Law and Internet Foundation

Criminal Justice 2007

JUSTICE IN THE DIGITAL ERA

Analytical Report

With the financial support of the Criminal Justice Programme
The European Commission - Directorate General Justice, Freedom and Security

With the partnership of

APTI Asociatia pentru Tehnologie si Internet

DFLabs Managing Infosecurity Risks

University of BRISTOL

Project Title	Justice in the Digital Era: Strengthening the capacity of magistrates in Bulgaria and Romania to investigate, prosecute and prosecute judgements in cases involving cybercrime
Project No.	JLS/2007/JPEN/225, ABAC № 30-CE-0178633/00-29
Country	Republic of Bulgaria
Implemented by	Law and Internet Foundation
Address	36-B, Patriarh Evtimiy Blvd. 1000 Sofia, Bulgaria
Telephone	+359 2 981 50 97
Fax	+359 2 981 50 97
Email:	george.dimitrov@dpc.bg
Contact Person	George Dimitrov

Report Date:	6 November 2008
Version:	v0.2
Authors:	Dr. George Dimitrov, President of the Law and Internet Foundation (Bulgaria) Bogdan Petrov, Centre for ICT Law (Bulgaria) Oleksandr Pastukhov, Centre for ICT Law (Bulgaria) Desislava Krusteva, Attorney-at-Law (Bulgaria) Dimitar Markov, Centre for the Study of Democracy (Bulgaria) Bogdan Manolea, APTI Centre (Romania) Dr. Maxim Dobrinoiu (Romania) Andrew Charlesworth, Senior Research Fellow, University of Bristol (United Kingdom) Dario Forte, CFE, CISM, University of Milan (Italy)
Start Date:	31 December 2007
End Date:	30 April 2009
Project Period:	16 months

TABLE OF CONTENTS

I. INTRODUCTION

1. THE INTERNET: BACKGROUND, STRUCTURE AND OPPORTUNITIES

Internet, the global alliance of information networks and a model of 'information superhighway' which development was supervised by world governments, was created by the US Defence Department in the late 60s of the 20th century with the purpose of transmitting launch orders from the command center to the launch pad when all other connections were useless. The Advanced Research Projects Agency (ARPA) was set up with that purpose. Later its mission expanded to include designing a system allowing access to US computer resources to many users simultaneously. As a result, the Agency created a network called ARPAnet.

The existence of such a network joining the country's main computer centers as well as the usage of technologies for information transmission distributed in autonomous packages allowed the organization of a flexible structure including all kinds of computers. The employment of their 'common language' -- TCP/IP protocols, which were swiftly adopted by the military for use in their own networks, MILnet, and by the universities was supported by the five extensive computer centers of the National Science Fund (NSF). The centers were equipped with supercomputers to ensure that the US scientific community had access to the information stored there. As a result, all extensive university computer centers joined the NSF's network which laid the foundation for all smaller networks. At that time it became possible to access the network via any computer logged on to it.

With a view to supporting and expanding the NSF network, in 1987 its management rights were transferred to private investors such as Merit Network Inc., IBM and NCI. In 1992 NSF withdrew its funding from the 'network of networks' thus allowing funding from other sources. From that time onward, the number of constituent networks on the Internet started growing constantly. In 1996 it covered 25 000 networks and 40 million users worldwide[1]. In August 2008 there were more that 176 million active Internet websites[2].

Nowadays Internet is a routine way for information transmission of any kind and is easily accessed by any personal computer user from anywhere on the planet thanks to satellite links.

[1] See Olivier Hance, Business and Law on the Internet (Best Of Editions, 1996), p. 40
[2] See http://news.netcraft.com/archives/2008/08/29/august_2008_web_server_survey.html.

The existence of Internet services such as Email, World Wide Web (WWW or Web), Telnet (distant access), F.T.P (File Transfer Protocol), Gopher, discussion groups (news groups), Internet Relay Chat (IRC or simply chat) and the regular emergence of new hybrids (e.g. IP telephony) contribute to enhancing the influence of Internet over all aspects of everyday life – education, work, healthcare and leisure activities.

The use of Internet in commerce, banned in the early days of the network, is growing rapidly in recent years. More and more businesses use Internet for advertising, marketing, providing services, contract signing, making and receiving payments, internal and external communication, market research, personal development models, business information exchange, personnel management and recruitment. According to some estimates, in 2008 in the US alone, goods and services amounting to 204 trillion dollars[3] shall be purchased on the Internet.

Data from the International Telecommunication Union states that in 2005 964, 2717 million people worldwide had Internet access[4]. In December 2007, Internet World Stats announced that 2.2 million people or 30% of Bulgaria's population and 7 million people or 31.4% of Romania's used the Internet.[5] According to some forecasts, in 2010 the total number of Internet users will have reached 1 781 billion.[6]

2. LEGAL ISSUES FOLLOWING THE EMERGENCE OF INTERNET

Along with its rapid development, Internet alters well-known socio-economic paradigms and the law does not make an exception.

[3] See *US Retail E-Commerce Resilient*, eMarketer, Apr. 16, *at* http://www.emarketer.com/Article.aspx?id=1006171&src=article_head_sitesearch.
[4] See http://www.itu.int/ITU-D/icteye/Reporting/ShowReportFrame.aspx?ReportName=/WTI/InformationTechnologyPublic&RP_intYear=2005&RP_intLanguageID=1.
[5] See http://www.internetworldstats.com/stats4.htm.
[6] See http://www.etforecasts.com/products/ES_intusersv2.htm#toc.

Regrettably, the existing legal framework in this area is founded on the realities at the time of the 'digital revolution' and in most cases is incapable of adequately adapting the social relations which appeared as a result of the development of information technologies.

Many years have to pass before the law catches up with contemporary technologies, if at all. Such a situation creates a number of problems for IT experts. They now need to be aware of the legal consequences of their actions on the Internet. One of the problems they face is to be able to anticipate how contemporary legal amendments can solve issues arising from the functioning of the Internet.

The above-mentioned issues refer not so much to developed countries such as the US, where the 'core' of Internet lies and the experts, 'the global trendsetters' of computer technologies, are based as to the less informatized countries, Bulgaria and Romania included. Although drafting specialized legislation has just begun, all prerequisites are present for both countries to make a significant contribution to the development of the 'paperless' world of information technologies.

II. ANALYSIS

1. CYBERCRIME – NOTION AND HISTORY

The notion "cybercrime" could be seen for the first time in the specialized scientific literature in the 1960s in relation to the cases of illegal use of computer systems, computer sabotage and computer espionage. The first more profound studies in the area of cybercrime were published in the 1970s, provoked by the occurrence of several extensive cases of abuses related to the use of information technologies. At the same time, many countries adopted specialized legislation in the area of personal data protection, in which they included provisions sanctioning infringements against such data that is collected, stored and transmitted electronically. Historically speaking, these were the first legal provisions in the area of cybercrime.

At the end of 1970s and at the beginning of 1980s the issue of sanctioning cybercrime acquires an ever growing impact as a result of the drastically increased number of cases of infringements committed through the use of computer and computer systems. The first cases of hacking, computer viruses, software piracy, etc. occurred then. In relation to many such cases, the traditional criminal legislation turns to be inapplicable, which forces many states to adopt new provisions incriminating various types of cybercrime, mostly in the area of the economic relations.

In the 1990s, cybercrime went beyond the boundaries of economic crime and started to affect an ever growing circle of public relations in the area of the state governance, administrative services, healthcare, transport, etc. The fast development of Internet as a global information and communication environment also poses a number of serious issues for the criminal policy of many states. The information technologies turn to a means of performing criminal activity by organized groups and to a serious factor in terms of national and international security.

All this leads to continuous striving of the states for improving the legal framework of cybercrime and gives a new impetus for the development of the international cooperation in this area. A great number of new provisions are adopted in the national legislation of some states and there start a number of international initiatives directed to synchronizing the internal

framework and creating mechanisms for efficient international cooperation in the fight against cybercrime.

In Europe, there is legal framework of cybercrime in all Member States of the European Union, as well as in Switzerland, Norway, Iceland, etc. Cybercrime is regulated also in the USA, Canada, Russia, Ukraine, Mexico, Australia, New Zealand, as well as in various states from Asia (Japan, Singapore, China, Malaysia, India), South America (Brazil, Chilly, Venezuela) and Africa (South Africa, Tunisia).[7]

In most of the states, the legal framework of cybercrime is included in the criminal codes of the respective states. From the point of view of the systematic place of the legal framework, more often the corpora delicti of the cybercrimes are formulated as qualified corpora of traditional crimes, such as theft, fraud, copyright infringement, etc., which are different from the main corpus delicti in terms of the special way of the crime commitment. More rarely, cybercrimes are included in separate sections of the criminal acts (Brazil, Estonia). In comparatively few states, cybercrime is regulated in special acts (Romania, China, India), and in some states there is a parallel framework in two normative acts (Japan, the USA).

In part of the states, mostly in those where cybercrime is regulated by a special law, the legal framework includes legal definitions of the main definitions used for the corpora formulation (computer, computer system, computer network, computer programme, computer data, etc).

Most of the states provide similar sanctions for cybercrime. The most common punishment is imprisonment for a different period of time (from 3 months to 12 years) depending on the nature of the infringement and the size of the damages caused. Along with imprisonment as an alternative or cumulative punishment, comparatively often a fine is also provided, as its size usually depends on the size of the damages caused. In China, deprivation of an access to Internet for a certain period of time is provided as a punishment.

[7] For more details on the legal framework of the cybercrimes in other states, see: Legislative Study on Cybercrime, Programme "Student Internships at the Parliament", Sofia, July 2001. The study covers the internal legislation of all European Union Member States and legal acts of countries from Eastern Europe, Asia, North and South America.

According to the criminal acts of most of the states, cybercrimes are of common nature. Only in Germany and Poland are provided cybercrime cases prosecuted under the victim's initiative.[8]

[8] For more details on the international cooperation for the fight against cybercrime, see: The Legal Framework – Unauthorized Access to Computer Systems. Criminal Regulation in 44 Countries (Updated April 7th, 2003) by Stein Schjolberg, Chief Judge, Moss Tingrett District Court, Norway.

2. LEGAL FRAMEWORK OF THE COMPUTER CRIMES UNDER THE BULGARIAN CRIMINAL LAW

2.1. Establishment and development of the legal framework – historical background

The legal framework of cybercrimes in Bulgaria is introduced by the Bulgarian Criminal Code (CC). Systematically, the major part of cybercrimes is organized in one of the recently created Chapter IX "a", called "Computer Crimes". Only the computer fraud (Art. 212a of CC) is regulated by the Chapter holding provisions on crimes against the property due to its specific subject and its proximity to the classic corpus of fraud under Art.212 of CC. Outside these regulations, computer crimes also include some corpora of otherwise traditional crimes that in one or another way are related to the use of information technologies. Such are the infringement of correspondence secret for a digitally sent message (Art. 171, Para. 1, Line 3 and Para. 3 of CC), formatting or damaging property of another by accomplishing access without right to a computer (Art. 216, Para. 3 of CC), false documentation in an digitally sent message (Art. 313, Para. 1 and 3 of CC). To the computer crimes we can also add the corpora of the crimes against intellectual property related to the use of information technologies (Art. 172a of CC), as well the digital dissemination of pornographic materials, including child pornography (Art. 159 of CC). Last in the legal framework of computer crimes are included the legal definitions of the terms related to these acts, such as "computer system" (Art. 93, Line 21 of CC), "computer data" (Art. 93, Line 22 of CC), "computer and information services provider" (Art. 93, Line 23 of CC), "computer network" (Art. 93, Line 25 of CC), "computer program" (Art. 93, Line 26 of CC) and "computer virus" (Art. 93, Line 27 of CC).

The legal framework of the computer crimes was introduced by the amendments of CC from September 2002.[9] In fact, it was born as a combination between the two bills introduced to the Parliament on the amendment of the Criminal Code. When formulating the corpora of most of the crimes, preference was given to the Bill introduced in July 2001.[10] For the legal definitions of the basic terms was used the other draft, introduced by the Council of Ministers in April

[9] See Criminal Code Amendment Act, adopted by the Thirty-Ninth National Assembly on 13th September 2002, promulgated in *State Gazette,* Issue 92 from 27th September 2002.

[10] See Criminal Code Amendment Bill, introduced to the National Assembly by Mihail Mikov (MP) on 19th July 2001, № 154-01-24.

2002.[11] The final result of this approach was that an internally contradictory framework was created and there was undesired discrepancy between the texts of the corpora delicti on the one hand and the legal definitions on the other.

The terminological discrepancy between the corpora delicti and the legal definitions, as well as a number of other weaknesses of the legal framework caused justified criticism in the legal community and as early as in January 2005 the Government introduced to the Parliament Criminal Code Amendment Bill, mostly concerning the texts on the computer crimes.[12] Due to its late introduction (as late as several months before the end of the Parliament's term of office) this bill was discussed only in the Parliament Committees but was voted on a plenary session even at the first reading.

The next government in its turn prepared a new Bill of the amendment on the legal framework of the computer crimes, which, together with a number of other amendment proposals for the criminal legislation, was introduced to the Parliament in March 2006.[13] However, subsequently the Bill has been withdrawn, without being voted at the first reading.

In August 2006 a group of members of the Parliament introduced the third Bill for amendments of the regulations on computer crimes.[14] This Bill was voted at the first reading in March 2007 and subsequently, after some changes, became a major part of the Criminal Code Amendment adopted in April 2007.[15] By this Amendment, a considerable revision took place of most of the texts related to computer crimes, as their edited version in most of the cases was considerably improved. A major part of the discrepancies existing up to that moment were removed. New legal definitions were added and there was achieved the required terminological compliance between the legally defined terms and the ones used for formulating the corpus of each crime.

---

[11] See Criminal Code Amendment Bill, introduced to the National Assembly by the Council of Ministers on 19th April 2002, № 202-01-22.

[12] See Criminal Code Amendment Bill, introduced to the National Assembly by the Council of Ministers on 5th January 2005, № 502-01-5.

