Teka Kom. Praw. – OL PAN, 2014, 105–119

CRIMES COMMITTED VIA THE INTERNET – SELECTED ASPECTS

Magdalena Samodulska

Prosecutor of Opole District Prosecutor's Office

Abstract. The author attempts to discuss the issues connected with crimes which are being committed via the Internet in the paper synthetically, beginning with differentiation of terms: „computer-related crime", „Internet crime" and „cybercrime" by presentation of exemplary methods of action of perpetrators of „Internet crimes" with the example of the so called „classic fraud" from article 286 § 1 of the Criminal Code and „computer-related fraud" which is listed in the category of computer-related crimes from article 287 § 1 of the Criminal Code.

Key words: computer-related crime, Internet crime, cybercrime, classic fraud, computer-related fraud

The considerations which are being presented in this paper do not pretend to include the comprehensive and exhaustive discussion of numerous aspects related to Internet criminality. It will rather become an attempt to indicate some legal solutions in view of newer and bolder forms of committing crimes connected with functioning of global computer network, which the Internet undoubtedly is.

In everyday life, in media coverage, we can come across alternative use of notions of „computer-related crime", „Internet crime" and „cybercrime". In American literature computer-related crimes are also often specified as cybercrimes[1], crimes related to digital technology[2] or Internet crimes[3].

Whereas it seems that those notions should not be identified with each other nor applied interchangeably. First of all because the term „computer-related crimes" is of conventional nature and performs mainly the sorting function of the given normative material[4]. As the term which is the most extensive notion, it includes within its scope the notion of „Internet crime" where the Internet is only of the possibilities of criminal use of a computer[5]. Next, „cybercrime" is a subcategory

[1] L.E. Quarautiello, *Cyber Crime: how to protect yourself from computer criminals?*, Tiare Pubns, 1996, following A. Adamski, *Prawo karne komputerowe*, Warszawa 2000, p. 33.

[2] N. Barrett, *Digital Crime – Policing the Cybernation*, Kogan Page 1997, following A. Adamski, *Prawo karne…*, p. 33.

[3] R. Clark, *Technological Aspects of Internet Crime Prevention*, 1998, following A. Adamski, *Prawo…*, p. 33.

[4] A. Adamski, *Prawo…*, p. 32.

[5] M. Sowa, *Ogólna charakterystyka przestępczości internetowej*, „Palestra" 2001, No. 5–6, p. 27–30.

of computer-related crime. Still it is hard to track a legal definition of those notions as they have not been worked out yet, both internationally or in Polish Criminal Code. Indeed both criminologists as well as dogmatists of criminal law have attempted to define them but no satisfactory results have been brought so far[6]. Creation of one legal and undoubted definition – embracing the diversity of those crimes, their object and methods of action – must be assumed practically impossible.

One of the first definitions of „computer-related crime" was the one presented by R. von Zur-Mühlen in 1973, according to which computer-related crime is „each criminal action in which computer is a tool or object of an assault"[7].

First to divide computer-related crimes was P. Sommer (alias H. Cornwall) who, on the basis of his own research and experiences, distinguished four types of this phenomenon:

1) crimes which are impossible to perform without the presence of a computer that is theft of IT systems and assaults at systems, theft of application programs of a computer, unauthorized entry into a computer (so called hacking), changes made to the software and data;

2) crimes „facilitated by computers" that is computer-related fraud, Internet fraud, theft of information, forgery, wiretapping, dissemination of information in the Internet which is forbidden by law;

3) frauds in business and private interests, which are performed with passive use of computers;

4) crimes connected with use of computers by expert criminals in order to support criminal activity and to communicate (especially with organized crime)[8].

In international environment, the basic division of computer-related crimes was regulated in Recommendation No. R(89)9 of the European Committee of Council of Europe which includes the so called minimum list and the so called optional list[9].

Minimum list includes acts which, in the opinion of Committee of Experts, all countries should adapt, within the obligations of a country to international co-operation in prosecution of cross-border crime, which undoubtedly includes crimes committed via the Internet, moreover due to its significant noxiousness. As a result minimum list included the following types of computer misuses:

– computer-related fraud;

---

[6] R. Czechowski, P. Sienkiewicz, *Przestępcze oblicza komputerów*, Warszawa 1993, p. 51 and next.

[7] R. von Zur-Mühlen, *Computerkriminalität. Gefahren und Abwehr, Neuwied*, Berlin 1973, following M. Siwicki, *Podział i definicja cyberprzestępstw*, „Prokuratura i Prawo" 7–8, 2012, p. 242.

