Vlado Bučkovski PhD[*]
Goce Naumovski PhD[**]

LEGAL RESPONSE TO CYBERCRIME: THEORETICAL CONCEPT AND MACEDONIAN LEGISLATION APPROACH

1. Introduction

Computers and information and communication technology development could play three different roles in the punishable crimes. Firstly, they could be the target of the punishable crime. The cases of viruses, hacking, etc. are typical examples of this role. Secondly, computers appear as means, media for data storing when committing crimes; and thirdly they could be means for committing a crime.[1]

The term "Cybercrime" encompasses not only the crimes linked to the Internet network, but also to other computer networks and devices of information and communication technology, even telephone lines and mobile networks.

The evolution of the Internet also meant new types of punishable crimes and a high level of diversity. As part of the so-called Cybercrime as broad term, the Internet crime encompasses all illegal acts committed on the Internet or with the help of the Internet (World Wide Web).

Cybercrime is a special challenge for the contemporary penal law and criminological sciences. Its relevance has caused an avalanche of researches as well as broad legislative activity on both international and national level.

According to the US data, 35.7% of all reported cases of crime in the United States are Internet crimes, while the damages from the Internet frauds are estimated to around USD 239 million. The ten most frequent cases of Internet frauds are presented in the chart bellow.[2] It is interesting to point out the so-called "Nigerian letters" or e-mails with attempts for fraud (directions for alleged easy earning through funds of former officials from the African and South African countries) are also present in our country.

On international level, the G-8 Ministers of justice and home affairs with their activities from December 1997, as well as the 1996 European Commission Action Plan contributed to the defining the Internet punishable crimes.

Both platforms on the Internet abuse, setting off from the transnational character of the Internet crimes, consider as Internet crimes all cases in which the following goods are violated:[3]

---

[*] Professor at the Iustinianus Primus Law Faculty, Ss. Cyril and Methodius University, Skopje.
[**] Associate Professor at the Iustinianus Primus Law Faculty, Ss. Cyril and Methodius University, Skopje .
[1] Y. F. Lim, *Cyberspace,* p. 248-251.
[2] *2007 Internet Crime Report,* FBI's Internet Crime Complaint Center (IC3), http://www.ic3.gov/media/annualreports.aspx
[3] Adamski A. (1998) *Crimes Related to the Computer Network. Threats and Opportunities: A Criminological Perspective,* Helsinki, Finland: European

- national security (instructions for making bombs, illegal production of drugs, terrorist activities);
- protection of minors (marketing abuse, violation and pornography);
- protection of human dignity (racial hatred and racial discrimination);
- economic security (frauds, directions for credit cards piracy);
- information security (hacking);
- privacy protection (illegal communication of personal data, electronic harassment);
- reputation protection (slander and offensive articles, illegal comparison advertising);
- intellectual property (illegal distribution of creators' works, for example software or music), etc.

Apart from the use of the terms "Internet crime" and "Cybercrime" in the field of penal law, we should also mention so-called computer or information penal law.[4] In the field of criminology, the term "cyber criminology" is used more and more frequently.[5]

2. Forms of Cybercrime

In scientific theory, there are numerous qualifications of the forms of Cybercrime.

According to Burden and Palmer,[6] Cybercrime refers to two groups of punishable crimes. The first group encompasses the so-called "punishable cybercrimes" which include cases of Hacking, Cyber Vandalism, Viruses Dissemination, Denial-of-Service Attacks and Domain Snatching.[7]

The second group incorporates cases of "electronically enabled punishable crimes", i.e. credit cards abuse; information abuse or theft; slander; blackmail; child pornography; hate web sites; money laundering; violation of copyright and related rights; cyber terrorism and encryption.[8]

Apart from the common classification, Yi Fem Lim also gave an interesting classification of special i.e. particular cases of punishable crimes in the field of Cybercrime. It encompasses: activities of Internet paedophilia; fraud; cyber stalking; gambling; selling alcohol; securities fraud and page jacking.[9]

Institute for Crime Prevention and Control, affiliated with the United Nations (HEUNI). Retrieved on December 15, 2006 from http://www.ulapland.fi/home/oiffi/enlist/resources/HeuniWeb.htm.

[4]В. Камбовски (1997): *Казнено право, посебен дел,* Просветно дело, Скопје.

[5]Jaishankar K. (2007), ''Cyber Criminology: Evolving a novel discipline with a new journal'' in: *International Journal of Cyber Criminology,* Vol. 1 Issue 1 January 2007. Retrieved on March 15, 2007, from http://www40.brinkster.com/ccjournal/editorial.htm

[6]Kit Burden and Creole Palmer (2003), ''Internet Crime: Cyber Crime-A New Breed of Criminal?'' in: *Computer Law and Security Report*, 19 (3): 222-227.

[7]Cybersquoting was described in the Chapter on Internet Domain.

[8]Kit Burden and Creole Palmer (2003), ''Internet Crime: Cyber Crime-A New Breed of Criminal?'' in: *Computer Law and Security Report*, 19 (3): 222-227.