[13] See Criminal Code Amendment Bill, introduced to the National Assembly by the Council of Ministers on 22nd March 2006, № 602-01-15.

[14] See Criminal Code Amendment Bill, introduced to the National Assembly by the Members of Parliament Svetoslav Spassov and Maria Angelova-Koleva on 9th August 2006, № 654-01-117.

[15] See Criminal Code Amendment Act, adopted by the Fortieth National Assembly o 26th April 2007, promulgated in *State Gazette,* Issue 38 from 11th May 2007.

In order to present a comprehensive picture for the purpose of this report, parallel to the analysis of the regulations of each crime presently in force, the old versions of the texts also will be also analysed, as well as the more important amendment proposals included in the bills that haven't been adopted by the Parliament.

2.2. Basic Terms

Art. 93. The words and phrases mentioned below are used in this Code with the following meaning:

...

21. "Computer system" is each separate device or combination of interrelated or similar devices that provides or one of which elements provides automatic data processing under a certain program.

22. "Computer data" is each presentation of facts, information or terms in a form susceptible to automatic processing, including computer programs.

23. "Computer and information services provider" is each legal or physical person that provides an opportunity for communication via a computer system or that processes or stores computer data for this communication service or for its users.

...

25. "Computer network" is a combination of interconnected computer systems or device that provides an opportunity for exchange of computer data.

26. "Computer program" is a sequence of machine instructions that are able to make a computer system perform certain functions.

27. "Computer virus" is a computer program distributed automatically and without the will or without the knowledge of the users of the computer systems and is designed for setting computer systems or computer networks in conditions undesired by their users or for making them achieve undesired results.

28. "Pornographic material" is obscene, unacceptable or incompliant with the public morality material that presents overt sexual behaviour. Such is considered a behaviour that presents actual or simulated sexual intercourses between person of the same or the opposite sex, sodomy, masturbation, sexual sadism or masochism or lascivious showing of one's reproductive organs.

2.2.1. General Notes

For formulating the corpora delicti of the computer crimes CC uses a great number of specific terms related to the use of information technologies. The accurate definition of the contents of these terms is of great significance for the effective application of the regulations. The legal

framework adopted in 2002 showed some inconsistency due to the inadequate terminological coordination between the Bills introduced to the Parliament. A major part of the legal definitions included in the first drafts of the Bills could not find place in the adopted text of the Act and in this way terms such as "computer", "computer resources", "information network", "computer program", "computer virus", etc remained without legal definitions although they have been used for the formulation of the separate corpora delicti. The only terms for which were provided legal definitions were "computer information system", "computer information data" and "computer and information services provider". Besides, most of the regulations from the Special Part of CC do not comply terminologically with the legal definitions under Art. 93 of CC.

Such inconsistency created prerequisites for difficulties in interpreting and applying the law, especially taking into consideration the complex and not familiar enough nature of the computer crimes. By the amendments on CC from April 2007, a major part of these weaknesses was eliminated, as the existing definintions were made precise, new definitions were added and the terminology in the general and the specific part was standardized to a great extent.

In its present edited version Art. 93 of CC gives legal definitions of six terms directly related to the computer crimes – "computer system", "computer data", "computer and information services provider", "computer network", "computer program" and "computer virus".

2.2.2. Computer System

In accordance with Art. 93, Line 21 of CC, "computer system" is each separate device or combination of interrelated or similar devices that provides or one of which elements provides automatic data processing under a certain program. The definition repeats verbatim the definition of the same term under Art.1 of the Convention on cybercrime.

The term "computer system" covers all devices designed for automatic digital data processing. Such a device can include hardware and software, as well as devices for data input, output and retention. In this case "automatic" means without direct human intervention, and "data processing" means that the data in the system are being processed via computer program performance. The computer system usually consists of a processor and various devices that

perform a specific function through interaction with the processor, for example, printer, monitor, CD-ROM, etc.

By the Criminal Code Amendment from April 2007 the term "computer system" replaced the initially defined term "computer information system" but the definition itself was kept. In this way, the terminology used by CC was brought into line with that of the Convention on cybercrime, which also uses the term "computer system".

By the same Amendment were edited most of the texts from the Special Part of CC related to the individual computer crimes. Before the amendments, although it has been legally defined, the term "computer information system" has not been used in any of the texts from the Special Part of CC. Instead of it, when formulating the corpora delicti, the legislator used the terms "computer resources" (Art. 319a, Para. 1 of CC) and "computer" (Art. 319b, Para. 1 and Art. 319d, Para. 1 of CC), about which however there were no legal definitions. By the Amendment this incompliance was eliminated and the terms "computer resources" and "computer" were replaced by "computer system". The only exception remained the text of Art. 216, Para. 3 of CC missed by the legislator, in which the term "computer" was kept.

2.2.3. Computer Data

Computer data is defined in Art. 93, Line 22 of CC as each presentation of facts, information or terms in a form susceptible to automatic processing, including computer programs. The definition is based on the definition of data of the International Organization for Standardization – ISO. "Susceptible to processing" means that the data is in a form that allows its direct processing by a computer system. The term "computer (*adj.*)" shows that the data is in a digital or other form allowing direct processing. Computer data is the resources of the computer. It can be stored in a certain computer system or on an external carrier, for example, magnet or optical disc, smart card, chip, etc.

By the Criminal Code Amendment from April 2007 the term "computer data" replaced the term initially used in the Act "computer information data". In this way, the same as with the term "computer system", the terminology in CC was standardized with that under Art. 1 of the Convention on cybercrime that also uses the term "computer data". However, unlike the term "computer system", the definition itself of the term "computer data" was also changed. The

original variant, which was following the Convention text verbatim, joined the definition of two terms – computer data and computer program. According to this variant, the data was defined as each presentation of facts, information or terms in a form susceptible to automatic processing, *including* such a program that is able to make a computer system perform a certain function. With the purpose of introducing shorter and clearer definitions, by the Amendment the Bulgarian legislator separated the two definitions, as he envisaged an individual legal definition of "computer program" and excluded from the definition of the term "computer data" the description of the program as such (a program that is able to make a computer system perform a certain function), referring to the new definition of "computer program".[16] As a whole, the latter follows the sense of the regulations on the Convention, although the Convention itself does not provide a separate definition of this term, and describes it within the definition for "computer data".[17]

By the same amendments were edited also the corpora delicti, in which the old term "computer information system" has been used. Before the Amendment, in the Special Part of CC both terms have been used – "computer information data" (212a, Para. 1 and 2 of CC) and "computer data" (Art. 319a, Para. 1 and Art. 319b, Para. 1 of CC). After the Amendment this incompliance is already eliminated and the law uses the term "computer data" everywhere.

2.2.4. Computer and Information Services Provider

In accordance with Art. 93, Line 23 of CC, "computer an information services provider" is each legal or physical person that provides an opportunity for communication via a computer system or that processes or stores computer data for this communication service or for its users. The definition follows almost verbatim the definition of the term "service provider" under Art. 1 of the Convention on cybercrime. In this way, the defined term covers a very broad circle of people related in one or another way to transmitting or processing data by computer systems. These people can be divided into three main groups. In the first place are all the persons (public or private) who provide to the users the possibility to communicate between themselves. It does not matter whether the users are a closed group (for example, the

[16] Proposals for the separation of the two definitions have been discussed in the legal texts as early as before the amendments made in 2007. For more arguments in favour of the definitions separation, see Markov, D., *Legal framework of the computer crimes under the Bulgarian Criminal Law*, in: *Electronic document and electronic signature. Legal treatment*. Ciela (Sofia), 2004, p. 374.

[17] The Amendment introduced also a curious although minor from a legal point of view grammatical editing of the definition, as the used in the original version disputable in terms of grammar plural form of the word "information" – "informations", was replaced with the singular form – "information".

employees of an enterprise who are provided with the service through a corporative network) or the provider offers their service publicly, as well as whether this is done against payment or free of charge. In the second place are the persons who store or in some other way process data on behalf of the persons providing the abovementioned services. In the third place are the persons who store or in some other way process data on behalf of the services users.

The term "computer an information services provider" is not used anywhere in the Special Part of CC. Only in the formulation of the regulation of Art. 319e of CC the law refers to "information services provision". However, as far as this regulation refers to the obligations of the intermediary of an electronic announcement under Art. 6, Para. 2, Line 5 of Electronic Document and Electronic Signature Act (EDESA), there will be found application of the definition of intermediary under Art. 6, Para. 1 off EDESA. Thus, in practice, the definition of the term "computer an information services provider", with the current version of the corpora in the Special Part, is redundant.[18]

The logical systematic place of the definition of the term "computer an information services provider" is in the Code of Criminal Procedure (CCrP), as precisely it uses the definition. In accordance with Art. 172, Para. 3 of CCrP, the computer an information services providers are obliged to assist the Court and the bodies of the preliminary proceedings with gathering and recording computer information data by applying special technical devices when this is required for detection of the grievous deliberate crimes mentioned in the law.

2.2.5. Computer Network

The legal definition of the term "computer network" was introduced by the Criminal Code Amendment from April 2007. Before that the law was using two separate terms – "information network" (Art. 319d, Para. 1 of CC) and "computer network" (Art. 171, Para. 3 of CC), as there was not a legal definition for either of them. By the amendments the terminology was standardized everywhere and CC already uses only the term "computer network".

[18] There was a proposal for repeal of the regulation of Art. 93, Line 23 of CC in two of the Criminal Code Amendment Bills – from January 2005 and from August 2006. And as in the first case the whole Bill did not reach voting at a plenary meeting due to the end of the Parliament's term of office, in the second case the proposal was repealed when the bill was discussed in the parliamentary committees.

According to Art. 93, Line 25 of CC, the computer network is a combination of interconnected computer systems or device that provides an opportunity for exchange of computer data. The connections between the individual components in the network can be land ones (e.g. via cable) and/or wireless (e.g. via radio waves, infrared rays, satellite).

There are various classifications of the computer network types. By the property, the networks can be home ones (connected in a network of devices with built-in computers, which form home's infrastructure), corporate ones (closed networks used only by the employees of a certain corporation) and public ones (networks open for use by all users, which can cover a certain region, state or the whole world). By the geographic restrictions, the networks can be local ones (serve small territories, most often individual buildings), urban ones (serve individual settlements or parts of settlements) and regional ones (connect computers that are in different geographic locations in a certain region). On their part, the individual networks also can get connected between themselves. Internet is a global network consisting of many interrelating networks, all using the same protocols. There are other types of networks as well, connected or not to Internet, via which computer data can be exchanged.[19]

Computer systems can be connected to the network as endpoints or as means of mediating the communication on the network. In this case, it is important that the combination of interconnected computer systems provides an opportunity for data exchange, which distinguishes the computer network from the individual computer systems interconnected in it.

Besides the interconnected computer systems, the so-called "devices" are also included in the definition for a computer network. These are the various types of devices that are not computer systems but participate in the construction of the network and have a certain role in the data exchange. Such devices are: routers that send the data protocols via the shortest possible way to their destination; switches that provide to each network computer individual connection with another computer from the network; hubs that copy the information received by one port and prepare it for sending through the other ports, etc.[20] As it is not clear from the regulation text to what extent we shall interpret the term "device", case law is to answer this

[19] For more information on the types of computer networks, see Tuzharov, Hr., *Computer Networks*. Pik (Veliko Tarnovo), 2002.

[20] For more information on the structure and components of computer networks, see Tuzharov, Hr., *Computer Networks*. Pik (Veliko Tarnovo), 2002.

question. From a theoretic point of view and taking into consideration that the basic feature of the computer network is providing an opportunity for data exchange, a possible criterion for determining which devices are part of the network can be precisely their role in the data exchange.

2.2.6. Computer Program

The legal definition of the term "computer program" was also introduced by the Criminal Code Amendment from April 2007. When adopting the original framework in 2002, one of the proposed Bills projected a legal definition of the term "computer program" but it was not adopted.[21]

In accordance with Art. 93, Line 26 of CC, the computer program is a sequence of machine instructions that are able to make a computer system perform certain functions. To a great extent the definition is based on the description of a computer program included in the definition of "computer data" under Art. 1 of the Convention on cybercrime where it is stated that the computer data also includes each "program able to make a computer system perform a certain function".

Both the Convention on cybercrime and CC view the computer program as a kind of computer data.[22] What distinguishes the program from the other types of data is its property to make a computer system perform certain functions.

For several years the Bulgarian legislator unjustifiably had been making a distinction between the terms "computer program" and "software".[23] This conclusion followed from the old version of Art. 172a, Para. 2 of CC, which determined as a crime against the intellectual property the illegal use of software *or* a computer program. In the theory there is no unified opinion on the distinction between these two terms and very often they are used as synonyms. Grounds for such interpretation are also given by the Copyright and Neighboring Rights Act (CNRA), which determines only the computer programs as subject to copyright. By the

[21] This definition qualified the computer program as a combination of commands and connected information that when accomplished in a certain form, make a computer system or a computer network perform assigned functions.

[22] For the opposite opinion, see Kopcheva, M., *Computer Crimes*. Cibi (Sofia), 2006, pp. 38-39. According to the author, defining the computer program as a kind of computer data is unacceptable in iew of the different nature of these two concepts, which are the two major categories of software.

[23] See also Kopcheva, M., *Компютърни престъпления. Computer Crimes*. Cibi (Sofia), 2006, p. 81. According to the author, the term "software" is broader than the term "computer program".

Criminal Code Amendment Act from August 2006 this incompliance was eliminated, as instead of the list of the different subjects to the Copyright, a broader term was introduced - "foreign subject to copyright or neighboring right". [24]

2.2.7. Computer Virus

The legal definition of the term "computer virus" was introduced as late as by the Criminal Code Amendment Act from April 2007, almost five years after the incrimination of introducing computer virus. When the legal framework of the computer crimes was being created in 2002, one of the discussed Bills proposed a legal definition of this term but it was not adopted by the Parliament.[25]

In accordance with Art. 93, Line 27 of CC, the computer virus is a computer program distributed automatically and without the will or without the knowledge of the users of the computer systems and is designed for setting computer systems or computer networks in a mode, undesired by their users or for making them achieve undesired results.