[8] H. Cornwall, Dataheft. *Computer Fraud, Industrial Espionage and Information Crime*, London 1990, p. 53–54, in: R. Czechowski, P. Sienkiewicz, *Przestępcze oblicza komputerów*…, p. 56 following B. Fischer – *Przestępstwa komputerowe i ochrona informacji. Aspekty prawno-kryminalistyczne.* Kantor wydawniczy „Zakamycze" 2000, p. 25 and next.

[9] Council of Europe, *Computer-Related Crime: Recommendation No. R (89)9 on computer-related crime and final report of the European Committee on Crime Problems*, Strasbourg 1989.

– computer forgery;
– damage to computer data or programs;
– computer sabotage;
– unauthorised access to computer system;
– computer interception;
– unauthorized copying, distribution or publication of legally protected programs;
– unauthorized reproduction of a topography[10].

Significant part of demands of the Expert Committee of Council of Europe in the scope of this list was reflected in the Criminal Code of 1997 by criminalization of, especially, the following computer-related crimes understood as acts addressed against computer systems[11]: computer-related fraud (article 287 § 1 of the Criminal Code), computer forgery (article 270 § 1 of the Criminal Code), unauthorized access to a system (article 278 § 2 of the Criminal Code), computer interception (article 267 § 2 of the Criminal Code), computer sabotage (article 269 § 1 and 2 of the Criminal Code), violation of the integrity of computer information recording (article 268 § 2 of the Criminal Code).

On the other hand optional list of computer-related crimes was voluntary and included actions the prosecution of which was left at the disposal of governments. It included the following four types of behaviour:
– alteration of computer data or computer programs;
– computer espionage;
– unauthorised use of computer;
– unauthorised use of legally protected computer program[12].

Polish legislator has not undertaken to propose a legal definition of „computer-related crime". This notion is not specified by both article 115 of the Criminal Code (which includes comment on statutory expressions), and no provision from specific part of the Criminal Code relates to it.

The attempts to define the notion of „computer-related crime" in Polish literature on this subject were undertaken by, among others: K. J. Jakubski and A. Adamski.

First of the authors linked „computer-related crime" with the criminal phenomenon which includes all criminal behaviour connected with functioning of electronic data processing, infringing the processed information, its medium and cycle in a computer and the whole system of computer links and the computer hardware itself and right to computer program[13].

On the other hand A. Adamski distinguished substantive and procedural aspect of computer criminality. In substantive view the author indicated two

[10] Council of Europe, *Computer-Related Crime: Recommendation No. R (89)9*...

[11] Previously the computer-related crimes were defined only as acts addressed against the legal interests which were traditionally protected, where a computer facilitated their committed or allowed committed them in a different way.

[12] Council of Europe, *Computer-Related Crime: Recommendation No. R (89)9*…

[13] K.J. Jakubski, *Przestępczość komputerowa – podział i definicja*, „Przegląd Kryminalistyki" 1997, No. 2, p. 31.

types of assaults taking place in computer-related crimes. First of all those are the crimes which are computer-related crimes in the strict sense or crimes against safety of electronically processed information, where the assault is directed at systems, data and computer programs. Computer system is here either an object or the environment of the assault. The other group of acts is specified as computer-related crimes (misuses) where the computer itself is the tool of a crime[14].

Using the above division, one should include crimes listed in chapter XXXIII of the Criminal Code to computer-related crimes in the strict sense mainly, and the chapter is entitled „Crimes against information protection", where the object of protection is widely understood information, that is: hacking (article 267 § 1 of the Criminal Code), computer wiretapping (article 267 § 2 of the Criminal Code), violation of integrity of computer information recording (article 268 § 2 of the Criminal Code), computer sabotage (article 269 § 1 and 2 of the Criminal Code).

And one should include to the group of crimes where a computer is a tool of the crime, first of all, the acts connected with the use of the Internet as an environment which facilitates dissemination of information which can be qualified as socially harmful like pornographic, racist ones, the ones which approve of committing crimes or incite to committing them[15]. Crimes specified in chapter XXXV of the Criminal Code are included also in this category of crimes – that is illegal acquisition of a computer program (article 278 § 2 of the Criminal Code), receiving of stolen property of a computer program (article 293 § 1 of the Criminal Code), wire fraud (article 285 of the Criminal Code), computer-related fraud (article 287 of the Criminal Code), and crimes defined in chapter XXXIV of the Criminal Code, that is computer forgery (article 270 § 1 of the Criminal Code), destruction or depriving an electronic document of force of evidence (article 276 of the Criminal Code), and other seemingly untypical computer-related crimes like for example privileged type of espionage (article 130 § 3 of the Criminal Code).

On the other hand A. Adamski linked the criminal procedural aspect of computer criminality with the fact that a computer system may contain evidence of criminal activity, constituting both the object and the tool of the assault[16].

