft occurs when a person uses information which confirms the identity of another person (for example somebody's name and surname), without the approval of the person in question and with the purpose to cause harm. Nevertheless, the term identity theft is not entirely sufficient. It is really very difficult to treat identity as something which is even possible to steal.

Identity theft, and more specifically impersonating another person, is criminalised in Article 190a § 2 of the Penal Code, which imposes penalties with regard to an offender who is pretending to be another person, uses an image or other personal information of that person – in order to cause personal or financial harm.

[29] P. Kardas, B. Michalski, *Przestępstwa przeciwko mieniu*, Warszawa 1999, p. 220.

 DOI: 10.7206/kp.2080-1084.113

Article 6(2) of the Data Protection Act of 29 August 1997 (consolidated text Journal of Laws of 2014 item 1182), defines personal data as any information relating to an identified or identifiable natural person. Therefore, „personal data are any information relating to an identified, or capable of being identified, person, and not only such information which is used to identify a person".[30] However, it is not always clear if e.g. information about digital profiles (such as e.g. username, login or password) can always be considered as personal data. Doubts concerning the digital profiles can therefore result in excessively narrowing the protection.

It is clear from Article 190a § 2 of the Penal Code, that the aim of the perpetrator is to cause harm to the impersonated individual. It may raise doubts, however, in a situation where the perpetrator accepts that the impersonated person can suffer harm, but the real aim of the perpetrator's action is to cause harm to someone else entirely. It seems that regardless of the questions raised in relation to this provision, it could be worth considering erasing the determination of the person to whom the offender causes harm and to leave the provision as follows „subject to the same punishment shall be whoever pretends to be another person, uses his or her image or other personal information in order to cause personal or financial harm...".

There is no doubt that Article 190a § 2 of the Penal Code penalises only such behaviour of the offender which concerns a really existing person. The data of a fictitious person are not personal data within the meaning of the Data Protection Act.

Offences related to child pornography

On a European level the subject of child pornography is governed by three basic instruments: Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA (OJ L 335, 17.12.2011, pp. 1–14)[31], Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Convention) and Convention on Cybercrime. However, the extent of sexual crimes

30 J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych. Komentarz*, Warszawa 2011, p. 334.

31 Adopted as Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA (OJ L 335, 17.12.2011, pp. 1–14), number of the Directive amended by Corrigendum to Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA (OJ L 18, 21.01.2012, p. 7).

against children is wide, therefore this analysis will focus only on those crimes that are primarily committed in cyberspace, i.e. child pornography, solicitation of a child for sexual purposes (grooming) and the presentation of pornographic material to children.

Child and child pornography – the definition of terms

The definition of a child adopted internationally specifies that child means every person who has not attained 18 years of age. Such a definition can be found in Article 1 of the Convention on the Rights of the Child of 20 November 1989 – child means every human being below the age of eighteen years unless under the law applicable to the child, the majority is attained earlier. The aim to protect youth below the age of 18 years is also the objective of the Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography. Also Article 9(3.a) of the Budapest Convention defines a minor as every person under the age of 18 years; however, every Party may require a lower age-limit, but this limit can not be lower than 16 years. Article 3 of the subsequent Lanzarote Convention determines any person under 18 years of age as a child.

Article 2(a) of the Directive on combating the sexual abuse and sexual exploitation of children and child pornography, provides that a child is a person below the age of 18 years. The directive also introduces the concept of age of sexual consent, i.e. age below which, in accordance with the national law, it is prohibited to engage in sexual activities with a child. Also, the Lanzarote Convention in Article 18(2) indicates the need to define in the national law the child's age below which it is prohibited to engage in sexual activities with his participation.

The term minor, as used by Polish criminal law, means a person who has not attained 18 years of age. The age of sexual content is defined at 15 years.

In various international documents child pornography is defined similarly and consistently – as any representation, by whatever means, of a child engaged in real or simulated explicit sexual activities or any representation of the sexual parts of a child for primarily sexual purposes (Article 3(1.c) of the Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography, Article 1(2) of the Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse). The Convention on Cybercrime on the one hand narrows the definition of child pornography defining it as any pornographic material which visually depicts a minor engaged in sexually explicit conduct (Article 9(2.a)). On the other hand, it extends the definition, deeming as child pornography also pornographic material which depicts a person appearing to be a minor engaged in sexually explicit conduct or realistic images representing

 DOI: 10.7206/kp.2080-1084.113

a minor engaged in sexually explicit conduct. However, the Convention leaves the recognition of such material as child pornography to the discretion of each Party (Article 9(4.4) provides for the possibility of reserving the right not to apply, in whole or in part, Article 9(2.b) and Article 9(2.c) of the Convention).