According to the so-formulated definition, the computer virus is a computer program characterized by two features – the way it is distributed and the impact it is designed for having on the infected computer system. As a whole, the definition follows the dominating opinion in the specialized literature that the computer virus is a program that is self-reproducing and that causes undesired results for the users.

In order to be qualified as a computer virus, on the one hand the program has to be distributed automatically, i.e. without the intervention of the computer system user, and on the other hand – against the will or without the knowledge of this person. The definition is unnecessarily complicated in this part. The automatic distribution in combination with the undesired consequences it causes should be absolutely enough for qualifying a certain program as virus. The attitude of the computer system user should not have relevance in law, as on the one hand it is difficult to prove, and on the other hand – it does not change the objective features of the respective program. Furthermore, if the computer system has a reliable antivirus protection, it

[24] See Criminal Code Amendment Act, adopted by the Fortieth National Assembly on 30th August 2006, promulgated in *State Gazette,* Issue 75 from 12th September 2006.

[25] According to this definition, the computer virus was qualified as a group of computer instructions, which are self-reproducing and are able to infect computer programs or computer data, to absorb computer resources, to change, to delete data or in some other way to disturb the normal functioning of a computer, computer system or computer network.

will notify the user about the existence of a virus, i.e. the virus already will not be distributed without the knowledge of this person.

The automatic distribution is most often accomplished when the created computer virus is attached to an existing program and after this program is performed, it is activated attaching its copies to other programs in the system. The infected programs in their turn copy the virus on other programs. The program to which the virus is attached has to be performed so that the virus is activated. This is also valid for the so-called "macro viruses", which although hidden in documents (computer data), also have a similar impact.

The other characteristic feature of the computer viruses are the consequences they cause to the infected computer systems or networks. In CC these consequences are determined as setting computer systems or computer networks in conditions undesired by their users or making them achieve undesired results. The undesired consequences caused by computer viruses can be various – from a harmless appearance of a message on the screen, through blocking resources and delaying the computer performance to deleting programs or data immediately or at a later stage.

In accordance with Art. 93, Line 27 of CC, in order for a program to be qualified as a virus, it is necessary for it to be designed for causing these consequences. The actual appearance of the consequences does not matter. This decision is justified, as it emphasizes on the virus properties, and not o the actual consequences it causes, which in some cases (for example, when there is a reliable antivirus protection) may not appear at all.

With a view of the undesired consequences, within the scope of the definition of computer virus under Art. 93, Line 7 of CC are included also the so-called "worms", which according to the predominant view in the specialized computer literature, are not viruses. The worms are programs that are self-reproducing without causing other harmful consequences except for overloading the memory due to the self-reproduction itself. However, the memory overload itself is setting the system into a condition undesired by its user, therefore the worms shall be qualified as computer viruses.

All the other programs, which even though cause certain undesired consequences, do not comply with the criteria of the definition under Art. 93, Line 27 of CC, shall not be qualified as computer viruses.

2.3. Copying, Using and Accomplishing Access to Computer Data in a Computer System without Right

> *Art. 319a. (1) A person who copies, uses or accomplishes access to computer data in a computer system without permission when such is required shall be imposed a fine of up to three thousand levs.*
>
> *(2) If the act under Para. 1 is committed by two or more persons having arranged in advance to commit such an act, the punishment is imprisonment for up to one year or a fine of up to three thousand levs.*
>
> *(3) If the act under Para. 1 is committed again or in relation to data for creating an electronic signature, the punishment is imprisonment for up to three years or a fine of up to five thousand levs.*
>
> *(4) If the acts under Para. 1 - 3 are committed in relation to information that is a state secret or other secret protected by law, the punishment is imprisonment for one to three years, if the person is not subject to a graver punishment.*
>
> *(5) If grave consequences have ensued from the act under Para. 4, the punishment is for one to eight years.*

2.3.1. Basic Corpora Delicti

Art. 319a, Para. 1 of CC regulates three major corpora delicti, which are distinguished by the form of the committed act: accomplishing access, copying and using computer data without permission.

The text was considerably improved with the amendments from April 2007. The old version (the person who accomplishes access without right to a computer, copies or uses computer data without permission when such is required) was unclear and was causing problems with the interpretation, especially in relation to the term "computer resources".[26]

[26] There was a proposal for replacing the term "computer resources" with "computer information data" in the Criminal Code Amendment Act introduced in January 2005, which however was not voted by the Parliament. For a detailed analysis of the previous version of the regulation, including proposals for its precision, see Markov, D., *Legal framework of the computer crimes under the Bulgarian Criminal Law*, in: *Electronic document and electronic signature. Legal treatment*. Ciela (Sofia), 2004, pp. 375-380.

A direct target of the crime are the public relations providing the inviolability of the different types of information presented in a digital form and its protection against its finding out, dissemination or any other use without right.

From an objective point of view, the crime is characterized by a specific object of encroachment – computer data within the meaning of Art. 93, Line 22 of CC.[27] The scope of application of the regulation is restricted to the clarification added to the text that the data should be in a computer system.[28] In this way unjustifiably are excluded all the hypotheses in which the data is not in a certain computer system and are stored out of it on another carrier. For example, a smart card is not a computer system within the meaning of Art. 93, Line 21 of CC and the access to the data on it, e.g. data for creating an electronic signature, will not be an indictable act under Art. 319a, Para. 1 of CC. Actually, in most of the cases the access to computer data stored on another carrier can be accomplished only after this carrier is put in the computer system, therefore at the moment of the encroachment the data will be in the system. However, in order to avoid the difficulties in the interpretation and application, the requirement for the data to be in the computer system shall become invalid and the act shall be indictable irrespective of where and how the data is stored.

The executive act of the crime is defined as copying, use and accomplishing access.

Copying is creating a copy (duplicate) of the computer data. In principle, copying itself does not violate the integrity of the data. The specific thing about it is that all copies are identical both between themselves and to the original (as long as we can at all speak about an original in the classic meaning of this concept). The only distinction between them is the time of their creation. Moreover, each copy of computer data is fit for being copied and new identical copies of the data to be made from it. All this determines the high level of public danger of this act and the need for its incrimination.

Using means the use of already existing data. Examples of using data are introducing it in a computer system, sending it to another computer, transferring it to various portable carriers, printing it on a paper carrier, etc.

[27] For more details on the term "computer data", see the analysis of Art. 93, Line 22 of CC (Line 2.2.3 above).
[28] For more details on the term "computer system", see the analysis of Art. 93, Line 21 of CC (Line 2.2.2 above).

According to the Explanatory Report on the Convention on Cybercrime, accomplishing access means penetrating in a certain computer system or in a part of it, including through another computer system when the two systems are connected to each other via public telecommunication networks or are in a common network (e.g. local network or Internet). However, in order for an indictable act under Art. 319a, Para. 1 of CC to be present, it is not enough access to a certain computer system to be accomplished. The access to the system is the broader concept and means presence of certain information in a foreign system. This access is not incriminated by law and that is the reason why the simple sending of a message or a file via electronic mail from one computer system to another, as well as sending an SMS to a mobile phone, cannot be qualified as a crime under Art. 319a, Para. 1 of CC. The executive act of the access without permission finds expression in access to computer data, i.e. presence of such information in a foreign computer system, which enables the offender to find out or to affect in a certain way the data in it. Access to certain data is each providing of an opportunity for finding out, copying, changing or affecting the data in any other way. The access without permission is often in the basis of other computer crimes with a higher level of public danger.

The incrimination of the access without permission as an individual crime is in compliance with the regulation of Art. 2 of the Convention on Cybercrime, which allows the parties to announce as a crime under their internal law the very illegal access to the whole computer system or to a part of it without the necessity for another criminal result.

Art. 319a, Para. 1 of CC determines a comparatively broad scope of the crime of accomplishing access. Along these lines, the Convention on Cybercrime explicitly projects an opportunity for the parties to limit the scope of application of the criminal repression, as they project additional requirements for the indictability of the act, for example, the offence to be committed in breach of the security measures, with the intention of taking computer data or with other criminal intention, as well as in relation to a computer system connected to another computer system. The Bulgarian law adopts a maximally broad approach and does not project such restrictions, by which it considerably expands the regulation's scope of application. This is reasonable, as in this way the computer data is protected against the broadest possible range of violations. An exception from the text's scope of application are only the cases under Art. 9, Para. 2 of CC,

when due to its insignificance the act is not of public danger or its level of public danger is obviously insignificant.

Under all three main corpora delicti the executive act can be accomplished only by acting.

From the objective point of view, in all the three hypotheses it is required for the executive act to have been committed without permission when such is required. The old version of the text used the term "unregulated access", which was closer to the term "illegal access" used by the Convention on Cybercrime, defined in the Explanatory Report on it as "access without right".

The need for permission can ensue both from the regulation of an enactment and under other applicable rules and procedures. The act however shall be indictable when under an enactment the person having granted the permission does not have the right to grant access to the computer to third parties, for example due to enhanced security requirements of the concrete computer. Examples of such enhanced security requirements are the systems for issuing and managing the certificates for advanced electronic signature. One of the requirements about the certification services providers issuing certificates for advanced electronic signature is to provide reliable security to the systems for issuing and managing certificates. In accordance with Art. 9 of the Ordinance on the activity of the certification services providers, on the order of its termination and on the requirements for providing certification services, the systems for issuing and managing certificates should be in specially protected rooms to which access is granted only to duly authorized officials in compliance with their functional obligations. The access to these systems of persons who are not employees of the certification services provider at any event will be unregulated, even when they have received permission from such an official.

The act will not be indictable when we talk about open systems designed for free (unrestricted) access. For example, such are the websites on the Internet. The maintenance itself of a publicly accessible Internet website contains the agreement of its owner to provide access to this website to an unrestricted number of users from the global network. When a person maintains an Internet website, they have various technical means by which they actually accomplish access to the systems of the users visiting their website. The most widely spread such means are the so-called "cookies" – messages which the server that is on a certain Internet website sends to

the browser of the user visiting this website. These messages are stored in the user's system and are sent back to the server each time when the user visits this website. The main purpose of the cookies is to identify the users and possibly to prepare a special outlook of the website depending on the received information (for example, instead of a standard main page the user receives a main page with their name on). According to the Explanatory Report on the Convention on Cybercrime, the application of such standard means incorporated in protocols and programs used in a mass scale taken alone cannot be qualified as illegal access because the circumstance that the user has decided to use these protocols and programs means that they have tacitly agreed with the application of these means. In the case with the cookies this tacit agreement also ensues from the fact that the user has not cancelled explicitly their original installation, neither has subsequently removed them from the system.

A crime will not be present also when the act is committed by a person who exercises their legally regulated powers, for example when conducting an inspection by a competent control body. In this case the act is lawful, regardless of the presence or lack of permission or consent by the person administrating or using the computer.

The moment as at which the court shall assess the presence or lack of permission is the moment of the executive act performance. The subsequent obtaining of a permission has no relation to the indictability of the act, but can be considered an extenuating circumstance, and in certain cases – also a circumstance excluding criminal liability due to insignificance of the act within the meaning of Art. 9, Para. 2 of CC.

In the hypothesis for copying computer data the crime is productive as the result is the newly created copy of the respective data. In the hypothesis for using data the crime is formal (crime of simple perpetration) – it is enough a certain action with the respective data to be present, which can be qualified as use. Accomplishing access also is regulated as a formal crime. For the indictability of the act it is enough the person to have accomplished access to certain data. The crime is completed by the actual commitment of the executive act, without the need for occurrence of another result. [29]

[29] See also Doncheva, D., *Computer crimes under Chapter Nine "a" of the Criminal Code*, Legal Thought, Issue 2, 2003. According to the author, the crime is productive, as the result consists of accessing, revealing the information in the computer.

Each liable person can be subject of the crime. From the subjective point of view, malice is present. The perpetrator realizes that for committing the respective actions, permission is required, and that they have not obtained such, but yet deliberately copies, uses or accomplishes access to the computer data.

The punishment under all the three main corpora is a fine up to 3 000 BGN.[30]

2.3.2. Qualified Corpora

CC regulates several qualified corpora of copying, using and accomplishing access or computer data without permission. Qualifying circumstances are the object of the crime (data for creating electronic signature, information that is a state secret or another secret protected by law), the subject (two or more persons or one person in case of repetition) and the criminal result (appearance of grave consequences).

When formulating the qualified corpora, CC uses only classic qualifying circumstances, without taking into account the specific nature of the computer crimes. There are not taken into consideration the model qualifying circumstances proposed by the Convention on Cybercrime, such as violating the security measures, criminal intention or violation related to the computer system. It is indisputable that these circumstances also enhance the act's public danger level, as at the same time they reflect some specific particularities of this type of acts. For example, the public danger level of an act committed by overcoming special security measures very often will be the same as or even higher than that of an act committed for the second time. It can be judged of the significance of these circumstances also by the opportunity provided in Art. 2 of the Convention on Cybercrime for the parties not to incriminate in their internal law the cases of illegal access in general but *only* those in which the abovementioned qualified circumstances are present. However, in the current version of Art. 319a of CC the presence of any of these circumstances will be judged only when the punishment is individualized, which, however, under the main corpus is only a fine and at that of a comparatively small amount.

2.3.2.1. Qualified corpora in relation to the subject of the crime

[30] In the Criminal Code Amendment Bill introduced in March 2006 it was proposed the fine to be revoked, but the Bill was withdrawn by the mover and the maximal amount was kept.

CC makes provisions for two qualified corpora with a view of the subject of the crime – when the act is committed by two or more persons who have arranged in advance the commitment of such an act (Art. 319a, Para. 2 of CC), and when it is committed for the second time (Art. 319a, Para. 3 of CC).