Summing up, the notion „computer-related crime" should be discussed in the category of some notional collection of crimes which have the common feature of occurrence of computers there, digitalized information, close ties with functioning of electronic data processing[17].

---

[14] A. Adamski, *Prawo…*, p. 30 and next.

[15] Sometimes a really useful instrument which allows committing some computer-related crimes is electronic mail for example in the situation of threatening another person with committing crimes to her detriment or detriment of immediate family, if this threat arises a justified fear in the threatened person that it would be fulfilled (see article 190 of the Criminal Code).

[16] A. Adamski, *Prawo…*, p. 34.

[17] B. Fischer, *Przestępstwa komputerowe…*, p. 23.

A distinct subcategory of computer-related crime is „cybercrime" understood as a type of economic crime where a computer is either an object or a tool of a crime. Those are all types of crimes where the Internet or other computer networks was used to commit them[18]. At the same time, one should not identify the above mentioned notion with the term „Internet crime" as the latter one includes only a group of acts which can be committed in the Internet only (for example misleading the users of IT systems as to the identity of a sender of a message which was sent by electronic mail in order to acquire personal data) or with its assistance (for example slander with use of a website).

According to Hołyst and Pomykała one can distinguish three basic forms of committing a „cybercrime" and that is when:

– a computer or a network are a tool of a crime (will be used to commit it),

– a computer or a network are the aim of a crime (are its „victim"),

– a computer or a network are used to additional tasks connected with committing a crime (for example to store data on illegal sale of drugs)[19].

With the development of new forms of committing „cybercrimes" three generations of it were defined:

– the so called first generation of cybercrimes – which includes assaults directed at a computer, computer networks and data;

– the so called second generation of cybercrimes – connected with development of ICT systems and attacks at their integrity and accessibility for the so called hackers;

– the so called third generation of cybercrimes – current – connected with noticeable process of automation of cyber-criminality which is the result of, among others, use of special software. The most important determinant of the newest generation of cybercrimes is the fact that they are committed not directly by the aggressors but they are the result of the so called programmatic attacks with use of the software which was developed to this end[20].

Significant contribution into defining the norms of international law on counteraction of cyber-criminality and standardization of applied terminology was by European and international legislation initiatives which were accepted at forum of such organizations as: the Council of Europe, Organization for Economic Co-operation and Development, United Nations, EU, International Criminal Police Organization „Interpol".

The most practical definition of cybercrime was formulated by International Criminal Police Organization „Interpol", indicating its vertical and horizontal

[18] D. Verton, *Black Ice. The Invisible Threat of Cyber–Terrorism*, following B. Hołyst, J. Pomykała, *Cyberprzestępczość, ochrona informacji i kryptologia*, „Prokuratura i Prawo", 1, 2011, p. 17.

[19] B. Hołyst, J. Pomykała, *Cyberprzestępczość*…, p. 17.

[20] A. Završnik, *Cybercrime definitional challenges and criminological particularities*; available online: http://www.inst–krim.si/upload/izdajanje/AZavrsnikcybercrime.pdf., following M. Siwicki, *Podział i definicja cyberprzestępstw…*, p. 244 and next.

view. Cybercrimes in vertical view are crimes which are specific for cyberspace, that is ones which can be committed only there, like for example hacking, computer sabotage. On the other hand, horizontal view assumes committing crimes with assistance of computer techniques, therefore this notion includes for examples computer-related frauds, money counterfeiting or also money laundry[21].

Committee of the Council of Europe in the Convention of the Council of Europe No. 187 on cybercrime of 23rd November 2001[22] distinguished the following types of crimes within cyber-criminality:

– crimes against confidentiality, integrity and availability of computer data and systems including: illegal access (article 2), illegal interception (article 3), data interference (article 4), system interference (article 5), misuse of devices (article 6),

– computer-related crimes including: computer-related forgery (article 7), computer-related fraud (article 8),

– content-related crimes including: crimes related to child pornography (article 9) and added in the additional protocol to the convention: dissemination of racist and xenophobic material through computer systems (article 3), racist and xenophobic motivated threat (article 4), racist and xenophobic motivated insult (article 5), denial, gross minimization, approval or justification of genocide or crimes against humanity (article 6),

– crimes related to infringements of copyright and related rights.

On the other hand European Union defined cybercrime in Communication from the Commission to the European Parliament, the Council and the Committee of the Regions of 2007[23] named „Towards a general policy on the fight against cybercrime", according to which cyber-criminality consists of four types of crimes that is:

– ones directed against confidentiality, integrity of data (so called CIA crimes) for example hacking, illegal wiretapping, computer espionage, computer sabotage,

– „classic" or „traditional" crimes committed with use of a computer for example computer-related frauds, documents forgery, extortion of goods or services,

[21] Compare M. Siwicki, *Podział i definicja cyberprzestępstw*…, p. 249.