The broadest definition is contained in the EU directive on combating the sexual abuse and sexual exploitation of children and child pornography. Child pornography is defined in Article 2(c) as any material that for primarily sexual purposes visually depicts a child, any person appearing to be a child or realistic images of a child, engaged in real or simulated sexually explicit conduct, as well as any depiction of the sexual organs of a child or any person appearing to be a child – including realistic images of the sexual organs of a child. The term realistic indicates that it is a so-called simulated child pornography, i.e. material produced in a way that does not involve a specific child, but is generated artificially (for instance when the material is produced as a result of a combination of many „innocent" images). An important change compared to the pre-existing solutions is the exclusion of the possibility to exclude any part of the definition by EU Member States.

The Directive, by introducing the above-mentioned definition as a minimum, requires that, in relations to the provisions of the Polish criminal law, at least such definition could be considered as binding (especially considering that there is no legal definition of child pornography in Polish law, although it would be advisable to adopt such definition).

Child pornography

The adopted documents require that EU Member States, as well as the countries belonging to the Council of Europe, adopt measures enabling prosecution of i.a. producing, making available, possessing and distributing child pornography by use of information systems.

It is forbidden by the Convention on Cybercrime, according to Article 9(1), to produce child pornography for the purpose of its distribution through a computer system, as well as offering, making available, distributing and transmitting child pornography with the use of a computer system. The recognition as an offence the procurement of child pornography through a computer system or possession of child pornography in a computer system or on a computer-data storage medium is left by the Convention to individual Party's decision as set out in Article 9(4), with the right not to apply in whole or in part Article 9(1.d), 9(1.e), and Article 9(2.b) and 9(2.c).

Offering, making available, distributing, transmitting and procuring child pornography for oneself or another person (Article 20(1.b)–20(1.d)) is also prohi-

bited by the Council of Europe Convention on the protection of children against sexual exploitation and sexual abuse. Any of the Parties may decide that producing and possessing child pornography (Article 20(1.a) and Article 20(1.e) respectively) is not punishable, in whole or in part, if it consists exclusively of simulated representations or realistic images of a non-existent child, and when it involves children who have reached the age of sexual consent where these images are produced and possessed by them with their consent and solely for their own private use. Criminalisation of knowingly obtaining access, through information and communication technologies, to child pornography, as provided for by Article 20(1) f of the Lanzarote Convention, remains at the sole discretion of the Parties to the Convention, subject to Article 20(4).

Directive on combating the sexual abuse and sexual exploitation of children and child pornography Article 5 imposes the requirement to ensure that the production, acquisition, possession, distribution, dissemination, transmission, offering, supplying of child pornography or making it available is punishable. Also knowingly obtaining access, by means of information and communication technology, to child pornography is punishable.

Criminal liability in respect of these activities may be excluded if the person appearing to be a child was in fact 18 years of age or older at the time of depiction (Article 5(7)).

Article 5(8) of the Directive allows the Member States to decide not to make producing and possessing of simulated pornography punishable if it remains in the possession of the producer for their exclusive private use and the production did not require any material depicting a child or sexual organs of the child or an adult which appeared as a child or sexual organs of the adult. It will be within the discretion of Member States to decide whether liability is excluded with regard to the production, acquisition or possession of material involving children who have reached the age of sexual consent where that material is produced and possessed with the consent of those children and only for the private use of the persons involved, in so far as the acts did not involve any abuse (Article 8(3)).

The Polish criminal law prohibits the production, fixation, storage, possession or acquisition of pornographic materials with a minor (Article 202 §§ 3–4a of the Penal Code). Various paragraphs of Article 202 differentiate the penalty depending on the activities pursued. The legislation provides the strictest penalty (from 2 to 12 years of imprisonment) for conduct described in Article 202 § 3 of the Penal Code, i.e. producing, fixating, acquiring, storing, possessing, distributing or presenting pornographic content with a minor. Fixation of pornographic materials with a minor is punishable somewhat lighter (Article 202 § 4 of the Penal Code – up to 10 years of imprisonment), and storage, possession or gaining access to pornographic

 DOI: 10.7206/kp.2080-1084.113

content with a minor is also punishable to a lighter extent (Article 202 § 4a of the Penal Code – from 3 months to 5 years of imprisonment).

The actions performed as specified in Article 202 § 4 apply only to fixation, without taking into account production of pornography. Fixation, depending on the definition adopted, may mean duplication of ready media or activities aimed at recording specific content on the media.