[9]Y. F. Lim, *Cyberspce,* p. 281.

McQuade's classification of Cybercrime forms takes as the basic criterion the way in which the crime is committed i.e. the specific form of information technology abuse.[10] Those forms encompass: writing and spreading malicious codes, thefts and frauds, interfering with computer services, computer spying and illegal trespassing; unlawful exchange of files, abuse of computers and electronic devices in the academic environment, on-line harassment and computer linked punishable crimes against sexuality and the so-called futuristic forms of Cybercrime.[11]

Having in mind the above mentioned, as well as other classifications, the Cybercrime forms could be globally classified in several groups: **1. Thefts and frauds; 2. Computer spying; 3. Hacking and illegal penetrating in computer systems; 4. Viruses distribution and other forms of malicious software (malware); 5. Cyber stalking; 6. Production and distribution of illegal pornography; 7. Cyber terrorism; 8. Violation of intellectual property rights.**

2.1. Thefts and frauds

The most common forms of thefts and frauds that include abuse of information and communication technology are: frauds with credit cards and securities, identity thefts and intercepting and usurping computer services.

2.1.1. Frauds with credit cards and securities

The credit cards fraud permits the perpetrator to use data from somebody else's credit card, in order to make an illegal purchase of goods or services or to make other changes on the account.

The credit cards fraud is so widely spread form of cybercrime that there is even special illegal software for searching data from existing, issued or forged credit cards. The potential perpetrators have access to these data. This technique is known as "carding".

We became aware of this issue when this type of data were received via credit cards bots inserted in Internet Relay Chat-IRC programmes that were "commanded" by the perpetrators to generate names of valid credit cards holders. A similar example is the "AOHell" programme used in the 1990s for attacking the users of the America Online provider (McQuade, 2006).

The possibility for fraud also exists in case of securities trade done via Internet. The effective, efficient and fast trade also means opportunity for new ways of securities frauds. The estimate is that more than 16% of the total trade happens on-line. Commonly, we speak about three categories of securities frauds: market manipulation; fraud offer and illegal brokering and touting (Fen Lim, 2002).

Market manipulations encompass attempts for spreading false information (via web sites, electronic mail, etc.) for the purpose of artificial increasing of the market value by increasing the demand for the less valuable securities. The information refers to change in the status of

[10]S. C. McQuade, III (2006): *Understanding and Managing Cybercrime,* Pearson.
[11]Ibid.

the companies, future business ventures. This form of fraud is also called "pump and dump scheme" (Fen Lim 2002).

2.1.2. Identity theft

It is a case of illegal acquisition and use of personal data in order to obtain goods and services on somebody else's behalf. The identity theft is frequently identified with credit cards fraud, but it could also have other forms. Among the many forms of identity thefts are the frauds in the course of electronic agreements (for example selling or buying real estate), electronic payment of bills, etc.

The US Federal Trade Commission Identity Theft Survey Report shows that in the period 1998-2003 over one million users of computer services were victims of this kind of cybercrime.[12]

2.1.3. Intercepting, usurping and interfering with computer and telecommunication services

Intercepting and usurping computer services encompasses all forms of interfering or preventing computer or telecommunication services that could have damaging consequences for a broad range of users of these services.

Among the most frequent forms of intercepting, usurping and interfering with computer services are: theft of a signal broadcasted by cable TV providers; Denial of Service Attack-DoS; sending unwanted and disturbing e-mails (Spamming) and installing programmes with advertising contents (Adware)(McQuade, 2006).

The theft of a signal broadcasted by cable TV providers refers all illegal acts for enabling access to the cable TV signal. They often encompass modifying of the existing devices in order to enable physical access to the signal, as well as use of new devices in order to convert the coded signal into a signal that could be viewable on a TV receiver.

Denial of Service Attack-DoS refers to an attack on computers in order to deny the services to authorised users. The attack is done in one of the following ways: disassembling the computer or the network into their components; attacking the software in order to prevent its functioning and overburdening the system and its resources and capacities in order to crash it and to disable it.

Sending unwanted and disturbing e-mails (Spamming).[13] Spamming means sending enormous number of e-mails of commercial or marketing nature that often have disturbing or insulting contents. The messages that are sent in this manner are called spam messages.

Some of the spam messages are aimed at stimulating recipient's sexuality, for instance by promoting sexual aids and pornographic services (McQuade 2006).

Installing programmes with advertising contents (Adware). Adware is a form of a computer programme that enables pop up of

[12]Synovate, *FTC Identity Theft Survey Report,* Washington D.C., 2003.

[13]The term spam originates from the TV series Monty Python, where for the first time this was used as a name for tinned meat product with good taste (McQuade, 2006).

certain contents of advertising nature (banner) on the desktop or integrating these contents in the communication software. After the installation, Adware is difficult to remove and could be de-installed only by using special software (McQuade 2006).

2.2. Computer spying

Computer Spying encompasses acts of using special computer software (spyware) that 'nests' in the computer in order to take over the control of the system by: collecting and receiving information; installing other types of software; redirecting the internet browser to other pages, etc.