[22] Convention of the Council of Europe No. 187 on cybercrime of 23rd November 2001, http://www. vagla.pl/skrypts/cybercrime_konwencja.html

[23] Compare Communication from the Commission to the European Parliament, the Council and the Committee of the Regions, Brussels of 22nd May 2007, KOM(2007) 267, final edition, available at http://eur–lex. europa. eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:PL:HTML. See also the Opinion of European Economic and Social Committee on Communication from the Commission to the European Parliament, the Council, European Economic and Social Committee and the Committee of the Regions: „Digital agenda for Europe", COM(2010) 245, final edition (2011/C 54/17), Official Journal of EU.C.2011.54.58.

– „content" crimes (concerning computer, servers content etc.) for example child pornography, delivery of criminal instruction (of a type „how to construct a bomb"), forbidden racist, fascist content etc.,

– crimes connected with infringements of copyright and related rights.

The last of the presented notions is an „Internet crime". This term can be discussed in two aspects. On one hand „Internet" will be the environment which is used to commit „an assault", and on the other hand it will be a tool used to commit „an assault". In the literature on the subject one can find a different understanding of the above mentioned term. M. Sowa, finds „Internet" to be only a tool to commit offences. Next, Internet criminality itself can be discussed when, without use of this network, committing a specific act could not take place or it would be significantly hindered[24]. In a word, if not for the globalization of the Internet network and network services offered via it (including the services offered by a man via it) it would not be possible to perform some acts which are illegal or it would be hindered[25].

Taking no account of the above, one can especially include the following into the category of „Internet crimes":

– hacking into mail accounts – mail servers,

– hacking into individual computers of users as well as into those belonging to companies and institutions,

– theft of data bases and information which is property of individual users as well as being secrets of companies and institutions,

– change of content of websites,

– deletion of data on hard drives of computers,

– immobilization of single computers which are connected to a network and of the whole networks,

– illegal trade in medicines, anabolic and steroids,

– games of chance and mutual wagering held via the Internet,

– trade in objects, the possession of which is forbidden or which come from a crime,

– different types of fraud and extortions during organization of auctions of sale of different types of objects, GSM accessories and mobile telephones, when organizing work abroad etc. (the so called Internet auction frauds),

– piracy (creation and administration of warez sites, servers for exchange of files via p2p programs, sites through which there is sale of illegally copied games and programs as well as music records or movies),

– dissemination of forbidden information and insult of people (by creation and administration of sites with child pornography – paedophilia, creation and

[24] M. Sowa, *Odpowiedzialność karna sprawców przestępstw internetowych*, „Prokuratura i Prawo" 2002, No. 4, p. 62.

[25] M. Sowa, *Ogólna charakterystyka*..., p. 27–30.

administration of sites with fascist information, placing information which injure the good name of people).

One should consider that most of the mentioned types of Internet crimes do not exist by themselves – the crimes supplement each other and penetrate each other.

In conclusion, presented definitions of „computer-related crime", „cyber-crime" and „Internet crime" only convince that not only there is not but it is not possible to create one and quite universal typology of those notions. They are quite ambiguous and therefore not precise so it would be difficult to form and propose such an expression which can be applied both in the sphere of criminal substantive law, procedural law and in the sphere of criminology and criminalistics. Attempts at defining those notions come at either enumerative list of various types of behaviour or too general expression of the subject. On the other hand, it is of value that there is a trend to define and classify it according to objective criteria, which allows to order this heterogeneous group of acts, also with the conclusions of practical nature. It is undisputable that constant technical development does not aid permanence to any of the definitions of those notions which are formed in literature.

The crimes which are committed via Internet most often and which are connected with it in a strict sense are the so called Internet frauds in a broad sense. One of the most frequent Internet frauds include: extortion of money and goods, using a number of credit card which had been stolen earlier, manipulation of a program, forgery of salary sheet, phishing and pharming[26].

In this article the most common type of Internet fraud will be discussed, that is extortion of goods and services within the so called classic fraud from article 286 § 1 of the Criminal Code, in correlation with computer-related fraud from article 287 § 1 of the Criminal Code.

Provision of article 286 of the Criminal Code in § 1 includes statutory features of the so called crime of classic fraud, according to which „Whoever, with the purpose of financial benefit, causes another person to dispose of his own or someone else's property disadvantageously by misleading him, or by taking advantage of a mistake or inability to adequately understand the action undertaken […] – shall be subject to the penalty of imprisonment for a period between 6 months to 8 years".