The issue which may give rise to doubts with regard to Article 202 § 4 of the Penal Code is the lack of criminalisation of production of child pornography and limitation of actions performed to fixation only. The jurisprudence interprets the concept of fixation, depending on the definition adopted, as duplication of ready media or activities aimed at recording specific content on the media. Oktawia Górniok claims that the fixating party is the person who, albeit absent from the process of creating pornographic content, duplicates ready items and media on which such content is stored.[32] Marek Bielski defines fixation as recording the content on the media which supports playback of the content.[33] Mateusz Rodzynkiewicz stresses that the fixating party is the person who undertakes actions aimed at recording the pornographic content on the medium (including the camera operator, photographer, etc.).[34]

According to the Dictionary of the Polish Language[35], fixation means, among other things: recording of sounds and images on tapes and discs, etc. for later playback. Production[36] includes the body of what has been produced, the process of creating the film, directing, shooting; production means involvement in the production, manufacture of something, shooting, directing, filming. Therefore, it should be considered that production is a broader concept than fixation and covers the whole range of activities which may end up in fixation of certain content.

Therefore, it seems reasonable to expand the catalogue of actions performed and related to child pornography to cover the production of such content. Article 202 § 4 could read as follows "Anyone who produces or fixates pornographic content with a minor is liable to imprisonment from one year to ten years".

Liability related to simulated pornography is derived from Article 202 § 4b of the Penal Code, which criminalises the production, distribution, presentation or

---

32 O. Górniok [in:] O. Górniok, S. Hoc, M. Kalitowski, S.M. Przyjemski, Z. Sienkiewicz, J. Szumski, L. Tyszkiewicz, A. Wąsek, *Kodeks karny. Komentarz. Tom II*, Gdańsk 2005, s. 214.

33 M. Bielski [in:] A. Zoll (ed.), op. cit., p. 680.

34 M. Rodzynkiewicz [in:] A. Zoll (ed.), op. cit., p. 680; similarly J. Piórkowska-Flieger [in:] T. Bojarski (ed.), op. cit., p. 508; M. Bielski, op. cit., p. 680.

35 M. Szymczak (ed.), *Słownik języka polskiego*, Warszawa 1998, Vol. III, p. 633.

36 Ibidem, Vol. II, p. 938; ibidem, Vol. III, p. 862.

possession of such pornography and defines it as a produced or processed image of a minor participating in a sexual activity. In order to fully incorporate provisions of the Directive, the category of punishable conduct should be extended to include acquisition of simulated pornography and extend its definition adopted in the provision to include realistic images of sexual organs of a child. Therefore, instead of a definition of "produced or processed image of a minor participating in a sexual activity", the definition of "produced or processed image of a minor participating in a sexual activity or images of sexual organs of a child" could be introduced.

The Polish criminal law does not provide sanctions for pornographic content with persons aged 18 or over who are depicted as children. The EU Directive allows to exclude criminal liability for actions related to child pornography and pertaining to an actual person appearing to be a child if that person is in fact 18 years of age or older (Article 5(7)). It should be noted that although the provisions of the Directive leave to the discretion of Member States to decide whether to punish child pornography produced with adults appearing to be a child, Article 5(8), which provides for exclusion of punishment for certain conduct related to simulated child pornography, reads that such exclusions must not apply to, among other things, pornographic materials with an adult appearing to be a child. Therefore, there may be situations where despite the fact that the state decides not to prosecute pornography depicting adults appearing to be children, it will have to punish simulated child pornography produced on the basis of pornographic material in which such persons were involved.

Also, the pornographic performances involving the participation of a child should be mentioned here. Both the Lanzarote Convention, as well as the EU Directive clearly indicate the need to criminalise recruiting a child for participation in pornographic performances or causing a child to participate in such performances, coercing a child into participating in pornographic performances or profiting from or otherwise exploiting a child for such purposes (Article 21(1.a) and 21(1.b) of the Convention, Article 4(2) and Article 4(3) of the Directive), as well as conscious presence at pornographic performances involving the participation of children (Article 21(1.c) of the Convention and Article 4(4) of the Directive). Pornographic performance is defined by Article 2(e) of the Directive as a live exhibition aimed at an audience (including by means of information and communication technology), of a child engaged in real or simulated sexually explicit conduct, or the sexual organs of a child for primarily sexual purposes.

Article 202 § 4c of the Polish Penal Code criminalises the participation in a presentation of pornographic content with a minor for attaining sexual satisfaction. In place of pornographic performances, the Code introduces presentation of pornographic content, as this concept seems to be broader than a pornographic

 DOI: 10.7206/kp.2080-1084.113

performance, in particular as it is not limited by the requirement of "live" viewing. The introduction of a broader definition of a prohibited act with regard to such a sensitive issue as sexual abuse of a child is absolutely justified. Given this, there could be certain doubts as regards the limitation of liability of the person who directly participates in a presentation of pornographic content with a minor only to situations when that person does so to attain sexual satisfaction – in particular where this is unnecessary narrowing with regard to provisions of Article 4(4) and Article 21(1.c) of the Lanzarote Convention.