The term 'spyware' originates from 1995, related to a comment regarding the business practices of Microsoft and it referred to using hardware devices for spying (such as small dimensions cameras). However, this term was used for the first time for software in 2000.[14]

There are certain dilemmas whether the term "spyware' is appropriate in the sense that it does not define the essence. The term "spyware", especially by the computer security experts, is replaced with "malware", in order to underline the maliciousness of the software (malus = bad), while the creators of this software call it "adware".[15]

Regardless of the terminology differences, the actions of the "spying" software are on the rise, due to at least two reasons: rise of the so-called "peer-to-peer" applications (e.g. Kazaa.com) and the marketing elements on the web pages.[16] For these reasons, people have been speaking about a kind of a "spyware inferno".[17] The legislation is trying to respond to this challenge. One of those attempts in the US legislation is the Spyware Control Act, adopted by the State of Utah, which has been showing certain results.[18]

2.3. Hacking (illegal penetrating of a computer system)

The standard broad definition of hacking encompasses all forms of using technology for purposes for which that technology is not intended.[19]

Computer hacking represents accessing a computer system without an expressed or indirect permission of the owner of the computer system.[20]

The more restricted meaning of the term hacking i.e. unauthorised penetration in the computer system as a form of cybercrime

---

[14]In this context the term was used by Gregor Freund, the founder of Zone Labs, at a press conference for the promotion of a new product (www.zonealarm.com).

[15]S. Wienbar, *Perspective: The Spyware Inferno* (http://news.cnet.com/2010-1032-5307831.html; 01.03.2009).

[16]Ibidem.

[17]Ibidem.

[18]Ibidem.

[19]R.Utrecht, quoted by P.A.Taylor, *Hackers: Crime in the Digital Sublime,* London, Rutledge, 1999, and S. C. McQaude, *Understanding and Managing Cybercrime,* Pearson, 2006.

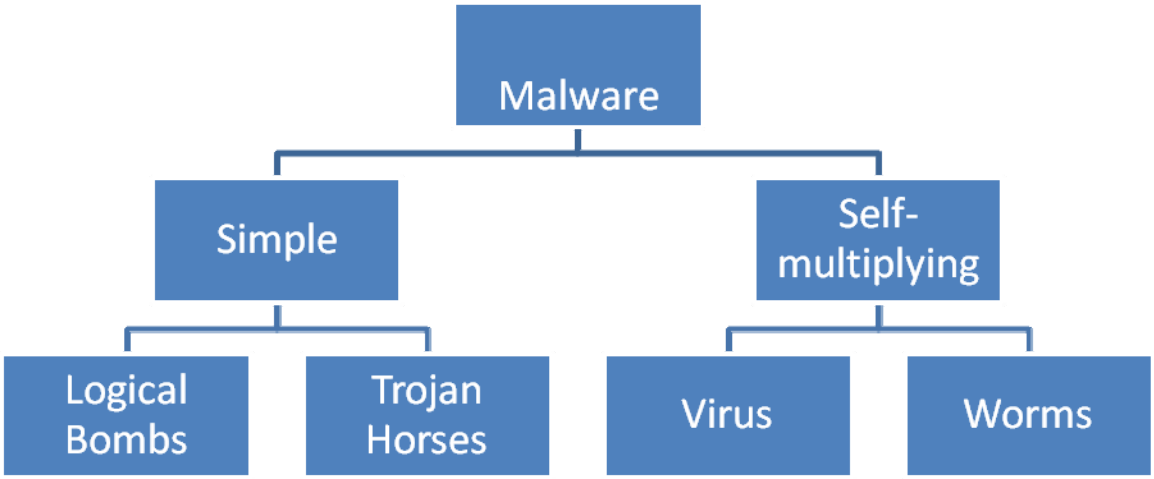
[20]D. I. Bainbride, *Introduction to Computer Law,* Pearson, 2004.

is illegal gaining access to one or more computer systems. This is done through abusing the security shortcomings and overcoming the security obstacles such as passwords and firewalls, in order to use or steal data or to insert new (external) programme functions (McQuade, 2006).

2.4. Viruses distribution and other forms of malicious software (malware)

The term computer virus was used for the first time in the 1970s within the ARPANET,[21] in order to mark computer self-applying programmes that were harmful to the computer system. Apart from the term "computer virus", another term is also used - "computer infection programme" i.e. malicious software (malware).

According to E. Filiol, the computer infection programmes refer to four categories of malware: logical bombs, trojan horses (trojans), viruses and worms.[22] You can see the schematic presentation of this classification in the chart below:



Schematic presentation of the computer infection programmes according to Filiol.

The nesting phases and the existence of the virus encompass: infection (spreading the virus in the overall environment i.e. the attacked computer system); incubation (virus's survival in the environment);

[21]T. Chen, J. Robert, *Statistical Methods in Computer Security,* 2004.
[22]E. Filol, *Computer Viruses: From Theory to Application,* Birkhauser, 2005, p. 82.

realisation (infecting of the system).[23] Filiol makes an interesting analogy of biological and computer viruses shown in the table below.