Art. 319a, Para. 2 of CC makes provisions for a graver punishment (imprisonment for up to one year or a fine up to 3 000 BGN) for the cases when the act is committed by two or more persons who have arranged in advance the commitment of such an act.[31]

In accordance with Art. 93, Line 12 of CC a crime is committed by two or more persons when at least two persons have participated in the commitment itself. This means that at least two persons perform elements of the executive crime. If one of the persons only facilitates the commitment of the crime without performing an element of the executive act (for example, provides a floppy disc on which the perpetrator copies the data), there will be accessory.

Moreover, it is necessary the co-perpetrators to have acted under an advance arrangement for committing such an act. The arrangement is advance when the persons have taken the decision for committing the crime and have coordinated their criminal intentions some time before the act, in a comparatively peaceful state of mind and discussing the motives that are "pro" and "con".[32] The advance agreement shall have for its object copying, using or accomplishing access to computer data, irrespective of whether the persons have specified in advance the object of the encroachment (a particular computer system or data).

Art. 319a, Para. 3 of CC makes provision for a qualified corpus, if the act is committed for the second time. The provided punishment is imprisonment for up to three years or a fine up to 5 000 BGN. Within the meaning of Art. 28, Para. 1 of CC, the crime is committed for the second time, if the perpetrator has committed it after being sentenced with an effective sentence for another similar crime. According to the case law, "crimes identical by type within the meaning of Art. 28 of CC are the crimes by which are performed one and the same or different corpora delicti of one and the same crime, including when it is considered privileged".[33] This means that

[31] In the Criminal Code Amendment Bill introduced in March 2006 it was proposed the fine to be replaced by a probation, but the Bill was withdrawn and the fine was kept.

[32] For more details on the previous concert, see Stoynov, Al., *Criminal Law. Special Part. Crimes against Property.* Ciela (Sofia) 1997, pp. 34-35.

[33] See Decree 2-70-ПЛ., Line 1.

repetition is present when the perpetrator has committed a crime under any of the corpora delicti under Art. 319a of CC, if before that has been sentenced with an effective sentence on any other crime under the same article.

2.3.2.2. Qualified corpora in relation to the object of the crime

The qualified corpora in relation to the object of the crime are provided for in Art. 319a, Para. 3 and 4 of CC.

Under Art. 319a, Para. 3 of CC the special object of the crime is data for creating electronic signature, and the provided punishment is imprisonment for up to three years or a fine up to 5 000 BGN.[34]

In accordance with § 1, Line 7 of the Supplementary Provision of EDESA, the data for the signature creation is unique information such as codes or cryptographic keys used by the signatory for creating an electronic signature. Depending on the type of electronic signature, the data for its creation is different. With the basic electronic signatures this is each piece of information (symmetric or asymmetric keys, pseudo-random numbers, unique information objects, etc) used the creation of the signature. With the advanced and the universal electronic signatures the data for the data for the signature creation is the so-called "private key" – one of a pair of keys used in an asymmetric cryptosystem for electronic signature creation (§ 1, Line 5 of the Supplementary Provision of EDESA). The secret of the data for a basic electronic signature creation is protected by the regulation of Art. 14 of EDESA, according to which no one except for the author has right of access to the data for electronic signature creation. The secret of the private key with the advanced and the universal electronic signature is protected by the regulation of Art. 18 of EDESA, according to which no one except for the author has the right to access the private key.[35]

The qualified corpora delicti with an object data for electronic signature creation was introduced by the Criminal Code Amendment Act of April 2007. The amendment was imposed

[34] In the Criminal Code Amendment Bill introduced in March 2006, it was proposed the fine to be replaced by probation, but the Bill was withdrawn and the fine was kept.

[35] For more details on the secret of the data for electronic signature creation, see Kalaydzhiev, A., Belazelkov, B., Stancheva, V., Dimitrov, G., Markov, D., Yordanova, M., *Electronic Document and the Electronic Signature. Legal Treatment*. Ciela (Sofia) 2004, pp. 73-75 and pp. 99-103.

with a view of the ever more widespread use of electronic signature and hence – the high level of public danger of the violations against the secret of this data, which did not comply with the punishment of a fine up to 3 000 BGN provided under the main corpus.

Under Art. 319a, Para. 4 of CC the special object of the crime is information that is a state secret or another secret protected by law, and the punishment is imprisonment for one to three years, if the perpetrator is not subject to a graver punishment.[36]

The state secret is legally defined in the Classified Information Protection Act (CIPA), which also the order determines the procedures for accessing such information. In accordance with Art. 25 of CIPA, a state secret is the information defined in the list under Appendix № 1, the unregulated access to which would cause danger to or would harm the interests of Republic of Bulgaria related to the national security, defence, foreign policy or the protection of the order established by the Constitution.

For a certain period of time a definition of state secret was provided also by Art. 104, Para. 3 of CC, which defined the state secret as facts, information and objects of military, politics, economic or other nature, the revealing of which by a foreign country or a foreign organization can harm the interests of the Republic and especially its security; the list of the facts, information and objects that constitute the state secret is adopted by the National Assembly and is promulgated in State Gazette. Although the text of Art. 104, Para. 3 of CC was not revoked by the adoption of CIPA, neither was it updated in compliance with the new legal framework of the state secret, this incompliance was eliminated later by the Criminal Code Amendment Act of March 2004.[37] In its current version, the text of Art. 104, Para. 3 of CC reads that the information constituting the state secret is determined by law.

In the criminal doctrine it is accepted that the definition for a state secret includes two cumulatively provided marks – formal and material. The formal mark is that the information constituting the state secret should be included in a list in the form of an appendix to the act.

[36] In the Criminal Code Amendment Bill introduced in March 2006, it was proposed that the imprisonment is increased to five years but subsequently the Bill was withdrawn and the maximal size of the punishment remained unchanged.

[37] See Criminal Code Amendment Act, adopted by the Thirty-Ninth National Assembly on 16th March 2004, promulgated in *State Gazette,* Issue 26 from 30th March 2004.

The material mark is expressed by the circumstance that the unregulated access to the respective information would cause danger for or would harm the interests of the Republic of Bulgaria. In order for certain data to be qualified as state secret, both marks should be present. Information that is included in the special list but the unregulated access to which would not cause danger for, nor would harm the interests of the state is not a state secret. The same applies also for information, the revelation of which would create danger for or would harm the interests of the state but is not included in the special list to the Act.

In the object of the crime under Art. 319a, Para. 4 of CC is also included all other information that is a secret protected by law. The regulation's scope of application was expanded by the amendments from April 2007. The old version provided as an object of the crime only information that is state secret.[38]

The Bulgarian legislation regulates a number of cases of information which privacy is protected by the law. The more important ones include: the insurance secret under Art. 93-94 of the Insurance Code (IC); the social insurance secret under Art. 109, Para. 2 of the Social Insurance Code (SIC); the adoption secret under Art. 67a of the Family Code (FC); the business secret under Art. 26, Para. 1 of CIPA; the industrial and trade secret under § 1, Line 7 of the Supplementary Provisions to the Protection of Competition Act (PCA); the bank secret under Art. 62, Para. 2 of the Credit Institutions Act (CIA); the different types of professional secret under Art. 20 of the Private Executive Magistrates Act (PEMA), Art. 26 of the Notary Act, Art. 35g of the Independent Financial Audit Act (IFAA); etc.

From the subjective point of view, it is characteristic for the qualified corpus under Art. 319a, Para. 4 of CC that the perpetrator realizes the information in relation to which they commit the respective acts is confidential.

The qualified corpus under Art. 319a, Para. 4 of CC has a subsidiary nature. It is applied only in the cases when the perpetrator is not object to a heavier punishment. Heavier punishments are provided, for example, for espionage (disclosing or gathering information that is a state secret with the purpose of disclosing it to a foreign state or foreign organization) under Art. 104, Para.

[38] For more arguments in support of this amendment, see Markov, D., *Legal Framework of the Computer Crimes under the Bulgarian Criminal Law*, in: *Electronic Document and Electronic Signature. Legal Treatment*. Ciela (Sofia), 2004, p. 384.

1 of CC, for disclosing information that is a state secret under Art. 357, Para. 1 and 2 of CC and for disclosing information of a military nature that is a state secret under Art. 393 CC.

The way in which the two qualified corpora are formulated with a view of the object of the crime creates confusion, which can cause difficulties in the practice. The problem ensues from the fact that the violation against information that is a secret protected by the law is provided in a different paragraph than the violation against the data for electronic signature creation. In practice however, the data for electronic signature creation is also information which secret is protected by the law. In its turn, this raises the issue under which text of CC will be qualified the criminal copying, using or accomplishing access to data for electronic signature creation. In case of literal interpreting, it is concluded that for the violations against data for electronic signature creation Art. 319a, Para. 3 of CC shall be applied, and for violations against any other secret protected by the law – Art. 319a, Para. 4 of CC.

However, the problem does not end there, as the regulation of Art. 319a, Para. 4 of CC is applied also in relation to Art. 319a, Para. 3 of CC (the text reads: "if the acts under *Para. 1 - 3* are committed in relation to..."). In this way, it is an absurd situation to obligatorily apply Art. 319a, Para. 4 of CC each time when the object of the violation is data for electronic signature creation, as formally this corpus delicti will be also committed – an act under Para. 3 will be present, committed in relation to information that is a secret protected by the law (in this case – data for electronic signature creation).

Even if it is assumed that the legislator has deliberately distinguished the data for electronic signature creation from the other information that is a protected secret and has provided a different regime in terms of the crimes against it, there still remains the issue with the regulation of Art. 319a, Para. 5 of CC, which provides even heavier punishments when grave consequences have ensued from the act. This regulation is applied only in relation to the acts under Art. 319a, Para. 4 of CC, i.e. in cases of violations against information that is a state secret or another secret protected by law, and cannot be applied when the object of the crime is data for electronic signature creation, although considerably graver consequences may ensue from copying or using data for electronic signature creation than from analogous acts against another protected secret, e.g. the secret of adoption.

The possible solutions for avoiding these contradictions are two: dismissing the data for electronic signature creation from Art. 319a, Para. 3 of CC (and the automatic application of Art. 319a, Para. 4 of CC on the grounds of the fact that the information concerned is a secret protected by law) or moving it to Art. 319a, Para. 4 of CC, where it would be presented as a special case of the protected secret (and where it is anyway its logical place from a systematic point of view, as precisely there are provided the qualified corpora delicti with a view of the crime object).[39]

2.3.2.3. Qualified corpora delicti in relation to the criminal result

The criminal result is a qualifying circumstance under Art. 319a, Para. 5 of CC. This is the only corpus delicti under Chapter Nine of CC, under which a grave crime within the meaning of Art. 93, Line 7 of CC is present, as the provided punishment is imprisonment for one to eight years.

The specific thing in this case is the presence of two qualifying circumstances. One of the qualifying circumstances is the criminal result, which is defined in the law as appearance of grave consequences. Furthermore, however, the regulation explicitly states that it is applied only in relation to acts under Art. 319a, Para. 4 of CC, i.e. the presence of the special object is also required – information that is a state secret or another secret protected by the law.

It is still disputable whether Art. 319a, Para. 5 of CC shall be applied when the grave consequences have appeared as a result of a violation against data for electronic signature creation. As far as the crimes with such data as their object are regulated in Art. 319a, Para. 3 of CC, the application of Art. 319a, Para. 5 of CC seems unacceptable. If, however, it is assumed that the data for electronic signature creation is information that is a secret protected by the law (which it actually is), then if grave consequences have ensued from the act, there will be grounds for the application of Art. 319a, Para. 5 of CC.

[39] For arguments in support of such a proposal, see also Markov, D., *Legal Framework of the Computer Crimes under the Bulgarian Criminal Law*, in Kalaydzhiev, A., Belazelkov, B., Dimitrov, G., Yordanova, M., Markov, D., Stancheva, D., *Electronic Document and Electronic Signature. Legal Treatment*. Ciela (Sofia), 2004, pp. 383-384. The article that analyses the old version of the text of Art. 319a, Para. 4 of CC (providing heavier punishment only if the crime object is information that is a state secret) defends the thesis that precisely I view of introducing heavier punishments for violations against data for electronic signature creation it is required to expand the scope of application of the regulation in relation to any information that is a secret protected by the law.

The problem arises from the amendment made in the original text of the Bill before it was voted at second reading. In its original version the Bill provided an individual qualified corpus delicti for violations against data for electronic signature creation (by creating a new Para. 4, according to which if the acts under Para. 1 – 3 are committed in relation to data for electronic signature creation, the punishment shall be imprisonment for up to three years or a fine up to 5 000 BGN) and an application of the regulation on the grave consequences both in terms of the acts against information that is a state secret or another secret protected by the law and in terms of the crimes with data for electronic signature creation as an object.[40]

From an objective point of view, the appearance of grave consequences should be a direct and immediate result of the executive act. Qualifying the consequences as grave shall be done in the court in every concrete case. As far as the qualified corpus delicti deals only with violations against information that is a state secret or another secret protected by the law, when judging the graveness of the consequences, the court shall be guided by the level of endangering or impairing the interests related to the respective secret.

2.4. Criminal Violations against Computer Programs or Data

Art. 319б. (1) The one that without the permission of the person administrating or using the computer system adds, changes, deletes or formats a computer program or computer data, in non-insignificant cases, is punished by imprisonment for up to one year or a fine up to two thousand levs.

(2) If by the act under Para. 1 are caused considerable damages or other grave consequences have occurred, the punishment is imprisonment for up to two years and a fine up to three thousand levs.

(3) If the act under Para. 1 is committed with the purpose of property benefits, the punishment is imprisonment for one to three years and a fine up to five thousand levs.

Art. 319в. (1) The one that commits an act under Art. 319б in relation to data submitted by virtue of the law, digitally or on a magnet, electronic, optical or other carrier is punished with imprisonment for up to two years and a fine up to three thousand.

(2)) If the act under Para. 1 is committed with the purpose of frustrating one's duty, the punishment is imprisonment for one to three years and a fine up to five thousand levs.

[40] An analogous solution was proposed before also by the Criminal Code Amendment Bill, introduced in January 2005, as in this Bill also the private key has been added to the data for electronic signature creation.