Causative act of this crime means leading another person to unfavourable disposal of his own or someone else's property which should be understood as causing a decision which is disadvantageous for a victim who disposes of his property. Perpetrator of this crime acts to gain financial benefit. Leading to disadvantageous disposal of property can take three executive forms that is:

1) **misleading, that is so called „active fraud"**, where a perpetrator, with his own deceitful endeavours, leads a victim to mistaken image of a specific

[26] see A. Janus, *Przestępczość internetowa*, p. 5 and next, source: http://www.sceno.edu.pl/articles.php?cms_id=92&cat=IT-artyku%B3y

state of facts for example about the value of an object, features of the goods being sold or purchased, ability to acquire benefits from concluded transaction etc.[27];

2) **taking advantage of someone else's mistake that is so called „passive fraud"**, in which there is a victim with for example mistaken image of value of an object, results of a transaction etc.[28];

3) **taking advantage of victim's inability to adequately understand the action undertaken**, which can be of permanent nature (for example a person is mentally ill, small child, elderly person without discernment) or temporary (for example distemper resulting from temporary illness or other disturbance of mental activities). As the law does not limit the prerequisites of inability to understand the action undertaken it can also arise from ignorance, superstition or credulity of a victim[29].

The fraud which is specified in article 286 § 1 of the Criminal Code is a substantive crime with criminal consequences that is for existence of which the result must take place in the form of disadvantageous disposal of property. If the disadvantageous disposal of property does not take place we just have attempted fraud[30].

A type of classic fraud which was the first to appear in the Internet and up to this day is most commonly applied by cybercriminals is the so called Nigeria fraud (also named advance fee fraud). This type of fraud had been known since 16th century with the name letter of Spanish Prisoner and writing and sending letters was used to commit it. Presently the perpetrators are using electronic mail to commit this type of a crime and by mail they send e-mail message to a chosen victim, allegedly from a person, who needs to regain a big sum of money from a given country (usually it is Nigeria, and that is where the name comes from, although it can be any other country currently – Great Britain, Spain is more often at stake). This person promises high reward for the assistance, and the assistance itself is to be a transfer of a big amount of money. Users (that is potential victims of a crime) if they believe in those assurances, they are drawn into a specific psychological game based on imaginary story, as a result of which they are asked to transfer a given amount of money to cover bank fees. After the payment the contact ceases and the money is lost. It is a basic form of this type of fraud. The most common types of Nigeria frauds are also: „political refugee from black land fraud", „investor fraud", „lottery prize fraud", „no owner account fraud", „Internet auction fraud", „inheritance fraud"[31].

---

[27] Judgment of the Supreme Court of 27.10.1986, ref. II KR 134/86, OSNPG of 1997, No.7, item 80.

[28] *Ibidem*.

[29] See A. Zoll, in: *Kodeks karny, Część szczególna, Tom III Komentarz do art. 278–363 k.k.*, ed. A. Zoll, Warszawa 2008, p. 255–273.

[30] *Ibidem*, p. 273 and next.

[31] Source: Crime Department of National Police Headquarters (*Jak uniknąć „oszustwa nigeryjskiego"*, http://www.policja.pl/portal/pol/154/39219/Jak_uniknac_quotoszustwa_nigeryjskiegoquot.html).

Detection of perpetrators of this type of crimes is minimal which is connected undoubtedly with unsatisfactory level of co-operation with Nigerian law enforcement. And this leads to specific pathology as the perpetrators of this type of crimes do not even use tools to hide their true IP address. The problems connected with Nigeria frauds have been examined internationally by United States Secret Service with seat in Washington continuously since nineties of the previous century but this service's opinion is also that recovery of money is practically impossible[32].

Next most common activity with criminal consequences of classic fraud is not fulfilling the obligations at Internet auctions. The fraud who runs the action, after he had collected money from a buyer, he either does not send the goods that were won or sends goods which are used or in other way inconsistent with the description which was placed previously. What is important is that more often the perpetrators acting at auctions are getting prepared to the criminal dealings for a quite a long time earlier. They are building a positive history of their transactions for many months, collecting positive comments from users. Only when the perpetrator considers that he is credible enough he starts offering goods which is of attractive price but not existent[33].

A new method which is being used by criminals is also extortion of personal and address data and opening accounts with the acquired data with the aim of their further criminal use. The mechanism of activity of perpetrators runs the following way. A perpetrator places job offers at various portals and he convinces potential victims to give their personal data, usually in a questionnaire which was prepared prior to that. A perpetrator opens a bank account in a Bank which offers electronic banking services with the data which were acquired in an above manner via the Internet network. Then he persuades a person who rendered his/her data available to send a symbolic one zloty to an alleged company account (in fact an account opened with acquired personal data) in order to confirm the truth of transferred personal data. Once the transfer is being made, a bank account which was opened by a perpetrator is being activated by the bank, which confirms this way whether the data provided in the Application for opening a checking and saving account are correct. A perpetrator administers this bank account which is fully functional from then on and which was opened with personal data of a different person[34].