Biological viruses	Computer viruses
Attacking specific cells	Attacking specific types of files
The infected cells cause new virus focuses	The infected programmes create new virus codes
Modification of the cells' genomes	Modification of the programme functions
The virus multiplies only in living cells	The virus uses format structures for copying mechanisms
The already infected cells do not get infected again	The spreading happens with a spreading order
Retrovirus	The virus can avoid the antivirus programme
Virus mutation	"Polymorphousness" (new forms of the virus)
Healthy carriers of the virus	Latent virus
Antigens	Infection markers-signatures

Table analogy between the biological and computer viruses according to Filiol

Distribution of computer viruses is one of the most common forms of cybercrime. According to the data provided by the US Attorney General Office in 2001, 29.1% of the cases involving cybercrime dealt with distribution of viruses and other malware.[24]

2.5. Cyberstalking

Cyberstalking means using computer or another form of information technology for following other people's activities and movements without them knowing about it for the purpose of frightening them, sexual pleasure and domination or other illegal motives (McQuade, 2006).

According to the data of the Association "Working to Halt On-line Abuse" (www.haltabuse.org), in 1997 most of the cases of cyberstalking started with e-mails, bulletin boards, messenger programmes etc.

As a form of cybercrime, Cyberstalking encompasses two elements: a) collecting information about the victim (on the Internet or from other sources) and b) stalking, disturbing, frightening the victim.

The second element, stalking, harassment and frightening are frequently without physical contact, but it includes appearance of the stalker in front of the home of the victim, telephone calls, leaving written messages, property damaging etc.

[23]Ibidem.
[24]R. Smith, P. Grabosky, G. Urbas, *Cyber Criminals on Trial,* Cambridge, 2004, p. 22.

Cyberstalking has certain similarities and differences when compared to conventional stalking **(**„Offline" stalking**) (**Fen Lim 2000), that are shown in the chart below.

	Cyberstalking	**„Offline" stalking**
Victim	Most frequently a woman	Most frequently a woman
Perpetrator	Most frequently a man	Most frequently a man
Motive	Desire to control the victim	Desire to control the victim
Distance of the perpetrator from the victim	Big or small	Small
Potential new perpetrators	The perpetrator could encourage third parties to harass the same victim	Small probability
Prosecution of the perpetrator	More difficult due to anonymity	Easier

Similarities and differences between cyberstalking and „offline stalking" (Fen Lim 2000)

The criminology experts differentiate a number of categories of Cyberstalking. According to E. Ogilvie, there are three categories of cyberstalking that correspond to the three categories of functions that are typical for the Internet as a medium.[25]

- Convincing: sending e-mails to the victim with threats, attempts for initiating or renewing a love affair, frightening etc.;
- Control: the perpetrator controls the computer and other devices belonging to the victim – an interaction of perpetrator's computer with the victim's. Examples of this type of cyberstalking are the perpetrator opening the CD drive of the victim by using software in order to prove that he can control her computer;
- Broad range: endangering the victim and spill over of consequences from the virtual into the real world. An example of this type of cyberstalking is placing discrediting pornographic photos or personal information about the victim on certain web sites.

With regard to the legislative initiatives on cyberstalking, a kind of positive experience is the UK example of adopting the so-called Protection from Harassment Act in 1997 that encompasses comprehensive regulations on this kind of cybercrime.

2.6. Production and distribution of illegal pornography

Information technology and especially the Internet enable an easy production and distribution of child and other types of illegal pornography, primarily because it ensures anonymity. In comparative

[25]E. Ogilvie, ''The Internet and Cyberstalking'', paper presented at the Stalking Criminal Justice Response Conference, Australian Institute of Technology, Sydney, 2000.

law, the actions of production, downloading, dissemination as well as simple possessing of materials with illegal pornographic contents are punishable.

Distribution is frequently done using any software for transfer of data and usually through communication and internet chat software (e.g. Internet Relay Chat-IRC), news groups etc. (Fen Lim, 2002).

According to the data provided by the US Justice Department, starting from 1995 the number of cases linked to child pornography on the Internet shows an annual increase of ten percent.[26]

In most legislations, apart from child pornography, production and distribution of illegal pornography refers also to contents of zoophilia, necrophilia and forms of sadomasochism. (McQuade, 2006).

2.7. Cyberterrorism

The term cyberterrorism refers to all acts that combine forms of terrorism and cyberspace.[27]

According to Denning, the acts of cyberterrorism have two important features:

1. These are illegal attacks and threats of attacks of computers, networks and information aimed at threatening governments and people in order to achieve certain political or social goals; and

2. The attack results in violence against persons or property or at least threatening persons or property to a certain degree in order to cause fear.[28]

Some criminology experts (Shelly) point at a number of common features on cyberterrorism and organised crime:[29] firstly, the victims are either individuals or groups; secondly, the perpetrators are hierarchically structured in networks or organisation; and thirdly, both groups of perpetrators use computer or telecommunication technologies for achieving their goals (getting funds, planning operations, recruiting new members) etc.