Article 11 of the Directive and Article 27(3) of the Convention provide for seizure and confiscation of the tools and proceeds of the crime which said legal acts refer to, including offences related to child pornography. This is implemented in the Polish law in Article 202 § 5, which provides for court-ordered forfeiture of tools or other items used for or designated for committing certain offences related to child pornography (including the offence of public presentation of pornographic content in a manner which may impose reception of such content on a person not wishing to receive such content).

The Directive requires that necessary steps must be taken to ensure that aiding and incitement to commit the actions described above is punishable and that an attempt with regard to production, distribution, dissemination, transmission, offering, supplying or making available child pornography is also punishable (Article 7). Similar provisions are laid down in Article 24 of the Lanzarote Convention.

Directive on combating the sexual abuse and sexual exploitation of children and child pornography criminalises also the organisation for others, whether or not for commercial purposes, of travel arrangements with the purpose of committing an offence concerning child pornography, as well as the dissemination of material advertising the opportunity to commit any of the offences concerning child pornography (Article 21).

Article 25 of the Directive indicates the need to ensure the prompt removal of web pages containing or disseminating child pornography hosted on the EU Member States' territory and to endeavour to obtain the removal of such pages hosted outside of their territory. It also provides – while leaving it to the discretion of the individual Member States – the ability to block access to Internet pages containing or disseminating child pornography, if these sites can not be deleted.

Public promotion or praise of paedophile conduct is criminalised by Article 200b of the Penal Code**.** It is worth wording this provision more precisely. One of the bills drafted by the Ministry of Justice (November 2012) postulated for changing the phrase "paedophile conduct" to "sexual conduct with regard to minors". Without going into details as to whether this change is desirable or not, it should be noted that the change would result in the standardisation of the nomenclature

used in the Code and from this viewpoint could be perceived as desirable. The implementation of Article 21(b) of the Directive would also be supported by expanding Article 200b of the Penal Code to include "facilitation of paedophile conduct". The final version of Article 200b of the Penal Code could read as follows: "Any person who publicly promotes, praises or facilitates sexual conduct with regard to minors is liable to a fine, restriction of liberty or imprisonment for up to 2 years".

Article 17 of the Directive lays down an obligation to ensure that the production of child pornography outside the territory of the European Union will be subject to jurisdiction of the Member States (with regard to their citizens) regardless of whether such an activity is an offence at the place where it is committed (similar provisions are included in Article 25 of the Lanzarote Convention). In accordance with the provisions of the Directive, the offences[37] defined in Article 5 (acquisition, possession, distribution, dissemination, knowingly obtaining access by means of information and communication technology, transmission, offering, supplying or making available and production) committed by using information and communication technology and access to them from the territory of a Member State fall within the jurisdiction of that state even if the devices of the ICT network (e.g. servers) remain outside its territory. Therefore, a solution should be introduced to the Polish criminal law that would allow to apply provisions of the Polish criminal law which penalise the production of child pornography with regard to Polish citizens acting outside the EU's territory, even if such an act is not an offence at the place where it is committed. The catalogue of provisions of the Polish Penal Code must also be extended to include a provision that would impose the jurisdiction of the Polish state with regard to the acts described in Article 5 of the Directive and committed by using an information and communication network if that network was accessed from within the territory of the Republic of Poland.

Solicitation of children for sexual purposes (grooming)

Both the Lanzarote Convention and Directive on combating the sexual abuse and sexual exploitation of children and child pornography criminalise the solicitation of children for sexual purposes (so called grooming). Article 23 of the Convention and Article 6 of the Directive require that the criminalisation be ensured of an intentional proposal, by means of information and communication technology, by an adult to meet a child who has not reached the age of sexual consent, for sexual exploitation of that child – where that proposal was followed by material acts leading to such a meeting, as well as to provide child pornography depicting that child.

[37] My considerations are limited to those provisions of the Directive which apply to child pornography.

 DOI: 10.7206/kp.2080-1084.113

The liability for grooming is regulated by Article 200a of the Polish Penal Code. Article 200a § 1 of the Penal Code criminalises establishing a contact, by using an information and communication system or a telecommunication network, with a minor under the age of 15 and an attempt to meet with such a minor with the intention of sexual abuse or production or fixation of pornographic content. Article 200a § 2 of the Penal Code criminalises the use of an ICT system or a telecommunication network to submit proposals of a sexual relationship to a minor under the age of 15, to have the minor subjected to or perform another sexual act or participate in the production or fixation of pornographic content provided that the offender acts with the intention to fulfil such a proposal.

It seems that the intention of the Directive (and the Lanzarote Convention) was to criminalise the use of an ICT network to solicit children for sexual purposes, not only as a mere preparation or an attempt at committing another offence of sexual nature, but to criminalise the very use of means of electronic communication (information and communication technologies). This may be also supported by recital 19 of the Directive's preamble, which underlines that the purpose was to introduce sanctions on new forms of sexual abuse and sexual exploitation of children, in particular "online solicitation of children for sexual purposes via social networking websites and chat rooms".