The legislator, in chapter XXXV „Crimes against property", just after classic crime of fraud from article 286 § 1 of the Criminal Code, specified a specific type of a crime that is computer-related fraud in article 287 § 1 of the Criminal Code

[32] *Ibidem.*

[33] *Ibidem.*

[34] Source: Crime Department of National Police Headquarters (*Phising a pranie pieniędzy i oszustwa w Internecie*, http://www.policja.pl/pol/kgp/biuro-sluzby-kryminaln/cyberprzestepczosc/86700,-quotPhishing-a-pranie-pieniedzy-i-oszustwa-w-interneciequot.html?search=536138).

which was unknown in Criminal Code of 1969. Pursuant to the cited provision „Whoever, with the purpose of financial benefit or cause damage to other person, affects automatic processing, gathering or transmitting IT data, or changes or deletes record or introduces new record on electronic IT data without being authorized to do so, shall be subject to the penalty of imprisonment for a period between 3 months to 5 years".

First of all, one might question why the legislator did not supplement provision of § 286 of the Criminal Code with new features, with which the scope of penalization of the crime of „classic" fraud would include the phenomenon connected with automatic processing instead of creation of a completely new regulation of article 287 of the Criminal Code.

At the beginning stage of development of IT technologies the regulation of „classic" fraud could perform its function. The devices which were processing data were much less complex and influencing the course of this process could have only been an intermediate stage between a misleading perpetrator and mistaken man who would operate a device, the decision of whom would mean whether there would be a property transfer or not. Currently, the situations when there is a human element in the process of processing data are seldom. Presently the computers are much more „independent" which is translated directly onto the problem in the process of application of the regulation of „classic" fraud[35].

The crime of computer-related fraud is different from crime of classic fraud with two elements. A priori, provision of article 287 of the Criminal Code does not require for the perpetrator to undertake any influence onto a person in order to lead him to disadvantageous disposal of his own or somebody else's property. Next, for committing the crime from article 287 of the Criminal Code the result in the sphere of property is not required, in the form of disadvantageous disposal of property or gaining by a perpetrator (or a different person) of financial benefit or worsening of a situation of entity whose property rights were reflected in the record of IT data[36]. The offence of computer-related fraud is different from classic fraud also in this that it does not include a victim with protection, as follows from its features of aspect of the crime as to the act, characterizing the place in which misdemeanour can be committed that is IT system[37]. It does not mean that the provision of article 287 of the Criminal Code does not protect a victim. As the main object of protection of this crime is property, then it

[35] A. Adamski, *Prawo…*, p. 115.

[36] See A. Zoll, in: *Kodeks karny…*, p. 317.

[37] See. B. Michalski, in: *Kodeks karny. Część szczególna. Komentarz*, *v. II*, ed. A. Wąsek, Warszawa 2004, p. 981; see also J. Wojciechowski, *Problem kwalifikacji prawnej wyłudzeń informatycznych z użyciem kart kredytowych*, St. Praw. 2006, No. 4, p. 141 and next, L.K. Paprzycki, *Oszustwo informatyczne właściwe i niewłaściwe a nielegalne wykorzystywanie dealerów*, St. Praw. 2006, No. 4, p. 123 and next.

indicates entity who is entitled to rights to property which are protected by article 287 of the Criminal Code as a victim[38].

The main purpose of the adopted regulation was to fill the legal loophole in criminalization of behaviours which infringed property and record of IT data reflecting specific rights to property, and which due to means of assault connected with use of modern ICT technologies were not covered with protection by the construction of classic fraud[39].

In the beginning differencing between article 286 of the Criminal Code and article 287 of the Criminal Code caused much difficulty to law enforcement in practice. In the construction of traditional type of crime of fraud the object of influence of the perpetrator is a person who is being deceived by him. The situation is different in case of computer-related fraud, in which there is no element of misleading another person or taking advantage of this mistake. The direct object of influence of the perpetrator is not a deceived person – victim but equipment of computer system. Doubts were created mainly on the basis of the notion of a mistake. Pursuant to views of most of the doctrine the notion of mistake is linked strictly with the notion of intellect. Therefore it is a mental state. It means it is not adequate in case of a computer.