The characteristics of the attack i.e. the actions are taken as the basic criterion for classification of cyberterrorism forms. Hence, according to the Centre for the Study of Terrorism and Irregular Warfare, Naval Postgraduate School in Monterey, California, USA, there are three types of cyberterrorism:[30]

- simple (non-structured). These actions of cyberterrorism are basic attacks against individual systems, using tools created by others.

---

[26]The President's Working Group on Unlawful Conduct on the Internet, Ap*pendix to the Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet,* March 2000.

[27]The term "cyberterrorism" was introduced by B.C. Colin. See: B. Colin, *The Future of Cyberterrorism, Crime and Justice International,* 1997, p. 17.

[28]D. E. Denning, *Cyberterrorism, Testimony Before the Special Oversight Panel on Terrorism Committee on Armed Services,* U.S. House of Representatives, Georgetown University, 2000.

[29]L. Shelly, ''The Nexus of International Criminals and Terrorism'' in: *International Annals of Criminology,* 20 (1/2), 85-92, 2002.

[30]*Cyberterror: Prospects and Implications,* Centre for the Study of Terrorism and Irregular Warfare, Naval Postgraduate School in Monterey, 1999.

The organisation of this attack is characterised by low level of analytical capabilities;

- advanced (structured). With these forms more sophisticated systems and networks are used, and the attackers develop their own basic tools. The organisation of the structured attacks has basic analytical features;

- complex (coordinated) where integrated complex tools are used (e.g. use of cryptography); there is high level of coordination and organisation of the attack in the sense of commanding and control.

Among the most typical examples of acts of cyberterrorism at the end of the 20th century we should list:[31]

- the attack in Massachusetts, USA in 1996 by a hacker linked to the "White Supremacist Movement" that consisted of breaking into the computer systems of several institutions resulting in sending racist messages on their behalf;

- the bombarding of the Institute for Global Communications with e-mails by Spanish demonstrators in 1998. The attack was a reaction to the fact that the Institute's web site hosted publications supporting the independence of Basque;

- the activities of the Tamil guerrilla in 1998, which sent more than 800 messages daily to all the Embassies of Sri Lanka in a period of two weeks;

- the support for the Mexican Zapatistas with the attacks by the so-called Electronic Disturbance Theatre in December 1997 and many others.

The actions of cyberterrorism cause huge material damages. For instance, the costs of dealing with the consequences from the infecting of 300,000 computers, resulting from the Code Red attack (whose target was the White House), amounted to three billion dollars, even though this has never been officially confirmed (McQuade, 2006).

Cyberterrorism has not yet reached the proportions of conventional terrorism. Still, having in mind the level of interaction of information technology and terrorist activities, it is absolutely possible to expect that the cyberterrorism will gain broader dimensions. It is a challenge to which the national legislation will have to respond. There should also be international initiatives that would incorporate proper measures and standards.

10.2.8. Violation of intellectual property rights

The need to criminalise the violation of intellectual property rights in the context of cybercrime results from several circumstances. Firstly, the perpetrators of the violation are tactically and strategically capable of avoiding the measures of civil legal protection. Secondly, usually these perpetrators repeat the violations. They are frequently organised in criminal groups and their activities threaten the security or the health of the people. Thirdly, a criminal organisation in the field of

[31]D. E. Denning, *Cyberterrorism, Testimony Before the Special Oversight Panel on Terrorism Committee on Armed Services,* U.S. House of Representatives, Georgetown University, 2000.

intellectual property is characterised with illegal distribution through a network that intends to avoid police and customs controls.[32]

The violation of intellectual property rights as a form of cybercrime always exists when information and computer technology is used as means. Criminalisation of these violations, nomo-technically could be covered either by the criminal codes or by the laws that regulate the right to intellectual property.

Among the more significant examples from the comparative law are the so-called Digital Millennium Copyright Act from 1998 (DMCA) and Lanham Act from 1946 in the US law as well as Copyright, Designs and Patents Act (complemented by the 2002 Copyright and Trademark-Offences and Enforcement Act) in the UK law.

Within the European Union, the so-called EU Directive on criminal measures aimed at ensuring the enforcement of intellectual property rights-IPRED2 was prepared. This Directive has not yet been adopted, because of the reactions among the scientific and expert public, both with regard to the question whether the EU is competent at all about this matter and with regard to the procedure.[33]

2.8.1. Digital piracy

Especially important is the criminalisation of digital piracy as a form of violation of copyright and related rights, a phenomenon that causes enormous material losses.

According to Graborsky and Smith, digital piracy is frequently defined as illegal reproduction of works belonging to somebody else in order to be used free of charge or presented as their own intellectual works.[34]

According to the report of the United States Report of the Working Group on Intellectual Property Rights,[35] the violations of copyrights on the Internet result from:

- Placing creator's work on the computer (disk, floppy, CD-Rom or other device for storing data as well as in RAM memory) for a period longer than "very short time".
- Scanning creator's work in digital format;
- Digitalisation of works such as photographs or sound recordings;
- Uploading digital file from the user's computer to another server;
- Downloading digital file from a server;
- Transfer of files from one to another computer;

---

[32]L. Harms, *The Enforcement of Intellectual Property Rights by Means of Criminal Sanctions, An Assessment,* WIPO Advisory Committee on Enforcement, Geneva, November 2007.