It seems reasonable to rephrase Article 200a, which could read as follows "Anyone who uses an ICT system or a telecommunication network to present a minor aged under 15 with a proposal to meet in order to engage in sexual activities or to produce or fixate pornographic content, with a view to a personal contact with that minor is liable to a fine, restriction of liberty or imprisonment for up to ... years".

Offenders are increasingly frequently using ICT networks to establish a contact with a minor. Such a contact will not always result in an actual meeting with a minor. The offender more often abuses a minor with whom he has established contact in a different way, for example by acquiring pornographic materials from that minor, such as intimate photographs of the minor, a striptease recorded in front of a Web camera, etc. It seems reasonable to amend Article 200a to take into account prosecution of the conduct described above. If the aforementioned proposal to formulate Article 200a is worded as § 1 of that article, then § 2 could read as follows: "Anyone who uses an ICT system or a telecommunication network to establish a contact with a minor aged under 15 years to obtain from that minor photographs, films or other content of pornographic nature depicting the minor is liable to a fine, restriction of liberty or imprisonment for up to ... years".

Presentation of pornographic material to a child

Different forms of presenting pornographic material to a child can be distinguished. It can for example consists in making available such content in a computer network, but it could also be the presentation of sexual activities to a child in order to achieve sexual satisfaction for the offender (the offender may take part in the sexual act, but may also not participate directly in it).

Causing, for sexual purposes, a child who has not reached the age of sexual consent to witness sexual activities or sexual abuse, even without having to participate, is criminalised in Article 3 of the Directive. Similarly, the Lanzarote Convention, criminalises in Article 22 the corruption of children, i.e. intentional causing, for sexual purposes, of a child below the age of sexual consent, to witness sexual abuse or sexual activities, even without having to participate.

The Polish Penal Code in Article 200 § 4, imposes penalties on the presentation to a minor under 15 years of age performance of a sexual act – in order to satisfy a sexual offender or a third party.

The Polish criminal law regulates the issues of presenting pornography to persons who do not wish to receive such content. Article 202 § 1 of the Penal Code penalises public presentation of pornographic content in a manner where such content is imposed on a person not wishing to receive such content. In addition, Article 200 § 3 of the Penal Code criminalises conduct which consists in the presentation to a minor aged under 15 years of pornographic content and supplying to that minor items of such nature or distribution of pornographic content in a way which allows the minor to become familiar with such content.

These regulations (i.e. Article 200 § 3 of the Penal Code and Article 202 § 1 of the Penal Code) need consideration, in particular with regard to an ICT network. According to the Dictionary of the Polish Language[38], public presentation refers to an activity that can be performed, among other things, in a public manner or in a public place, where the term "public" means, among other things, "designated, accessible to everyone", as well as "taking place in a location accessible to everyone". In accordance with this definition, public presentation may be understood as such presentation of pornographic content which is available without limitations to an unspecified number of persons.[39] A similar view is expressed by Patrycja Kozłowska and Marzena Kucharska who define public presentation as presentation where "given the location (e.g. a public place open to everyone) or method of action, it is

[38] M. Szymczak (ed.), op. cit., Vol. II, p. 1074.

[39] M. Mozgawa, P. Kozłowska, *Prawnokarne aspekty rozpowszechniania pornografii (analiza dogmatyczna i praktyka ścigania)*, "Prokuratura i Prawo" 2002, 3, p. 17.

 DOI: 10.7206/kp.2080-1084.113

or could be seen by an unspecified number of non-individualised persons or by a definite but greater number of persons, e.g. at a meeting. As a rule, this means all forms of presentation which allow any potential recipient to become familiar with such content, without the need to overcome any obstacle or meet any particular requirements".[40]

In its judgment of 16 February 1987 (WR 28/87, OSNKW 1987, Vol. 9–10, item 85), the Supreme Court found that the distribution of pornographic materials[41] (prints, writing, photographs or other items) should be understood as such conduct of the offender which consists in making available to the public such materials by, among other things, reproduction, copying and other types of making available such content to a wide and unspecified circle of persons. According to the judgment, an action of the offender which consists in the presentation of such items (e.g. screening of a film) can not be treated as distribution if it is made available to a small and strictly defined circle of persons.

The Dictionary of the Polish Language defines "imposing" as "forcing someone to act in a certain manner, to submit oneself to something"[42], which in the light of Article 202 § 1 of the Penal Code may be interpreted as forcing to receive (e.g. watch) pornographic content against their will, where it is irrelevant whether such a person is actually at risk of such reception, the potential possibility of such a situation occurring is sufficient.[43]

Particular attention should be paid to the problem of dissemination of pornography in computer networks. The issue of pornography in the virtual space comprises also the fact of pornography, including hard pornography, being widely available to minors.