Also in the doctrine, the construction of article 287 of the Criminal Code was spelling serious doubt in the beginning especially due to terminology that was used for characteristics of the features of this forbidden act. Only with the act of 18th March 2004 on change of the act – Criminal Code, act – Code of Criminal Proceedings and the act – Misdemeanour Code [40], the original shape of crime of computer-related fraud was changed. The modifications that were introduced were connected with singing of the convention on cybercrime of 28th November 2001 by the Republic of Poland and included replacement of the original feature „sending with the expression „transmission", replacement of the expression of the direct object „information" with „IT data" and the expression „record on computer data device" with the expression „record of IT data". Adopted expressions allowed to penalize the activities of the perpetrator independent of the type of device on which the data was recorded[41].

On the other hand, the crime of computer-related fraud is in some way connected with the regulation of classic fraud. In order to settle whether we deal with the crime of classic fraud or crime of computer-related fraud one should settle whether in a given case the act of a perpetrator was directed not only against property but also a person (classic fraud). It should also be settled whether there was „misleading" a machine (computer-related fraud) or whether a man was misled. In article 287 § 1 of the Criminal Code, as equivalent of

[38] See. A. Zoll, in: *Kodeks karny…*, p. 321.
[39] See A. Zoll, in: *Kodeks karny…*, p. 319.
[40] Journal of Laws No. 69, item 626.
[41] See A. Zoll, in: *Kodeks karny…*, p. 318.

„misleading" and „disposal of property" the expression was formed „causing damage in property of another person by affecting the result of data processing".

Furthermore, both in article 286 of the Criminal Code as well as in article 287 of the Criminal Code the legislator stressed the purpose of the perpetrator which is financial benefit. This condition means that if the purpose of the activity of a perpetrator is not financial benefit, and in the case of computer-related fraud also no other which was provided alternatively in this provision (this means in order to cause damage) – then he would not be treated as a fraud within the understanding of criminal law[42]. An example of computer-related fraud which is being committed for financial benefit is causing a transfer of often big amount of money to the account of a perpetrator as a result of password being cracked in a computer network of a bank. And the liability for computer-related fraud which was committed to cause damage to another person, relates both to cases when the damage is a result of activity of a perpetrator, which is specified in a prescribed way by listed features of aspect of a crime as to the act, characterizing his behaviour and to the situation when the activity of the perpetrator is only a way to cause other damage[43].

The other problem was created as a result of settlement whether a computer-related fraud is a substantive crime or formal one. Part of the doctrine, following A. Adamski[44], R. Korczyński and R. Koszut[45] and R. Góral[46], declared themselves in favour of formal nature of this crime due to lack of result in form of disadvantageous disposal of property in its statutory features. On the other hand, as considered by P. Kardas and M. Dąbrowska-Kardas, an argument for substantive nature of a crime was that the behaviour of the perpetrator is not enough for execution of features of this crime but also existence of results of this behaviour. It is to follow from construction of features of the crime which characterize the act by the so called functional specification of the result[47].

In the literature on the subject the mixed view is also represented (B. Michalski), which divides the regulation of article 287 of the Criminal Code into two variants: formal – substantive. Affecting automatic processing, gathering or transmission of IT data is to be of formal nature as the condition for committing of a forbidden act in this case is only „affecting" the above mentioned processes and not causing their actual disturbances. On the other hand change, deletion or introduction of a new record of IT data as a required result of existence of a crime

[42] See K. Daszkiewicz, *Kodeks karny z 1997 roku. Uwagi krytyczne*, Gdańsk 2001, p. 353–354.

[43] J. Wojciechowski, *Kodeks karny, Wyd. II poprawione i uaktualnione. Komentarz. Orzecznictwo*, Warszawa 2000, pp. 537–538.

[44] A. Adamski, *Prawo…*, p. 116.

[45] R. Korczynski, R. Koszut, *„Oszustwo" komputerowe*, „Prokuratura i Prawo" 2002, No. 2, p. 35.

[46] R. Góral, *Kodeks karny. Praktyczny komentarz*, Warszawa 2007, p. 497.

[47] J. Giezek, N. Kłaczynska, G. Łabuda, *Kodeks karny. Część ogólna*, ed. J. Giezka, Warszawa 2007, p. 43.

indicates its substantive nature[48]. It is an opinion which has not been met in the doctrine yet, where one does not find crimes of mixed nature with and without criminal consequences. It does not seem to be accurate due to the fact, at least, of inability to specify a defined moment of committing a crime in such a situation and – therefore – the beginning of prescription period.

Analysing the above, the most accurate seems to be the argument of substantive nature of this forbidden act. Admittedly, the existing doubts as to the legal nature of the discussed crime should be adjudged fast and unambiguously by a judicial decision of the Supreme Court.