[33]More about the reactions on the Directive's text see: *Letter of the Dutch Parliament to EU Commissioner Frattni, concerning the IPERD2 Directive,* July 2006, available at: europapoort.nl (10.01.2009).

[34]P. N. Graborsky, R.G. Smith, *Crime in the Digital Age: Controlling Telecommunications and Cyberspace Illegalities,* Transaction Publishers, 1998, p. 89.

[35]*United States Report of the Working Group on Intellectual Property Rights,* U.S. Information Infrastructure Task Force, 1995.

- Every transfer of files where a note appears on the screen.

According to the European Union data, the losses from digital piracy amount to hundreds of billions Euros and about 200,000 jobs are threatened.[36]

With regard to software piracy, according to the data of the Business Software Alliance, the piracy rate globally in 2007[37] was 38% with losses of over USD 47 billion, in the EU Member States 35% and losses of over USD12 billion and in the Republic of Macedonia 68% and over 11 USD million.

3. International sources

10.3.1. The Convention on Cybercrime adopted by the Council of Europe (2001)

The Convention consists of several sections. The first section contains definitions of the basic notions. The second section regulates the measures that should be undertaken on national level by the Member States: measures that refer to the substantive and procedural penal law and competence. Within this section, the following offences that are punishable in the area of internet crime have been defined:

1. Offences against confidentiality, integrity and availability of computer data and systems that incorporate: a) illegal access; b) illegal interception of computer data; c) illegal damaging of databases; d) system interference; and e) misuse of devices;
2. Computer-related offences a) Computer-related forgery; b) Computer-related fraud;
3. Content-related offences (child pornography);
4. Offences related to infringements of copyright and related rights;
5. Aiding or abetting the commission of offences that are punishable; and
6. Corporative liability.

The third section of the Convention regulates the international cooperation and legal aid while the fourth and last section contains the final provisions.

By May 7, 2008, 22 States signed or ratified the Convention, including the Republic of Macedonia.

4. Legislation of the Republic of Macedonia

One could conclude that the Macedonian penal legislation is modern and follows the European and world standards in regard to cybercrime.

---

[36]Combating Counterfeiting and Piracy in the Single Market COM (98) 569, Final Act.

[37]*Fifth Annual BSA and IDC Global Software Piracy Study,* available at: bsa.org.

The Criminal Code of the Republic of Macedonia envisages several offences that are punishable and which are linked directly or indirectly to information technology. The schematic presentation of these offences is given in the graph bellow.

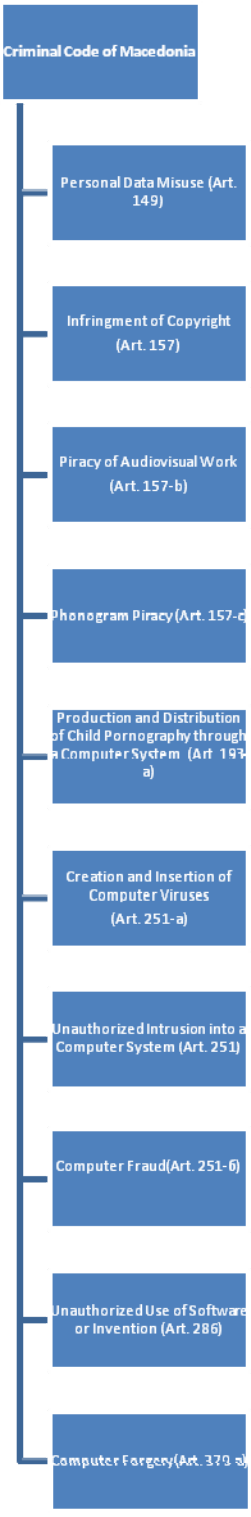


Diagram: Schematic presentation of the offences in the area of cybercrime regulated in the Criminal Code

4.1. Abuse of personal data

In compliance to Article 149 of the Criminal Code, collecting, processing or use of personal data without consent of the citizen represents abuse of personal data. Protection of personal data is one of the constitutional categories (safety and confidentiality of personal data).

Relevant for cybercrime is the form of abuse of personal data that consists of penetration in the personal data computer information system with an intention by the perpetrator to acquire benefit for himself or somebody else or to inflict damages (Article 149, Paragraph 2).

The sanctions for this offence are: a fine or a sentence imprisonment of up to one year.

The most serious form of abuse of personal data is when the crime is committed by an official in the course of performing his/her official duties for which a sentence imprisonment of three months up to three years is envisaged.[38]

4.2. Damaging and illegal penetrating in a computer system

The offence of "damaging and illegal penetrating in a computer system" from Article 251 of the Criminal Code (CC) encompasses: entering, altering, hiding, deleting or destroying or making the computer data and programmes unusable or making the use of the computer system or the computer communications more difficult (Paragraph 1).