Pornographic content in the computer network is available to virtually an unlimited circle of people, so it should definitely be considered to be publicly presented. The placement of such content in the network meets the criteria of dissemination and sharing.[44] If a service offering pornographic content is open only to authorised users (persons who must fulfil certain conditions, for example pay for the service or apply access code), then it is not possible to consider it publicly presented pornography.

---

40 P. Kozłowska, M. Kucharska, *Prawnokarne aspekty pornografii*, "Prokuratura i Prawo" 1999, 4, p. 33.

41 According to Article 173 of the Penal Code of 1969.

42 M. Szymczak (ed.), op. cit., Vol. II, p. 286.

43 M. Rodzynkiewicz, op. cit., p. 573; P. Kozłowska, M. Kucharska, op. cit., p. 35.

44 K.J. Jakubski, *Rozpowszechnianie pornografii w sieci komputerowej Internet*, "Prokuratura i Prawo" 1997, 7–8, pp. 50–51; J. Warylewski, *Pornografia w Internecie – wybrane zagadnienia karnoprawne*, "Prokuratura i Prawo" 2002, 4, p. 54.

According to Jarosław Warylewski, the person who warns the user of possible contact with pornography and requires confirmation of the legal age of such a user and their consent to receive pornographic content can not be accused of committing an offence under Article 202 § 1 and Article 200 § 4 of the Penal Code (after recent amendments to the Code the former Article 202 § 2 of the Penal Code is currently Article 200 § 4 of the Penal Code).[45] The above view is justified, but only in a situation where the person making pornographic content available is able to check whether the recipient has actually reached the legal age and is able to secure their service against unauthorised access. It does not seem justified to claim that a person who makes available pornographic content can not be charged with an offence under Article 202 § 1 and 2 of the Penal Code based merely on a statement of the interested party that the conditions required by the law have been met, in particular with regard to online sites, where the admission of a statement that is not confirmed in any way does not fulfil the requirement of acting with due diligence. A similar view is presented by Michał Sowa, who raises the dubiousness of effective release of a website author from potential liability by placing a disclaibahaviorer that the website is intended for adults only.[46] The confirmation could be for example the number of the payment card, because even if the ineligible person uses a card of an "eligible" person, it can be concluded that the service provider acted with due diligence, while the cardholder did not act with due diligence. Andrzej Adamski presents the position of a German administrative court stating that given the anonymous nature of the Internet, the number of the national identity card or the payment card is not a sufficient pass to use services of an adult website.[47]

The opinion of Jarosław Warylewski seems also unjustified as he claims that "reaching pornographic content online requires the user to take certain intentional activities, therefore persons who do not wish so will most likely not come across pornography".[48] The author is right in weakengin his statement with the reservation "most likely". We often deal with cybersquatting, which consists in registering popular domain names in bad faith so that popular words or addresses are used to redirect the user to websites containing pornographic content. Searching for completely "safe" phrases online often leads to websites containing pornographic content.

---

45 J. Warylewski, *Pornografia w Internecie...*, op. cit., p. 54; M. Sowa, *Ogólna charakterystyka przestępczości internetowej*, "Palestra" 2001, 5–6, p. 32.

46 M. Sowa, op. cit., p. 32.

47 A. Adamski, *Karnoprawna ochrona dziecka w sieci Internet*, "Prokuratura i Prawo" 2003, 9, p. 73.

48 J. Warylewski, *Przestępstwa przeciwko wolności seksualnej i obyczajności. Rozdział XXV Kodeksu karnego. Komentarz*, Warszawa 2001, p. 218; idem, *Pornografia w Internecie...*, op. cit., pp. 55–56.

 DOI: 10.7206/kp.2080-1084.113

Article 200 § 5 of the Code which criminalises advertising or promotion of activities which consist in the distribution of pornographic content in the manner which allows a minor aged under 15 years to come across such content may give rise to certain doubts. Is the mere advertising or promoting of the distribution of pornographic content criminalised, as it might make such content available to a minor aged under 15 years, or is advertising and promoting of making pornographic content available to a minor aged under 15 years subject to a penalty? In the first case, if we assume that advertising or promoting as such makes pornographic content available, then we are dealing with an offence of presenting pornographic content to a minor aged under 15 years or distributing such content in the manner which allows such a minor to become familiar with such content (Article 200 § 3 of the Penal Code) – and the additional criminalisation does not seem necessary. In the second case, we are dealing with peculiar praising of an offence consisting in the presentation of pornographic content to a minor aged under 15 years. In this situation, considering the fact that by its very nature advertising or promotion is addressed to an unlimited group of recipients, application of Article 255 § 3 of the Penal Code could be considered (public praising of an offence).