Within the crime of computer-related fraud, the practice so far defined three types of manipulation[49]:

1) manipulation with data – which means entering untrue information to a database to acquire unauthorized benefits for example entering corrections in documents, providing untrue information on beneficiaries, creation of „fake accounts", manipulation of cash businesses, embezzlement in state administration[50].

2) manipulation with a program – which means entering or conversion of existing program instruction which causes automatic execution of tasks the operator has no control of for example keeping the so called double-entry bookkeeping[51].

Manipulation with a program is one of the ways to commit a crime in a strict sense via the Internet. The perpetrator prepares a program and „implants" it into the system for a system to perform specific actions without the will of an operator. A typical example is also for example hacking into a banking system and adding a program which „cuts" minimal amounts from bank accounts and transfers them to one account[52].

3) manipulation with the result – which means manipulation with peripheral – system devices and devices of input – output for example extortion of cash from a cash machine with stolen magnetic card[53].

Summing up, computer-related frauds are very common and their scope is practically unlimited. One should consider that the perpetrators of this type of crimes have excellent knowledge of IT techniques and extraordinary intellect abilities. A random person cannot be a computer fraud but only such one who has specialist qualifications in IT. Perpetrators of misdemeanour from article 287 of the Criminal Code, contrary to the entity of the crime from article 286 of the Criminal Code that is of classic fraud, do not need any knowledge of psychology which allow them to learn the weaknesses of human nature. Computer

[48] B. Michalski, in: O. Górniok, W. Kozielewicz, E. Pływaczewski, B. Kunicka-Michalska, R. Zawłocki, B. Michalski, J. Skorupka*, Kodeks karny. Część szczególna. T. II. Komentarz do art. 222–316*, ed. A. Waska, Kraków 2006, p. 1041.

[49] A. Adamski, *Prawo…*, p. 118 and next.

[50] B. Fischer, *Przestępstwa komputerowe*…, p. 33.

[51] *Ibidem*, p. 34.

[52] A. Adamski, *Prawo karne…*, p. 119 and next.

[53] *Ibidem*, p. 119 and next.

fraud does not mislead another person, does not take advantage of his mistake or inability to adequately understand the action undertaken as it takes place in case of misdemeanor from article 286 of the Criminal Code. His task may turn to be more difficult in a given case. He has to face complex equipment and technological processes, and not human psychology, which might be easier to outwit and deceive[54].

Misdemeanour of computer-related fraud was also on the list of crimes, the committing of which by a natural person justifies liability of collective entities within the understanding of the act of 28.10.2002 on liability of collective entities for forbidden acts which are punishable – article 16 section 1 item 6 of the cited act.

In conclusion, it should be stated that with the growing popularity of the Internet and the number of its commercial applications, furthermore constant development, a task of the legislator should be to strengthen legal-criminal protection of electronically processed information. It is huge freedom of criminal activities in the Internet, in view of other computer-related crimes that causes biggest concerns. Positive law should set standards of protection which include the development of information technology and not allow the infringement of various legal interests without threat of penalties. Furthermore, increase of awareness of threats among users of the Internet network as well as knowledge of factors which aid them, which is of great importance in case of computer-related fraud should be the basic element of prevention. According to statistical data, placed at the website of National Police Headquarters article 287 of the Criminal Code is not the so called dead letter of the law[55].

PRZESTĘPSTWA POPEŁNIONE PRZEZ INTERNET – WYBRANE ZAGADNIENIA

Streszczenie. Autor podejmuje w artykule próbę syntetycznego omówienia zagadnień związanych z przestępstwami, które mogą być popełnione za pomocą Internetu, począwszy od rozróżnienia terminów: „przestępczość komputerowa", „przestępczość internetowa" i „cyberprzestępczość", poprzez przedstawienie przykładowych metod działania sprawców „przestępczości internetowej" na przykładzie tzw. „oszustwa klasycznego" z art. 286 § 1 kodeksu karnego i „oszustwa komputerowego", który znajduje się w kategorii przestępstw komputerowych z art. 287 § 1 kodeksu karnego.

Słowa kluczowe: przestępczość komputerowa, przestępczość internetowa, cyberprzestępczość, oszustwo klasyczne, oszustwo komputerowe

[54] E. Jakimiuk, J. Zając, *Systematyka oszustw w prawie karnym i taktyka ich zwalczania*, Legionowo 2008, p. 49–50.

[55] Information is available at the official website of National Police Headquarters – www.policja.pl. the statistics present numbers of committed misdemeanors of computer-related fraud: 1999 – 217, 2000 – 323, 2001 – 279, 2002 – 368, 2003 – 168, 2004 – 390, 2005 – 568, 2006 – 444, 2007 – 492, 2008 – 404.