The offence is also committed by the one who penetrates the computer system for the purpose of acquiring illegal property or other benefit for himself/herself or for somebody else or causing property or other damages; and for the purpose of transferring computer data that s/he is not supposed to have (Paragraph 2).

In both cases the sanction is either monetary or sentence imprisonment of up to three years.

The form of the offence is more serious if the perpetrator:

- commits the offences from Paragraphs 1 and 2 against a computer system, data or programmes that are protected with special protection measures or are used in the work of the state bodies, public enterprises or public institutions or in the international communications or as a member of a group created for committing such crimes. In this case, the sanction is a sentence imprisonment of up to five years (Paragraph 3);
- commits the offences from the Paragraphs 1 and 2 and acquires significant property benefit or causes a significant damage. In this case, the perpetrator would be punished with sentence imprisonment of six months to up to five years;
- commits the offence from Paragraphs 3 and acquires significant property benefit or causes significant damages. In this case, the perpetrator would be punished with sentence imprisonment of one to five years.

The crime of damaging and illegal penetration in the computer system also refers to illegal production, acquisition, selling, storing or

[38]More about the punishable crime "Abuse of personal data" see: Камбовски, В. (1997), *Казнено,* p. 129.

making available to others special devices, means, computer programmes or computer data intended or suitable for committing the offences from Paragraphs 1 and 2. The sanction is monetary or sentence imprisonment of up to one year.

4.3. Creation and insertion computer viruses

Article 251-a from the Criminal Code regulates the making or taking over of computer viruses from somebody else, with the intention of inserting it in somebody else's computer or computer network. The sanction for this crime is monetary or sentence imprisonment of up to one year.

A more serious form of this offence is the use of a computer virus and causing damages in somebody else's computer, system, data or programme. In this case, the sanction is a sentence imprisonment of up to five years (Paragraph 2).

If with the crime from Paragraph 2 a more significant damage was caused or the crime was committed as part of a group for committing such a crime, the perpetrator will be punished with sentence imprisonment of one to five years.

4.4. Computer fraud

The Article 251-b of the Criminal Code envisages a monetary sanction or a sentence imprisonment of up to three years in the cases of illegal acquisition of property for oneself or somebody else by entering untrue data in a computer or information system; by failing to enter true data; by forging an electronic signature; or causing untrue results to appear for somebody else during electronic processing and transfer of data.

If the perpetrator acquires more significant property s/he should be sanctioned with sentence imprisonment of up to five years, and if the perpetrator acquires significant property s/he should be sanctioned with sentence imprisonment of one to ten years.

Illegal production, acquisition, selling, storing or making available to others special devices, means, computer programmes or computer data intended for committing the crime from Paragraphs 1, should be sanctioned with monetary sanction or sentence imprisonment of up to one year.

4.5. Production and distribution of child pornography using a computer system

Production of child pornography for the purpose of its distribution as well as transfer or offering or in some other way making child pornography available via a computer system represents a punishable crime, according to Article 193-a. The sanction for this is a sentence imprisonment of three to five years.

Acquisition of child pornography using a computer system for oneself or somebody else, as well as possession of child pornography in the computer system or medium that serves for storing computer data

with the intention of showing them to somebody else or for distribution is punishable with a sentence imprisonment of six months up to three years.

4.6. Computer forgery

According to Article 379-a of the CC computer forgery is unauthorised production, entering, altering, deleting of computer programmes that are decided or suitable to serve as a proof of facts that have value in legal relations or making them unusable, as well as use of those data or programmes as true. The sanction is a monetary or sentence imprisonment of up to three years.

A qualified form of computer forgery exists when the crime is committed in relation to computer data or programmes that are used in the work of public bodies, public institutions, enterprises or other legal and natural persons that perform activities of public interest, or in the legal traffic with abroad, or if their use causes significant damages. In these cases the sanction is a sentence imprisonment of one to five years (Paragraph 2).

Illegal production, acquisition, selling, storing or making available to others special devices, means, computer programmes or computer data intended for making computer forgeries is punishable with a monetary sanction or sentence imprisonment of up to three years (Paragraph 3).

4.7. Punishable crimes whose subject of protection is intellectual property

The Criminal Code of the Republic of Macedonia envisages several punishable crimes where the computers are used as means for committing the crime or a medium for storing data when committing the crime where the subject of protection is intellectual property.[39]

The violation of copyright or related rights represents unauthorised publication, showing, reproduction, distribution, performing, broadcasting or in another way illegal encroaching on somebody else's copyright or related right i.e. a work, performance or subject of related right (Article 157, Paragraph 1). The sanction is a monetary or sentence imprisonment of up to one year. If the crime from Paragraph 1 was used for acquisition of a significant property, the sanction is sentence imprisonment of three months to up to three years.

If the crime from Paragraph 1 was used for acquisition of significant property, the sanction is sentence imprisonment of six months to up to five years.