2.4.1. Main Corpora Delicti

A direct object of the criminal encroachments against computer programs and computer data are the public relations providing the inviolability of these programs and data and their protection against illegal damaging.

From objective point of view, the crime is characterized by a special object – a computer program within the meaning of Art. 93, Line 22 of CC or computer data within the meaning of Art. 93, Line 26 of CC.[41]

The executive act is described in four different forms – adding, changing, deleting and formatting. With all the four forms the act can be committed only by acting.[42]

Adding a computer program or computer data is introducing a new program or data in a computer system. Introducing the program or data can be done by the peripheral devices of the computer (e.g. by the keyboard), as well as by their transferring from a portable information carrier (compact disc, floppy disc) or remotely by using another computer system. Taken alone, the adding of a computer program or data doesn't damage the programs and data already existing in the computer program. In some cases, however, such damaging is possible when by the added program or data the normal functioning of the other programs is impaired or the integrity of other data in the system is impaired. A typical example of adding a program that impairs the normal functioning of the system is the introduction of a computer virus, which however is separated as an individual crime under Art. 319d of CC.

Changing a computer system or data means qualitative or quantitative modification of already existing programs or data. The modification usually leads to a change in the program's functioning and to a modification and to a change in the data content.

The deletion means terminating the access of the users to the respective program or data. In most of the cases deletion does not mean a complete erasure of the program or data from the computer system. When a program or data is deleted, the computer erases the information

---

[41] For more details on the definitions of the terms "computer data" and "computer program", see the analysis of Art. 93, Line 22 and 26 of CC (Item 2.2.3 and Item 2.2.6 above).

[42] For more details on the executive acts and the relation between them, see Doncheva, D., *Computer Crimes under Chapter Nine "a" of the Criminal Code*, Pravna Missal, Issue 2, 2003.

indicating its location on the hard disc. This information is used by the operation system for the construction of the computer's directories structure. When this information is erased, the respective program or data becomes invisible to the operation system. It exists but the operation system does not know how to reach it. By recovering this information, which can be done by special programs, the deleted programs or data can also be recovered.

The erasing means a complete obliteration of the program or data from the computer system or network. In case of erasing, the whole information is obliterated and the respective program or data cannot be recovered by any means. In actual fact, the only way of completely erasing certain information from the computer is recording new data on the existing data. The operation system regularly records new information on the data for which the information about its location has been erased. This means that the longer period of time has passed from the deletion of certain data (from erasing of the information about their location), the more likely it is for the operation system to record other data on it and the data to be completely erased.[43]

The crime is productive. With the different forms of the executive act the result is respectively the newly emerged program or data in the system (on adding), the change in the existing program or data (on changing), the lack of an existing program or data (on deleting and erasing).[44]

From an objective point of view, it is necessary that the executive act is executed without the permission of the person who uses or administrates the computer system. The person administrating the system is the one to whom its maintenance has been assigned, and the person using the computer system in practice performs certain actions with it.

[43] In the Criminal Code Amendment Bill, introduced in January 2005, it was proposed the executive acts „delete or format" to be substituted by „remove or temporarily erase". The proposal aimed at highlighting the difference between the cases in which the data can be recovered and the cases in which they are irrecoverably formatted.

[44] In the Criminal Code Amendment Bill, introduced in August 2006, it was proposed that also a specific result is added as an element of the objective part - by the executive act "the operation of the computer system is disturbed". This proposal was dropped as early as during the discussion of the Bill in the Parliament and was not included in the text proposed for voting at the second reading. The legislator's decision is justified, as the adding of another element would complicate unnecessarily the editing of the text, would aggravate the process of proving (disturbing the operation of the computer system would be subject of proof as an element determining the indictability of the act) and would complicate the interpretation when "disturbance" of the system operation is present. The occurrence of specific consequences, including "disturbance" of the system operation, could be considered by the court at their assessment whether the case is insignificant, at the punishment individualization and at the application of the qualified corpus under Art. 319b, Para. 2 of CC.

By the amendments from April 2007, the text of Art. 319b, Para. 1 of CC has been made precise from terminological point of view, as the term "computer" used in the old version, for which there was not a legal definition, has been substituted by the legally defined term "computer system".[45]

From an objective point of view, it is very important that the case is not insignificant. In accordance with Art. 93, Line 9 of CC, an insignificant case is a case the commitment of which either with a view of the insignificance of the harmful effects, or with a view of other extenuating circumstances, has a lower level of public danger compared to the usual cases of crime of such a type. Whether the case is insignificant is subject to the court's assessment in each concrete case.

The subject of the crime can be each criminally liable person except for the persons administrating or using the computer system. From a subjective point of view, the crime is deliberate. The perpetrator is aware that he or she does not have the required permission but nevertheless adds, changes, deletes or formats the programme or data.

The punishment provided under the main corpus is imprisonment for up to one year or a fine up to 2 000 BGN.[46]

2.4.2. Qualified Corpora Delicti

The Criminal Code provides for several qualified *corpora delicti* in Article 319 "b", Paragraph 1 of the Criminal Code. The qualifying circumstances are the criminal result (infliction of considerable damages or occurrence of other grave consequences), the criminal purpose (self-interested purpose or frustration of the execution of an obligation) and the object of the crime (information given by virtue of a law electronically or on a magnetic, electronic, optical or other medium).

2.4.2.1. Qualified corpora delicti in relation to the criminal result

[45] There was an analogous proposal as early as in the Criminal Code Amendment Bill, introduced in January 2005, which has not been adopted due to expiry of the Parliament's term.

[46] In the Criminal Code Amendment Bill, introduced in March 2006, it was proposed the fine to be substituted by a probation, but due to the withdrawal of the Bill by the mover, the punishment has not been amended.

The criminal result is a qualifying circumstance as per Article 319 "b", Paragraph 1 of the Criminal Code. The law indicates two possible results – infliction of considerable damages or occurrence of other grave consequences. The stipulated graver punishment is imprisonment for up to two years and a penalty of up to BGN 3000.[47]

According to case law, the considerable damages cover only the property damages. They constitute the reduction of the property (reduction of the assets or increase of the liabilities) of a certain person. There are two criteria to determine whether the damages are ordinary or considerable – the absolute value of the damage and its relative value compared to the value of the whole property. According to case law, if the relative value of the damage is significant and in its absolute value it is insignificant, there shall be no considerable damage within the meaning of the law. And when the absolute value of the damage is significant, but compared to the value of the damaged patrimonium it is insignificant, there shall be a considerable damage.[48] Considerable property damages means mainly that the damages are such in their absolute value, i.e. cash equivalent of the caused damages is significant.[49]

As for the occurrence of other grave consequences, they shall be interpreted as infliction of non-material damages, since the material damages are covered by the term considerable damages. When these consequences are grave is a factual matter and shall be subject to assessment by the court on a case by case basis.

The two possible results are indicated alternatively.[50] In any case, it is necessary to have a cause-effect relationship between the criminal result and the executive act.

2.4.2.2. Qualified corpora delicti in relation to the object of the crime

[47] The Criminal Code Amendment Bill put forward in March 2006 proposed that the maximum amount of the penalty be dropped out, but eventually the penalty was not modified.

[48] See Interpretative Ruling № 6 dated 15.11.1973 of the General Part of the Criminal Code as per interpretative criminal case № 2 dated 1973

[49] See Interpretative Ruling № 2 dated 09.08.1993 of the General Part of the Criminal Code as per interpretative criminal case № 2 dated 1993

[50] The preliminary variant of the Criminal Code Amendment Bill put forward in August 2006 proposed that the two results – infliction of considerable damages or occurrence of other grave consequences – be united under the common wording "infliction of considerable grave consequences". The proposal was dropped out during the discussion of the draft in the Parliament, even though its eventual approval would have eliminated the groundless division of property and non-property consequences and made the editing of the provision more precise.

The object of the crime is a qualifying consequence as per Article 319 "c", Paragraph 1 of the Criminal Code and is determined as information, which is given by virtue of the law electronically or on a magnetic, electronic, optical or other medium. The stipulated graver punishment is imprisonment for up to two years and a penalty of up to BGN 3000.[51]

From an objective point of view, it is sufficient for an explicit legal provision to stipulate an obligation for presentation of specific information, as well as a possibility for this information to be presented electronically or on a magnetic, electronic, optical or other carrier. The applicable field of the provision covers two groups of cases. First, there are the hypotheses, in which the law stipulates an obligation that the information be presented only electronically or on a special medium. Second, there are cases when the law stipulates an obligation that the information be presented and a possibility for this to happen electronically or on such a carrier (as an alternative to presentation on paper). The interpretation of the provision in the sense that the information is presented only in an electronic form or on a special medium would groundlessly narrow its applicable field.

For the interpretation of the term "electronically" the existing legal definitions in other laws may be used. According to § 1, Item 1 of the Supplementary Provisions to the Trade Register Act (TRA), a transmission "electronically" is a transmission of information in a digital form using devices for electronic processing, including digital compression and storage of the information, where the transmission is implemented using a lead, radio waves, optical, electromagnetic or other means. According to § 1, Item 20 of the Supplementary Provisions to the Social Insurance Procedure Code (SIPC), „electronic transmission" is a transmission through electronic equipment for processing (including digital compression) of information and using a cable, radio broadcasting, optical technologies or any other electromagnetic means. In practice, the presentation of information electronically may include various hypotheses such as sending by e-mail, presenting on the Internet, using a fax modem, etc.

As for the various types of carriers, the list in Article 319 "c", Paragraph 1 of the Criminal Code is exemplary and not exhaustive. Three types of carriers are indicated (magnetic, electronic and

[51] The Criminal Code Amendment Bill put forward in March 2006 proposed that the maximum amount of the penalty be dropped out, but due to the withdrawal of the draft this proposal was not elaborated upon.

optical) and it is explicitly added that the provision will also apply to information presented on other media.

The only legal definition of the term "electronic medium" in Bulgarian legislation is in § 1, Item 5 of the Supplementary Provisions to the National Standardization Act (NSA), according to which an "electronic carrier" is a technical device, which stores or transmits information in a digital form.

The magnetic carriers may be floppy magnetic disks (diskettes), hard drives, magnetic tapes, etc. The common thing between them is the fact that the carrier of the information is a thin surface and the reading of the information is done using the physical properties of the electromagnetic effect. In order for them to be used, the magnetic carriers must be placed in a special device for writing and/or reading, which is equipped with the respective magnetic head.

The optical carriers usually come in the form of optical discs. They are characterized by the fact that they have a special surface and the writing and reading of information is done using a laser or other high-frequency beam. Compared to the magnetic carriers, the optical carriers have a larger storage capacity for information and are more reliable, on account of which they are becoming more and more widespread.

In determining the various types of carriers, the provision of Article 319 "c", Paragraph 1 of the Criminal Code is not precise, since it mixes different categories of terms. The term "electronic carrier" is a generic term and includes the specific terms "magnetic medium" and "optical medium". The misunderstanding is a result of the change in the text of Article 319 "c", Paragraph 1 of the Criminal Code implemented with the amendments to the Criminal Code in August 2007. The old version of the text used only the term "magnetic term" and was harshly criticized due to the groundless narrowing of its applicable field and the exclusion of the other types of media, including the optical ones.[52]

[52] The preliminary variant of the Criminal Code Amendment Bill put forward in August 2006 stipulated only a replacement of the term "magnetic carrier" with "electronic carrier" but during the discussion of the changes in the Parliament it was decided to add optical and electronic carriers to magnetic carriers and to expand the applicable field of the provision even more by adding "other" carriers. An analogous proposal was also contained in the Criminal Code Amendment Bill put forward in January 2005 but it was not approved since the Parliament could not vote on the draft due to the expiration of its mandate. For a detailed analysis of the previous variant of the provision, including proposals for its specification, see Markov, D., *Legal framework of computer crimes as per the Bulgarian criminal law*, in: *Electronic document and electronic signature. Legal treatment*. Publisher: Siela. Sofia, 2004, page 389.

Even with specific weaknesses from a terminological point of view, the so changed provision is relatively clear and in contrast to the old editing its applicable field adequately complies with the actual public relations, which it concerns. Nevertheless, in order for it to be entirely precise, it should contain only the generic term "electronic carrier", which is technologically neutral and includes not only known carriers (including magnetic and optical), but also all new types of media, which could be invented in the future.

Article 319 "c", Paragraph 1 of the Criminal Code does not contain limitations regarding the matter who presents the respective information and to whom it is presented. In particular, there is no requirement that this information be presented by or to a state body. From an objective point of view, it is sufficient to have a legal provision regulating an obligation for presentation of specific information.

At present, several laws stipulate a possibility for presentation of information electronically or on an electronic medium. Such possibility is stipulated in the tax legislation. SIPC gives a possibility to submit electronically requests for issuing documents, which are of significance to recognizing, exercising or lapsing of rights and obligations (Article 89, Paragraph 2 of SIPC), and of declarations and other documents and information subject to submission (Article 99, Paragraph 1 of SIPC). According to the Value Added Tax Act (VATA) the applications for registration (Article 101, Paragraph 3 of VATA) may be submitted electronically and the references-declarations, the VIES-declarations and the accounting registers may be submitted electronically (Article 125, Paragraph 7 of VATA), as well as on a magnetic or optical medium (Article 125, Paragraph 6 of VATA).

The customs legislation also stipulates a possibility for submission of information electronically. The Customs Act (CA) stipulates that the submission of declarations to the customs authorities may be implemented electronically (Article 67, Paragraph 1, Item 2 of CA), and the Rules of Application of the Customs Act (RACA) regulate the conditions and the order for such submission of declarations (Article 134 – 136 "a" of RACA).

The laws regulating the right of access to information also stipulate that information may be presented electronically or on an electronic medium. The Public Information Access Act

(PIAA) gives a possibility for submission of applications for granting of access to public information electronically (Article 24, Paragraph 2 of PIAA) and for receiving such information in the form of a copy on a technical carrier (Article 26, Paragraph 1, Item 4 of PIAA). The Personal Information Protection Act (PIPA) also stipulates a possibility for submission of applications for granting of access to personal information electronically (Article 29, Paragraph 2 of PIPA) and for presentation of the information itself also electronically (Article 31, Paragraph 2 of PIPA).