Taking the above into account, the provision which distinguishes conduct related to the presentation of pornographic content could take the following form:

> "Article ...
>
> § 1. Anyone who publicly presents pornographic content in such a way that this may impose reception of such content on a person who does not wish to receive such content is liable to ...
>
> § 2. Anyone who presents pornographic content to a minor aged under 15 years or makes available to that minor items of such nature or distributes pornographic content in the manner which makes it possible for such a minor to become familiar with such content is liable to ..."

Conclusions

Over the years the Internet (as a synonym of the global network) has been developing without fixed, rigid rules of conduct, which does not mean an absence of rules altogether. The scientific community, which primarily used the network in the beginning of its existence, was able to effectively enforce respect for the freedom of all network users, with the result that the freedom of action of one individual

did not inflict on the freedom of others. The development of a global network and its opening to the public initiated an era of the cyber network resulting in far-reaching legal implications in the real world. The law has only begun to rule in cyberspace – as a public medium used by individuals whose freedom must be protected and where illegal activities must be punished.

The above considerations are related only to a part of the problem, i.e. the matters governed by generally accepted international regulations: Council of Europe Convention on Cybercrime, Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, Directive 2013/40/EU on attacks against information systems and Directive 2011/93/ EU on combating the sexual abuse and sexual exploitation of children and child pornography.

A comparison of the provisions of the mentioned instruments with the Polish Penal Code shows that its provisions to a large extent are consistent with the obligations imposed on EU Member States and Parties to the mentioned Conventions.

It seems that, in relation to the offenses against the confidentiality, integrity and availability of data and computer systems, the Polish criminal law is fairly well aligned with both the Convention on Cybercrime and the Directive on attacks against information systems. It should be noted, however, that the provisions concerning protection of data integrity require clarification (Article 268a of the Penal Code).

Although the regulation of computer related crimes (computer related forgery and computer related fraud) does not seem to require special modifications, it must be noted – especially in relation to electronic documents and electronic means of payment – that this area will likely pose new challenges in the near future.

Identity theft is in some way associated with computer fraud. Indeed, in many countries, the offense is treated as a fraud. But fraud, a crime against property, can not always be seen as synonymous with identity theft, especially when the victim has not suffered property damage, but mostly personal harm. The possibility of prosecuting the creation of fictitious identities to cause another person property damage or personal harm should also be taken into account.

As often, one of the most difficult topics that the criminal law has to face is the protection of children against sexual exploitation. Admittedly, sexual exploitation of children, including child pornography, is not a new phenomenon. However, at least the distribution of child pornography was rather limited prior to the development of digital communication technologies. A global network enabling the transfer of any large amounts of information in a very short period of time, has not only resulted in the dissemination of enormous quantities of illegal material, but also has led to a continuous increase in the demand for new materials, which in turn inevitably brings about the growing exploitation of an even larger number of children.

 DOI: 10.7206/kp.2080-1084.113

The catalogue of the offenses criminalised by Polish criminal law in relation to the sexual offenses against children is wide, but the question whether the liability of the offender in some cases seems to be restricted by law, requires examination. The use of a much wider definition of offenses related to such sensitive issues as sexual exploitation of a child is entirely justified. Against this background, limiting the protection of a child solicited by ICT means for sexual purposes to children below the age of consent, may raise some doubts. Similarly, limiting the liability for the presentation to a minor under the age of 15 years a performance of sexual act to situations where the presentation is made in order to satisfy the sexual offender or a third party, seems an unnecessary narrowing of the offender's liability. Issues concerning the liability for simulated child pornography needs also some modification, where above all the definition needs to be broadened.

Finally, the issue of blocking access to certain websites should also be mentioned. The discussion concerning the blocking of sites with illegal content is not new. Raising doubts as to its effectiveness are of course legitimate, although it is a fact that blocking sites with content related to child pornography has been relatively successful and can contribute to the prevention of access to such content to those who do not take additional steps to find such content. The experiences of countries where the content related to child pornography has been blocked indicate that, despite all the weaknesses, this method deserves to be promoted, especially since research indicates that sharing child pornography via the Internet may stimulate the manifestation of paedophile behaviour that otherwise might remain dormant.[49] The best solution, of course, would be to be able to remove entirely sites containing child pornography, but this is possible only if the server offering such content is located in a country whose jurisdiction allows the removal of sites with prohibited content. In any other cases, the blocking of access seems to be the fastest method to impede such access.

Bibliography

Adamski A., *Karnoprawna ochrona dziecka w sieci Internet*, "Prokuratura i Prawo" 2003, 9.
Adamski A., *Prawo karne komputerowe*, Warszawa 2000.
Barta J., Fajgielski P., Markiewicz R., *Ochrona danych osobowych. Komentarz*, Warszawa 2011.
Bielski M. [in:] A. Zoll (ed.), *Kodeks karny. Część szczególna. Tom II, Komentarz do art. 117–277 k.k.*, Warszawa 2008.