The subject of protection of the punishable crime of **unauthorised use of somebody else's invention or software (Article 286)** is the right of the inventor, legally regulated and protected as an industrial property right. The crime is committed by the person who

[39]More about the penal legal protection of intellectual property see: Наумовски Г., Груевска А., Стефаноски Љ. (2007): ''Казнено-правните аспекти на интелектуалната сопственост во Република Македонија'' in: *Зборник во чест на Панта Марина,* Правен факултет „Јустинијан Први“ Скопје.

uses, publishes, gives or transfers somebody else's registered or protected invention without authorisation, as well as the one who uses somebody else's software in an unauthorised manner.

The punishable crime of **audiovisual work piracy (Article 157-b)** whose subject, the audio-visual work i.e. videogram or its in unauthorised way multiplied copies regardless whether those are 35mm (cinema right), video and DVD rights or Video – CD rights is protected from illegal production, import, reproduction, distribution, storage, renting, selling or in another way making it available to the public.

The frequent violations of copyright and related rights of music works impose the need of introducing the crime of **Phonogram Piracy (Article 157-c),** therefore incriminating phonogram piracy regardless whether it is a musical work reproduced on a cassette, CD, DVD or Video-CD rights.

Literature:

Adamski A. (1998) *Crimes Related to the Computer Network. Threats and Opportunities: A Criminological Perspective.* Helsinki, Finland: European Institute for Crime Prevention and Control, affiliated with the United Nations (HEUNI). Retrieved on December 15, 2006 from: http://www.ulapland.fi/home/oiffi/enlist/resources/HeuniWeb.htm.

Bainbride, D. I (2004): *Introduction to Computer Law,* Pearson.

Burden, K., Palmer, C., (2003): Internet Crime: Cyber Crime-A New Breed of Criminal? *Computer Law and Security Report*. 19 (3): 222-227.

Chen, T., Robert, J. (2004): *Statistical Methods in Computer Security.*

Cyberterror: Prospects and Implications, Centre for the Study of Terrorism and Irregular Warfare, Naval Postgraduate School in Monterey, 1999.

Combating Counterfeiting and Piracy in the Single Market COM (98) 569, Final Act.

Denning, D. E. (2000): *Cyberterrorism, Testimony Before the Special Oversight Panel on Terrorism Committee on Armed Services,* U.S. House of Representatives, Georgetown University.

Fen Lim, Y. (2007): *Cyberspace Law: Commentaries and Materials*, 2nd edition, OUP Sydney.

Filol, E. (2005): *Computer Viruses: From Theory to Application,* Birkhauser.

Fifth Annual BSA and IDC Global Software Piracy Study, available at bsa.org.

Graborsky, P. N., Smith, R. G., (1998): *Crime in the Digital Age: Controlling Telecommunications and Cyberspace Illegalities,* Transaction Publishers.

Harms, L. (2007): *The Enforcement of Intellectual Property Rights by Means of Criminal Sanctions, An Assessment.* WIPO Advisory Committee on Enforcement, Geneva, November 2007.

Internet Crime Report, 2007, FBI's Internet Crime Complaint Center (IC3), available at http://www.ic3.gov/media/annualreports.aspx

Jaishankar K. (2007): ''Cyber Criminology: Evolving a novel discipline with a new journal'' in *International Journal of Cyber Criminology,* Vol. 1 Issue 1 January 2007.Retrieved on March 15, 2007, from http://www40.brinkster.com/ccjournal/editorial.htm

Камбовски, В. (1997): *Казнено право, посебен дел,* Просветно дело, Скопје.

Letter of the Dutch Parliament to EU Commissioner Frattni, concerning the IPERD2 Directive, July 2006, available at europapoort.nl (10.01.2009).

McQuade, S.C III (2006): *Understanding and Managing Cybercrime,* Pearson.

Наумовски Г., Груевска А., Стефаноски Љ. (2007): ''Казнено-правните аспекти на интелектуалната сопственост во

Република Македонија'' in *Зборник во чест на Панта Марина, Правен факултет „Јустинијан Први“ Скопје.*

Ogilvie, E. (2000): ''The Internet and Cyberstalking'', paper presented at the Stalking Criminal Justice Response Conference, Australian Institute of Technology, Sydney.

Shelly, L. (2002): ''The Nexus of International Criminals and Terrorism'' in: *International Annals of Criminology,* 20 (1/2), 85-92.

Smith, R., Grabosky, P., Urbas, G. (2004): *Cyber Criminals on Trial,* Cambridge.

Synovate, *FTC Identity Theft Survey Report,* Washington D.C., 2003.

Taylor, P.A. (1999): *Hackers: Crime in the Digital Sublime,* London, Rutledge.

The President's Working Group on Unlawful Conduct on the Internet, *Appendix to the Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet,* March 2000.

United States Report of the Working Group on Intellectual Property Rights, U.S. Information Infrastructure Task Force 1995.

Wienbar,S.(2009): *Perspective: The Spyware Inferno* (http://news.cnet.com/2010-1032-5307831.html; 01.03.2009).