Other laws, which stipulate a possibility of presentation of information electronically, are the Health Insurance Act (HIA) inn the part dealing with the obligation of the executors of medical assistance to present to the regional health-insurance funds specific information and documentation only on an electronic or magnetic medium in a form agreed with the National Health-Insurance Fund (Article 66, Paragraph 3 of HIA), the Audit Office Act (AOA) regarding the right of the bodies of the Audit Office to require references and other information on an electronic carrier in relation to the preliminary investigations or audits performed by them (Article 31, Paragraph 1, Item 2 of AOA), etc.

2.4.2.3. Qualified corpora delicti in relation to the special purpose of the perpetrator

The Criminal Code stipulates two qualified *corpora delicti* with a view to the special purpose of the perpetrator – when the crime is performed with the purpose of material benefit (Article 319 "b", Paragraph 3 of the Criminal Code) and when it is performed with the purpose to frustrate the execution of an obligation (Article 319 "c", Paragraph 2 of the Criminal Code).

Article 319 "b", Paragraph 3 of the Criminal Code indicates the special purpose of the perpetrator as a property benefit and the stipulated punishment is imprisonment from one to three years and a penalty of up to BGN 5000.[53] This is the so-called "self-interest purpose". The perpetrator seeks to achieve favorable changes in its property or in the property of a third party. The actual achievement of the purpose is of no significance for the indictability of the act, but it would be assessed upon the individualization of the punishment.

[53] The Criminal Code Amendment Bill put forward in March 2006 proposed that the minimum time for imprisonment and the maximum amount of the penalty be dropped out but the proposal was not elaborated upon due to the withdrawal of the draft.

In Article 319 "c", Paragraph 2 of the Criminal Code the special purpose of the perpetrator is expressed as frustration of the execution of an obligation and the stipulated punishment is imprisonment for up to three years and a penalty of up to BGN 5000.[54]

The text of Article 319 "c", Paragraph 2 of the Criminal Code applies only in relation to acts under Article 319 "c", Paragraph 1 of the Criminal Code, i.e. it is necessary for the special object of the crime to be cumulatively available – information, which is presented by virtue of a law electronically or on a magnetic, electronic, optical or other medium. Usually this is information, the presentation of which is related to the origination of an obligation for a specific person. For example – the references and the declarations under the tax and customs legislation, which are a prerequisite for the origination of specific tax or customs obligations.

Frustration means creation of obstacles for the execution of the obligation. It is not necessary for the perpetrator to be a debtor under the obligation, the execution of which he/she strives to frustrate.[55] The type and the amount of the obligation are of no significance. The qualifying circumstance is only the intent of the perpetrator to frustrate the execution of the obligation. The realization of this purpose is of no significance to the indictability of the act. The actual frustration of the execution of the obligation, however, may be assessed by the court when deciding on the punishment.

2.5. Introduction of Computer Viruses and Other Malicious Programmes

Article 319 "d". (1) Whoever introduces a computer virus in a computer system or a computer network shall be punished with a penalty of up to three thousand leva.

(2) The punishment under Paragraph 1 shall also be imposed on the one who introduces some other computer program, which is designed to disrupt the activity of the computer system or the computer network or to gather, obliterate, delete, change or copy computer data without permission, when such permission is required, as far as the performed act does not constitute a graver crime.

(3) If the act under Paragraph 1 results in the occurrence of considerable damages or if it is performed again, the punishment is imprisonment for up to three years and a penalty of up to a thousand leva.

[54] The Criminal Code Amendment Bill put forward in March 2006 proposed that the maximum amount of the penalty be dropped out but due to the withdrawal of the draft it was preserved.

[55] Also see Kopcheva, M., *Computer crimes*. Publisher Sibi. Sofia, 2006, page 95. According to the author, the obligation is foreign, i.e. it does not pertain to the perpetrator of the crime.

2.5.1. Main Corpora Delicti

Article 319 "d" of the Criminal Code establishes two main *corpora delicti*, which differ in the means of committing the crime – a computer virus under Article 319 "d", Paragraph 1 of the Criminal Code and a computer program, which is designed to disrupt the activity of a computer system or a computer network or to gather, obliterate, delete, change or copy computer data without permission, when such permission is required, Article 319 "d", Paragraph 2 of the Criminal Code.

The immediate object of the crime are the social relations securing a normal functioning of computer systems and networks and the privacy of computer data.

From an objective point of view, the crime is characterized by a special *corpus delicti*. The first case is about a computer virus within the meaning of Article 93, Item 27 of the Criminal Code.[56] In the second case, the means of the crime is defined as a computer program, which is designed to disrupt the activity of a computer system or a computer network or to gather, obliterate, delete, change or copy computer data without permission, when such permission is required. In the specialized literature these programs are also known as "malicious programs".

The introduction of a malicious program, which is not a virus, in a computer system or network, was criminalized with the amendments of the Criminal Code of April 2007. The new text of Article 319 "d" , Paragraph 2 of the Criminal Code comes as a response to the criticism regarding the former legal framework, which excluded from its applicable field the various harmful or malicious programs that are not computer viruses. The reasons for the proposed amendments even indicated that compared to the introduction of computer viruses, the introduction of other malicious programs presents "the same, even a higher level of public hazard".[57]

---

[56] For a more detailed definition of the term "computer virus" see the analysis of Article 93, Item 27 of CC (Item 2.7 above).

[57] The Criminal Code Amendment Bill put forward in January 2005 attempted to incriminate the introduction of malicious programs, but the Parliament did not vote on it. The draft proposed to replace the term "computer virus" with the more detailed "harmful program product (software) with the purpose to be used for disruption of computer information data or the activity of a computer information system". The Criminal Code Amendment Bill put forward in August 2006 had a different approach and proposed that the original text of Article 319 "d", paragraph 1 of CC be supplemented by adding to computer viruses as a means for the crime "other computer program with the purpose of disrupting the activity or implementing (or performing) an illegal effect on a computer system or a computer network or with the purpose of illegal gathering, obliteration, deletion, changing or copying of computer data". Eventually the legislator approved a different ruling and incriminated the introduction of a malicious program as an individual main corpus delicti.

Article 319 “d” , Paragraph 2 of the Criminal Code mentions a computer program, which is designed to disrupt the activity of a computer system or a computer network or to gather, obliterate, delete, change or copy computer data without permission, when such permission is required. In particular, these are programs, which are not distributed automatically (they are not self-replicating). All programs, which are distributed automatically and have the indicated designation, fall within the scope of the definition of a computer virus under Article 93, Item 27 of the Criminal Code and their introduction will be qualified as introduction of a computer virus under Article 319 “d” , Paragraph 1 of the Criminal Code.

The purpose of a malicious computer program is formulated as a “violation of the operation of a computer system or a computer network” or “gathering, obliterating, deleting, changing or copying of computer data without permission, when such permission is required”. The violation of the activity of a computer system or a computer network means a negative change in the functioning of the system or the network such as slowing down of the speed, discontinuation of one or more programs and so on. Gathering of computer data without permission is when a person gets access to specific data, to which he/she has no access. Obliteration is the complete removal of specific data from the computer system or network. Deletion is the destruction of the information indicating the location of the data. Compared to obliterated data, deleted data can be restored in some cases. Changing computer data means introduction of a change in already existing data. Copying is related to the creation of one or more copies of the data.

There are many and various malicious programs, also known as malware. For example, the various types of spyware gathering information on the user of a computer system (for example, searching habits, visited sites and others), showing unwanted advertisements, changing the contents of the browser, redirecting the results of the search to paid announcements and others. One other malicious program is the so-called logger, which copies each pressing of a button when typing in passwords, numbers of credit cards, registration codes of program products, passwords, etc. Yet another malicious program is the so-called dialer – an application, which controls the modem of a computer and using it dials telephone numbers of services with added value. Some of the most widespread malicious programs are to so-called Trojan horses, which ask the user to install them, but at the same time they have hazardous contents and can

immediately affect the system and lead to unwanted consequences, including installation of other malicious products.

The executive act is defined in the law as "introduction".[58] Introduction constitutes incorporation of the virus or other malicious program in a specific computer system or network. With the amendments from April 2007 the text of Article 319 "d" , Paragraph 1 of the Criminal Code was specified from a terminological point of view and the terms "computer" and "information network" used in the old editing, for which there were no legal definitions, were replaced by "computer system" and "computer network", respectively, which are legally defined.[59]

The introduction of the virus can happen in all manners, in which computer data can be introduced into the computer – from direct introduction through the peripheral devices of the system (the devices for reading of information stored on external drives) to remote introduction (through e-mail, chat, instant messaging programs and even SMS). The law does not require for the virus to be introduced in foreign system or network. Such a decision is well-grounded, because due to the specific properties of computer viruses often their introduction in any computer creates a serious hazard of their distribution in other computers and networks.

The crime has an outcome. The result is the presence of the virus or the malicious program in a specific computer system or network.[60]

In contrast to Article 319 "d", Paragraph 1 of the Criminal Code, penalizing the introduction of a computer virus, Article 319 "d" , Paragraph 2 of the Criminal Code, concerning other malicious programs, is of subsidiary nature and applies only if the act does not constitute a grave crime. For example, if using the introduced program the perpetrator has copied electronic

[58] When the provision of Article 319 "d" of CC was accepted in 2002 the original variant of the draft stipulated criminal liability for a broader scope of acts related to the distribution of computer viruses, including for their creation. The broadening of the scope of executive acts was also proposed in the Criminal Code Amendment Bills put forward in January 2005 and August 2006. Both bills stipulated the addition of the acts creation, transmission and distribution. Eventually introduction remained the only form of the executive act in the law. However, when the computer virus or other malicious program is created by one person and is introduced in the computer system or network by another person, the creator of the virus will bear criminal responsibility as an accomplice (accessory).

[59] For a detailed analysis of the former variant of the provision, including proposals for its specification, see Markov, D., *Legal framework of computer crimes as per the Bulgarian criminal law*, in: *Electronic document and electronic signature. Legal treatment*. Publisher: Siela. Sofia, 2004, page 392.

[60] See Doncheva, D., *Computer crimes under chapter 9 "a" of the Criminal Code*, Legal reflection, book 2, 2003. The crime is completed when the virus reaches a specific computer or information network, regardless of whether it is activated or neutralized by a special antivirus program.

signature creation data or information constituting a state secret, the act will be qualified under Article 319 "a", Paragraph 3 of the Criminal Code or Article 319 "a", Paragraph 4 of the Criminal Code, respectively.

The subject of the crime under both main *corpora delicti* may be any person liable under criminal law. From a subjective point of view there is malice. The perpetrator aims to introduce the computer virus or other malicious program in a specific computer system of network. Guilt as an element from the subjective point of view of the crime is of great significance to the introduction of computer viruses due to the specific nature of these programs to self-replicate. Indictable shall be only that act, during which the perpetrator is aware that the instructions he/she is introducing into a computer constitute a computer virus and nevertheless he/she aims to introduce it. There will be no crime if the person is not aware that the program or the data to be introduced into the computer contain a virus or some other malicious program. The same applies to the cases when due to the activation of the virus the system automatically introduces the virus in other computer systems or networks or sends it by e-mail.

The punishment stipulated by the Criminal Code for the introduction of a computer virus or some other malicious program is a penalty of an amount of up to BGN 3000.

2.5.2. Qualified Corpora Delicti

Article 319 "d" , Paragraph 3 of the Criminal Code envisages two qualified *corpora delicti* of the introduction of a computer virus or some other malicious program. In the first case, the act is qualified with a view to the objective point of view, where the qualifying indication is the criminal result indicated in the law as the occurrence of considerable damages.[61] The exclusion of the occurrence of other grave consequences from the criminal result is an omission of the legislator. Thus the non-material damages are groundlessly excluded from the qualifying circumstances.

In the second case, the act is qualified when it is performed repeatedly. The special quality of the subject of the crime is the qualifying circumstance. Within the meaning of Article 28,

[61] See more detailed information on the infliction of considerable damages in the analysis of Article 319 "b", Paragraph 2 of CC (Item 4.2.1 above).

Paragraph 1 of the Criminal Code, the crime is performed repeatedly if the perpetrator has performed it after being sentenced with an effective verdict for such a crime. Considering the case la, according to which similar in type crimes are "those, which implement the same or different corpora delicti of the same crime, including when it is qualified or privileged", repeatability will also be present when the perpetrator introduces a computer virus after being sentenced with an effective verdict for introducing other malicious computer program and vice versa.[62]

Under both qualified *corpora delicti*, the stipulated punishment is imprisonment for up to three years and a penalty of up to BGN 1000.

2.6. Distribution of Passwords and Passcodes to Computer Systems or Data

Article 319 "e". (1) Whoever distributes passwords or passcodes to a computer system or computer data and this results in the disclosing of personal data or information constituting a state secret or other secret protected by the law shall be punished by imprisonment for up to one year.
(2) For an act under Paragraph 1, performed with a self-interest purpose or if considerable damages have been inflicted or other grave consequences have occurred with it, the punishment if imprisonment for up to three years.

2.6.1. Main Corpus Delicti

The immediate object of the crime are the social relations providing the confidentiality and privacy of information in electronic form constituting personal data or a secret protected by the law.

From an objective point of view, the crime is characterized by a special object – passwords or passcodes to a computer system or data. With the amendments of April 2007, the provision of Article 319 "e", Paragraph 1 of the Criminal Code was changed from a terminological point of view. According to the old wording, the object of the crime was defined as "computer or system passwords".[63]

[62] See more detailed information on the acts performed under the conditions of repeatability in the analysis of Article 319 "a", Paragraph 3 of CC (Item 3.2.1 above).
[63] The Criminal Code Amendment Bill put forward in January 2005 proposed a change in Article 319 "e", Paragraph 1 of CC, which stipulated that the object of the crime be changed from "computer of system passwords" to "passwords for

A password is a sequence of symbols allowing a specific user to have access to a specific computer system or data. A passcode is also a sequence of symbols, which the user types in to gain access to a specific computer system or data. Since there are no legal definitions of the terms "password" and "passcode" in the law, it is difficult to determine the difference between them. In the specialized literature the most common standpoint is that the passcode consists only of numbers, while the passwords may include various symbols (letters, numbers, signs and so on).