[49] E. Quayle, *Pornografia dziecięca w Internecie. Działania prewencyjne i terapeutyczne wobec sprawców*, "Zagrożenia dzieci w Internecie" 2005, 13, p. 7, http://fdn.pl/nr-5-13-2005-zagrozenia-dzieci-w-internecie (15.01.2016).

Garfinkel S., Spafford G., *Bezpieczeństwo w Unixie i Internecie*, Warszawa 1997.
Goldsmith J.L., *Against Cyberanarchy*, "University of Chicago Law Review" 1998, 65(4).
Górniok O. [in:] O. Górniok, S. Hoc, M. Kalitowski, S.M. Przyjemski, Z. Sienkiewicz, J. Szumski, L. Tyszkiewicz, A. Wąsek, *Kodeks karny. Komentarz, Tom II*, Gdańsk 2005.
Hardy I.T., *The Proper Legal Regime for Cyberspace*, "University of Pittsburgh Law Review" 1994, 55.
Jakubski K.J., *Rozpowszechnianie pornografii w sieci komputerowej Internet*, "Prokuratura i Prawo" 1997, 7–8.
Johnson D.R., Post D., *Law and Borders – the Rise of Law in Cyberspace*, "Stanford Law Review" 1996, 48(5).
Kardas P., Michalski B., *Przestępstwa przeciwko mieniu*, Warszawa 1999.
Kopczyński G., *Pojęcie dokumentu i fałszu materialnego w nowym kodeksie karnym*, [in:] L. Bogunia (ed.), *Nowa Kodyfikacja Prawa Karnego*, Vol. II, Wrocław 1998.
Kozłowska P., Kucharska M., *Prawnokarne aspekty pornografii*, "Prokuratura i Prawo" 1999, 4.
Marek A., *Kodeks karny. Komentarz*, Warszawa 2010.
Mejssner B., *Niezbite cyfrowe dowody*, http://cio.cxo.pl/artykuly/55536/Niezbite.cyfrowe.dowody.html
Michalski B. [in:] *Kodeks karny. Część szczególna. Tom II. Komentarz pod redakcją Andrzeja Wąska*, Warszawa 2010.
Mozgawa M., Kozłowska P., *Prawnokarne aspekty rozpowszechniania pornografii (analiza dogmatyczna i praktyka ścigania)*, "Prokuratura i Prawo" 2002, 3.
Piórkowska-Flieger J. [in:] T. Bojarski (ed.) *Kodeks karny. Komentarz*, Warszawa 2012.
Piórkowska-Flieger J., *Przestępstwa przeciwko wiarygodności dokumentów w nowym kodeksie karnym*, "Przegląd Sądowy" 1997, 10.
Quayle E., *Pornografia dziecięca w Internecie. Działania prewencyjne i terapeutyczne wobec sprawców*, "Zagrożenia dzieci w Internecie" 2005, 13, http://fdn.pl/nr-5-13-2005-zagrozenia-dzieci-w-internecie
Reed C., *Internet Law: Text and Materials*, Cambridge 2004.
Rodzynkiewicz M. [in:] A. Zoll (ed.), *Kodeks karny. Część szczególna. Tom II, Komentarz do art. 117–277 k.k.*, Warszawa 2008.
Skorupka J., *Przedmiot ochrony przestępstwa z art. 310 k.*, "Palestra" 2002, 7–8.
Skorupka J., *Wady oświadczenia woli w wybranych przestępstwach gospodarczych*, "Przegląd Sądowy" 2000, 4.
Sowa M., *Ogólna charakterystyka przestępczości internetowej*, "Palestra" 2001, 5–6.
Szymczak M. (ed.), *Słownik języka polskiego*, Warszawa 1998.
Warylewski J., *Pornografia w Internecie – wybrane zagadnienia karnoprawne*, "Prokuratura i Prawo" 2002, 4.
Warylewski J., *Przestępstwa przeciwko wolności seksualnej i obyczajności. Rozdział XXV Kodeksu karnego. Komentarz*, Warszawa 2001.
Wąsek A. [in:] O. Górniok et al. (eds.), *Kodeks karny. Komentarz. Tom I*, Gdańsk 2005.

 DOI: 10.7206/kp.2080-1084.113

Wróbel W. [in:] A. Zoll (ed.) *Kodeks karny. Część szczególna. Tom II, Komentarz do art. 117–277 k.k.*, Warszawa 2008.

Wróbel W. [in:] G. Bogdan, K. Buchała et al. (eds.), *Kodeks karny. Część szczególna. Komentarz do k.k.*, t. 2, Kraków 1999.

Zakrzewski R., *Ochrona wiarygodności dokumentów w nowym kodeksie karnym*, "Przegląd Ustawodawstwa Gospodarczego" 1999, 7–8.