Passwords and passcodes are the most commonly found means of protection of computer systems and data against illegal access. They are utilized for authentication of various users using the same computer system or network at the same time or consecutively. Passwords and passcodes are used to provide access for users to e-mail, online communication means (ICQ, Skype), Internet sites for electronic trading, electronic databases, etc. A password or passcode may also protect computer data sent between two computer systems, stored on an external drive or in a computer, which various users have access to.

From an objective point of view, the executive act of the crime is the distribution. Distribution means bringing specific information, in this case the respective passwords or passcodes, to the attention of third parties. The executive act may be performed only by an action. The passwords can be distributed electronically, as well as in other manners, including on paper. Whether the distribution has been performed gratuitously or against payment is of no significance to the indictability of the act.[64]

From an objective point of view, the crime is resulting. The result is indicated as disclosure of personal data or information constituting a state secret or some other secret protected by the law.[65] The disclosure of other secrets protected by the law was added with the amendments to

---

access to a computer information system or computer information data". For a detailed analysis of the former variant of the provision, including proposals for its specification, see Markov, D., *Legal framework of computer crimes as per the Bulgarian criminal law*, in: *Electronic document and electronic signature. Legal treatment*. Publisher: Siela. Sofia, 2004 , page, page 394-395.

[64] Also see Kopcheva, M., *Computer crimes*. Publisher Sibi. Sofia, 2006, page 64. According to the author Article 319 "e", Paragraph 1 of CC applies only to the gratuitous distribution since the law stipulates a qualified corpus delicti when the act has been performed with a self-interest objective (Article 319 "e", Paragraph 2 of CC). However, it is possible that the perpetrator has received some kind of benefit without having a self-interest objective in the moment of performing the act, or that he/she has had the objective to gain some kind of benefit and that objective has been realized.

[65] The Criminal Code Amendment Bill put forward in March 2006 proposed that the act be indictable even when it cannot lead to disclosure of personal information of a state secret. The draft was withdrawn and the proposal was not elaborated

the Criminal Code from April 2007. Before the changes the criminal result under Article 319 "e", Paragraph 1 of the Criminal Code included only the personal data and the state secret.[66]

Disclosure means bringing specific information to the attention of a person or persons who have no right of access to such information.

Personal information is defined in PIPA, which also regulates the rules of operation of such information and the order for access to it. According to Article 2, Paragraph 1 of PIPA, personal information is any information concerning a natural person who is identified or can be identified directly or indirectly through an identification number or through one or more specific indicators. According to the Bulgarian Identity Documents Act (BIDA), personal information is the name, birth date, unified civil number (or personal number of a foreigner), sex and nationality of the person (Article 16, Paragraph 1 of BIDA).

The other types of information included in the criminal result are those constituting a state secret or some other secret protected by the law.[67]

In order for an indictable act under Article 319 "e", Paragraph 1 of the Criminal Code to be present, there must be a causal relationship between the executive act and the criminal result. The causal relationship is also an element of the objective point of view of the crime and means that the disclosure of personal data or information constituting a state secret or some other secret protected by the law must be a direct and immediate consequence of the distribution of the passwords or passcodes.

Any person who can be criminally liable may be the subject of the crime. For the indictability of the act it is of no significance whether the perpetrator has known the respective passwords or codes legally. From a subjective point of view, there is a malice covering the executive act (distribution), as well as the criminal result (disclosure of personal data or information constituting a state secret or other secret protected by the law).

---

upon. The preservation of the variant, in which the crime is present only upon the actual disclosure of personal data or a secret protected by the law, is well-grounded since the proving of the potential possibility for disclosure would create difficulties in the practice.

[66] The addition of other secrets protected by the law was proposed in the Criminal Code Amendment Bill put forward in January 2005, but subsequently the Parliament did not vote on it.

[67] For detailed information constituting a state secret or other secret protected by the law see the analysis of Article 319 "a", Paragraph 4 of CC (Item 3.2.2 above).

The stipulated punishment under the main *corpus delicti* is imprisonment for up to one year.

2.6.2. Qualified Corpora Delicti

Article 319 "e", Paragraph 2 of the Criminal Code regulates two qualified *corpora delicti*. The first hypothesis is when the act has been performed with a self-interest purpose. This is a qualified *corpus delicti* with a view to the subjective point of view and the special purpose of the perpetrator is the qualifying circumstance. The act is performed with a self-interest purpose when the perpetrator desires to achieve property benefit for himself/herself or for somebody else though the act.[68]

The second hypothesis is when considerable damages have been inflicted or other grave consequences have occurred with the act.[69] The other grave consequences were added as a result from the crime with the amendments to the Criminal Code of April 2007. Thus the property damages, as well as the non-material damages constitute an indictable result. The change was necessary, since in many cases, in particular the disclosure of personal data, the inflicted damages may be of non-proprietary nature.[70]

2.7. Crimes Related to the Electronic Document and Electronic Signature Act

Article 319 "f". Whoever violates the provisions of Article 6, Paragraph 2, Item 5 of the Electronic Document and Electronic Signature Act upon provision of information services shall be punished with a penalty of up to five thousand leva, if he/she is not subject to a graver punishment.

The immediate object of the crime under Article 319 "f" of the Criminal Code are the social relations providing the normal sending, receiving, writing and recording of electronic announcements. These social relations are regulated in the Electronic Document and Electronic Signature Act (EDESA).

[68] For more detailed information on the self-interest objective see the analysis of Article 319 "b", Paragraph 3 of CC (Item 4.2.3 above).
[69] For more detailed information on the infliction of considerable damages and the occurrence of other grave consequences see the analysis of Article 319 "b", Paragraph 2 of CC (Item 4.2.1 above).
[70] The Criminal Code Amendment Bill put forward in August 2006 proposed that the property and non-property damages be united under the common wording "considerable grave consequences". During the discussion of the draft in the Parliament however it was decided that the two types of damages should be indicated alternatively.

The norm of Article 319 "f" of the Criminal Code is a blanket norm because it refers for one of the elements of the crime (the executive act) to another normative act – EDESA.

From an objective point of view, the executive act is expressed in the violation of the obligation to store the information for the time and the source of the transmitted electronic announcements for a term of two years. The term of two years was introduced with the Criminal Code Amendment Act adopted in April 2007. Before the change, this term was six months. The proposal for an increase of the term was reasoned with the argument that in this way it complies with the time needed to conduct investigations of the committed computer crimes.

The executive act may be performed through an action (destruction of the respective information), as well as through inaction (failure to undertake the necessary measures to protect the information). The crime is formal – it is sufficient to have the executive act performed.

The crime under Article 319 "f" of the Criminal Code is characterized by a special subject. This is a person in the capacity of a mediator upon the electronic announcement within the meaning of Article 6, Paragraph 1 of EDESA. The requirement for the subject to be in such capacity arises from the forwarding to the norm of Article 6, Paragraph 2, Item 5 of EDESA, which applies only in relation to the mediators upon electronic announcements. The term "mediator upon the electronic announcement" is legally defined in Article 6, Paragraph 1 of EDESA as a person that on assignment by the titular sends, receives, records or stores an electronic announcement or performs other services related to it.

Upon the definition of the subject of the crime under Article 319 "f" of the Criminal Code it should be taken into consideration that the main criminal-legal principle that criminal responsibility is personal and only natural persons can bear criminal responsibility. Therefore the subject of the crime under Article 319 "f" of the Criminal Code will be the mediator – a natural person. When the mediator upon the electronic announcement is a legal entity (for example internet service provider) the subject of the crime will be the natural person – the employee of the provider who according to the internal rules is responsible for the storing of the indicated information.

From an objective point of view, the law requires the executive act to be performed upon the delivery of information services. The Criminal Code does not give a legal definition to the activity of delivering information services. Upon the adoption of the text in 2002, one of the original variants of the draft stipulated a legal definition of the term "providing information services" (any person who processes or stores computer data in favor of services making it possible to communicate through a computer system), which, however, was not approved. The contents of the activity on delivering information services can be defined on the grounds of the legal definition of the term "computer and information services provider" given in Article 93, Item 23 of the Criminal Code. Within the meaning of this definition, the delivery of information services will constitute offering the possibility to communicate through a computer system or processing or storing of computer data for this communication service or for its users.[71]

The requirement for the executive act to be implemented upon delivery of information services is redundant. For the indictability of the act it is sufficient for the person to be in the capacity of a middleman at the time of the electronic communication and not to have executed the obligation to store the indicated information within the term determined by the law.[72]

From a subjective point of view, the crime is deliberate. The perpetrator is aware that he/she is bound to store the indicated information for the specified term, but nevertheless he/she violates this obligation.

The provision of Article 319 "f" of the Criminal Code is of subsidiary nature. It applies only in cases when the perpetrator is not subject to a graver punishment.

The stipulated punishment is a penalty of up to BGN 5000. Besides that, Article 6, Paragraph 3 of EDESA also stipulates liability for damages resulting from the non-execution of the obligation to store information.[73]

[71] For more detailed information on the term "computer and information services provider" see the analysis of Article 93, Paragraph 23 of CC (item 2.4 above).
[72] The Criminal Code Amendment Bill put forward in January 2005 proposed that the expression "upon delivery of information services" be dropped out, but the draft was not voted on in a plenary hall.
[73] The Criminal Code Amendment Bills put forward in March and August 2006 proposed that Article 319 "f" of CC be dropped out due to the "lack of public hazard imposing the criminalization of the guilty non-execution of obligations on

2.8. Computer Fraud

Article 212 "a". (1) Whoever rises or maintains a deceit in relation to a given person with the purpose of gaining benefits for himself/herself or for somebody else by introducing, changing, deleting or obliterating computer data or using foreign electronic signature and thus inflicts damages to this person or to somebody else shall be punished for computer fraud by imprisonment for one to six years and a penalty of up to six thousand leva.
(2) The same punishment shall be imposed on the one who introduces, changes, deletes or obliterates computer data without having the right to do so, in order to gain something, which he/she should not possess.

2.8.1. Main Corpus Delicti under Article 212 "a", Paragraph 1 of the Criminal Code

Computer fraud is criminalized as a crime against property. Its systematic place is in Section Four "Fraud" of Chapter Five "Crimes against property" of the special part of the Criminal Code.

The immediate target of the crime on one hand are the public relations securing privacy and normal exercising of property rights and, on the other hand, those guaranteeing the security of computer data and providing the legal creation and use of electronic signatures.

From an objective point of view, computer fraud under Article 212 "a", Paragraph 1 of the Criminal Code is characterized by a special object of encroachment. This is computer data within the meaning of Article 93, Item 21 of the Criminal Code.[74] The text of the provision was detailed with the amendments to the Criminal Code of April 2007 and in both paragraphs the old term "computer information data" was replaced by the new "computer data". Computer data is also an object of the crime in the hypothesis of computer fraud through the use of foreign electronic signature, because electronic signature within the meaning of EDESA constitutes such data. The material media, on which the data is stored, can also be the object of computer fraud. These can be magnetic and optical discs, computer systems and other media.[75]

---

behalf of the mediators upon electronic announcements under Article 6, Paragraph 1, Item 5 of EDESA". Eventually, however, the text was preserved.

[74] For more detailed information on the term „computer data" see the analysis of Article 93, item 21 of CC (item 2.2 above).

[75] See Stoynov, Al., *Computer fraud*, Modern law, book 4, 2002. According to the author the object of computer fraud is also the person, influenced by the perpetrator, as well as the property in the factual possession of the deceived person.

The executive act of the crime includes two interconnected elements. The first element is indicated in the law as rising or maintaining a deceit in relation to some other person.[76] The deceit constitutes an false awareness of facts and circumstances of the objective reality. In the case of computer fraud, as well as in the case of ordinary fraud under Article 212 of the Criminal Code, these are facts and circumstances related in a specific manner to the legal action undertaken or not undertaken by the deceived person. The rising of a deceit constitutes an initial creation of incorrect awareness of specific facts and circumstances, while the maintaining of a deceit is expressed in the confirmation of incorrect awareness created without the participation of the perpetrator.

The second element of the executive act is indicated in the law as introducing, changing, deleting or obliterating computer data or use of foreign electronic signature.

The introduction, changing, deleting and obliteration of computer data are the same executive acts as in the criminal encroachments upon computer programs and data under Article 319 "b" of the Criminal Code, regardless of the terminological difference between the two provisions (Article 212, Paragraph 1 of the Criminal Code uses the terms „introduces", „amends" and „obliterates", while Article 319 "b", Paragraph 1 of the Criminal Code uses the terms „adds", „changes" and „destroys").[77]

A use of foreign electronic signature means a use of a specific electronic signature by any person other than its author. The use itself is expressed in the creation of a signature through the use of the data, to which, under Article 14 of EDESA, only the author can have access.[78]

---

[76] The Criminal Code Amendment Bill put forward in August 2006 proposed one more executive act as an alternative to the rising and maintaining of a deceit – causing of disruption in the functioning of the computer system. The proposal however did not receive enough support during the discussion in the Parliament and was not included in the text proposed for voting at second reading.

[77] For more detailed information on the executive acts see the analysis of Article 319 "b", Paragraph 1 of CC (item 4.1 above). The Criminal Code Amendment Bill put forward in January 2005 proposed that the executive acts "deletes or obliterates" in both paragraphs of Article 212 "a" of CC be changed to "removes or temporarily obliterates" but since the Parliament failed to vote on this draft the wording of the acts remained unchanged.

[78] The Criminal Code Amendment Bill put forward in January 2005 proposed that the use of foreign signature be dropped out as an executive act under the main corpus delicti of Article 212 "a", Paragraph 1 of CC. The Parliament however failed to vote on the draft and the proposal was not elaborated upon. The Criminal Code Amendment Bill put forward in August 2006 also proposed a similar change. It proposed that the use of foreign signature be replaced by use of foreign electronic signature creation data or foreign personal data without permission. During the discussion of the draft in the Parliament however this proposal was not approved and was dropped out from the variant of the text proposed for voting at second reading.

The second element of the executive act is a manner or means for implementation of the first element – rising or maintaining a deceit.

Computer fraud under Article 212 "a", Paragraph 1 of the Criminal Code is an effective crime. The criminal results are two – first, the result is the occurred change in the computer data and second – the occurrence of damages for the deceived person or some other person.[79]

Any criminally liable person may be the subject of computer fraud under Article 212 "a", Paragraph 1 of the Criminal Code. In the event of computer fraud through using foreign electronic signature, the author of the signature cannot be the subject of the crime, because to him/her the signature is not foreign.

From a subjective point of view, the crime is deliberate. The perpetrator performs an encroachment knowing that he/she rises or maintains a deceit in relation to the deceived person. Besides that, the law requires the presence of a special purpose. This is about a self-interest purpose – the perpetrator aims to achieve benefits for himself/herself or for somebody else.[80]

The stipulated punishment under the main *corpus delicti* of computer fraud under Article 212 "a", Paragraph 1 of the Criminal Code is imprisonment from one to six years and a penalty of up to BGN 6 000.[81]

2.8.2. Main Corpus Delicti under Article 212 "a", Paragraph 2 of the Criminal Code

Computer fraud under Article 212 "a", Paragraph 2 of the Criminal Code differs from the crime under Article 212 "a", Paragraph 1 of the Criminal Code in several ways.[82]

---

[79] See Stoynov, Al., *Computer fraud*, Modern law, book 4, 2002. According to the author the harm from computer fraud may be either only property, or a combination of property and moral damages.

[80] For more detailed information on self-interest objective see the analysis of Article 319 "b", Paragraph 3 of CC (item 4.2.3 above).

[81] The Criminal Code Amendment Bill put forward in March 2006 offered complete editing of Article 212 "a", Paragraph 1 of CC. It stipulated that the rising and maintaining of a deceit to be dropped out, that only introduction, changing, deleting and destroying (instead of obliterating) of computer data and the use of foreign electronic signature remain as executive acts, that there should be a clarification that the benefit and the occurred damages are "property", i.e. they are of property nature, and that the maximum amount of the penalty be dropped out. The draft however was withdrawn and the proposed changes were not realized.

First, there is a difference in the executive act. In Article 212 "a", Paragraph 2 of the Criminal Code, the executive act is indicated as an illegal introduction, changing, deleting or obliteration of computer data. There is no rising or maintaining of deceit in relation to some other person.

From an objective point of view, in the case of computer fraud under Article 212 "a", Paragraph 2 of the Criminal Code, the law explicitly requires the act in relation to the computer data to be performed without the perpetrator having the respective right to do so.

The crime under Article 212 "a", Paragraph 2 of the Criminal Code is also effective, but the result covers only the occurred change in the computer data. The indictability of the act does not depend on the occurrence of damages for the deceived person or for other persons.

The subject of the crime under Article 212 "a", Paragraph 2 of the Criminal Code may be any criminally liable person with the exception of the persons who have the right to perform the indicated actions towards the respective computer data.

From a subjective point of view, the crime under Article 212 "a", Paragraph 2 of the Criminal Code is also a deliberate crime, but it is characterized by a different purpose – achievement by the perpetrator of something, which he/she should not possess. If the perpetrator aims for a third party to achieve as a result of the act something, which that third party should not posses, the act will not be indictable underArticle 212 "a", Paragraph 2 of the Criminal Code.[83]

The stipulated punishment under the main *corpus delicti* of computer fraud under Article 212 "a", Paragraph 2 of the Criminal Code is the same as under Article 212 "a", Paragraph 1 of the Criminal Code – imprisonment for one to six years and a penalty of up to BGN 6 000.

2.9. Crimes against Intellectual Property

[82] For more detailed information on relations between corpora delicti see the analysis of Article 212 "a", Paragraphs 1 and 2 of CC, as well as on the relations between computer fraud and other types of fraud. Stoynov, *Computer fraud*, Modern law, book 4, 2002.

[83] The Criminal Code Amendment Bill put forward in March 200 stipulated that Article 212 "a", Paragraph 2 of CC be dropped out, but the provision was preserved.

Article 172 "a". (1) Whoever records, reproduces, disseminates, broadcasts or otherwise uses without the consent of the holder of the respective right required by law foreign object of copyright or similar right or copies of it shall be punished by imprisonment for up to five years and a penalty of up to five thousand leva.

(2) Whoever holds without the consent of the holder of the respective right required by law material carriers containing foreign object of copyright or similar right amounting to a large sum or holds a matrix for reproduction of such carriers shall be punished by imprisonment from two to five years and a penalty from two to five thousand leva.

(3) If the acts under Paragraphs 1 and 2 is performed repeatedly or have caused considerable harmful consequences, the penalty is imprisonment from one to six years and a penalty from three thousand leva to ten thousand leva.

(4) When the act under Paragraph 2 amounts to significantly large sums the punishment is imprisonment from two to eight years and a penalty from ten thousand leva to fifty thousand leva.

(5) For insignificant cases the perpetrator shall be punished according to the administrative order of the Copyright and Related Rights Act (CRRA).

(6) The object of the crime shall be confiscated in favor of the state regardless of whose property it is and shall be destroyed.

Infringements of intellectual property rights were incriminated for the first time in Bulgarian legislation with the amendments of the Criminal Code of 1995.[84] These texts remained almost unchanged until 2006, when with the consecutive changes to the Criminal Code, the legal framework of crimes against intellectual property was substantially changed.[85]

The crimes against intellectual property include various types of criminal acts, of which only a few are related to information technologies. Due to the rapid development of these technologies during the last few years, however, they gradually turned into the main object and means for committing crimes against intellectual property. At present, the main problem facing the protection of copyrights is namely the illegal distribution of objects of intellectual property using the modern information technologies.

The main provision related to the crimes against intellectual property, which can be defined as computer crimes, is Article 172 "a" of the Criminal Code.

[84] See the Criminal Code Amendment Act, published in State Gazette, issue 50, 1 June 1995.
[85] See the Criminal Code Amendment Act, approved by the Fortieth National Assembly on 30 August 2006, published in State Gazette, issue 5, 12 September 2006, in force since 13 October 2006.

2.9.1. Main Corpus Delicti under Article 172 "a", Paragraph 1 of the Criminal Code

Article 172 "a", Paragraph 1 of the Criminal Code incriminates the illegal use of foreign copyrighted materials or copies thereof.

The immediate target of this crime are the social relations existing around a normal implementation of copyright and related rights, as well as the conditions and order of exercising of those rights established by the state.

From an objective point of view, the object of the crime is defined as "an object of copyright or a related right, including copies thereof". Before the changes to the Criminal Code of 2006, two individual main *corpora delicti* existed with the same executive act (recording, reproducing, distribution, broadcasting or transmission using a technical device or use in any other manner without the consent of the holder of the respective right required by law) and the same sanction (imprisonment for up to three years and a penalty from BGN 1000 to BGN 3000), but with a different object. One of the main *corpora delicti* mentioned foreign work of science, literature or art, and the other – rights in a sound recording, video recording or radio broadcasting, television broadcasting, software of computer program. After the amendments were introduced, the two were united and the object of the crime was defined with the general term „foreign object of copyright or related right or a copy thereof". The same amendment increased the degree of the punishment, which is now imprisonment for up to five years and a penalty of up to BGN 5000.[86]

The objects of copyright are legally defined in CRRA. According to Article 3, Paragraph 1 of CRRA an object of copyright is any work of literature, art and science, which is a result of a creative activity and is expressed in any manner and any objective form whatsoever. In addition to the definition, as an example are given the most widespread objects of copyright, such as literary works, including works of scientific and technical literature, music and theatrical works, films, works of art and so on.

[86] The Criminal Code Amendment Bill put forward in August 2006 proposed that the copies of objects of copyright be dropped out as an individual object of the crime and that the punishments be reduced: imprisonment – to up to three years, and penalty – from BGN 1000 to BGN 3000. The proposal however was not approved.

According to Article 72 of CRRA, the rights related to the copyright include the rights of artists-performers over their plays, of the producers of sound records over their sound records, of the producers of the initial record of a movie or some other sound recording work over the original and the copies obtained as a result from this record, and of the radio and television organizations over their broadcasts.

A copy of an object of copyright is each individual piece of it. The copies include the originals of the respective object of copyright or related right, as well as their copies.

The object of the crime is characterized by the fact that it is about foreign object of copyright or related right, i.e. the perpetrator is not the holder of the respective right.

The copyright holders and the related rights are defined in detail in CRRA. In principle, the copyright holder is the author of the work. In specific cases determined by CRRA, other persons can be the copyright holders. For example, the copyright over a film or other audiovisual work belongs to the director, the script-writer and the cameraman, while the authors of the music, dialogue, of the already existing literary work, based on which the work has been created, the scenography, the costumes, as well as other works, included in it, retain their copyright over their own works.

As far as the related rights are concerned, their holders are the artists-performers (over their plays), the producers of sound records (over the sound records), the producers of the initial record of a film or any other audiovisual work (over the original and the copies obtained as a result of thas record), and radio and television organizations (over their broadcasts).

For all other persons, the respective work is foreign object of copyright or related right.

The executive act of the crime is extremely broad and several acts are described, which, according to the legislator, are the most common cases of such infringements (recording, reproduction, distribution, broadcasting and transmission) and any other use.[87]

[87] Upon the approval of the changes in CC it was discussed whether to add two more acts (importing and exporting) to the exemplary listing, but eventually this proposal was rejected.

Reproduction and distribution are legally allowed in CRRA. According to § 3 of the Supplemental Provisions of CRRA, „reproduction of a work" is the direct or indirect duplication in one or more copies of it in whatsoever manner and form, temporary or permanent, including its recording in a digital form on an electronic medium. According to § 4 of the Supplemental Provisions of CRRA, „distribution of a work" is the sale, exchange, granting, leasing, as well as storing in commercial quantities, and offer for sale or leasing of originals or copies of the work.

The legal definitions under CRRA can be used for clarification of the contents of the remaining executive acts of the crime under Article 172 "a", Paragraph 1 of the Criminal Code. Thus, for example, on the grounds of § 7 of the Supplemental Provisions of CRRA, which gives definition to the term "sound recording", the contents of the executive act recording can be defined as fixing on a permanent tangible medium of an object of copyright in a manner allowing for its perception, reproduction, consecutive recording, broadcasting wirelessly or through a cable or some other technical device.

The term „broadcasting of a work wirelessly", defined in § 5 of the Supplemental Provisions of CRRA, can be assumed as equal to the executive act of broadcasting, since before the last changes to the Criminal Code of 2006, Article 172 "a" of the Criminal Code was also mentioning the wireless broadcasting. The broadcasting covers each broadcasting on the radio or television using ground infrastructure, as well as its inclusion into a continuous communication network leading to a satellite and from there back to Earth through signals, carrying programs, under the control and responsibility of the broadcasting organization with a view to being received, whether directly and individually by the audience or indirectly by an organization other than the broadcasting one.

As far as the last indicated form of the executive act – transmitting – is concerned, its content is similar to that of broadcasting with the difference that instead of wirelessly it is implemented through a cable.[88]

[88] The Criminal Code Amendment Bill put forward in August 2006 proposed that the clarification "through a technical device" be added to the executive acts "broadcasting" and "transmitting", but the proposal was not approved.

Besides these explicitly indicated cases, the executive act of the crime under Article 172 "a", Paragraph 1 of the Criminal Code is also present upon each "use in any other manner" of the respective copyright. Thus the legislator is trying to cover as large a scope as possible in case of encroachments upon the objects of copyright and related rights. On one hand, this is justified by the rapid development of information technologies and the danger of the listed forms of the executive act to turn out to be insufficient for the sanctioning of all encroachments in this field hazardous to the public. On the other hand, however, the extremely broad scope of acts, which could be qualified as crimes under Article 172 "a", Paragraph 1 of the Criminal Code, can give rise to groundless strictness on behalf of the competent bodies in relation to violations, which do not present the level of public hazard necessary to engage in the grave procedure of the criminal process. In fact, the Criminal Code contains some limitations that only really grave cases of infringement of copyright and related rights will be prosecuted. Such limitations are like the general provision of Article 9, Paragraph 2 of the Criminal Code, according to which the act will not be qualified as a crime if it is insignificant, such is the provision of Article 172 "a", Paragraph 5 of the Criminal Code, stipulating the imposing of an administrative punishment for insignificant cases. Nevertheless, the broad wording of the executive act in practice leaves the assessment whether the perpetrator is subject to criminal liability entirely in the hands of the prosecutor's office and the court.

An important element of the objective point of view of the crime is the lack of the consent of the holder of the respective right required by law. The cases, in which this consent is required, the order for its obtaining and the term of its operation are regulated in detail in CRRA.

The subject of the crime is any criminally liable person with the exception of the holders of the copyright or related rights. From a subjective point of view, the crime is deliberate. The perpetrator is aware that he/she is not the holder of the copyright or related right over the respective object, as well as that he/she has not obtained the consent of the holder of the right.

The stipulated punishment for the acts under Article 172 "a", Paragraph 1 of the Criminal Code is imprisonment for up to five years and a penalty of up to BGN 5000.

2.9.2. Main Corpus Delicti under Article 172 "a", Paragraph 2 of the Criminal Code

Article 172 "a", Paragraph 2 of the Criminal Code incriminates the illegal holding of media containing foreign objects of copyright or related rights or a mould for reproduction of such media. Such acts were criminalized for the first time with the amendments to the Criminal Code of 2006.[89]

The immediate object of the crime, besides the social relations in the sphere of copyright and related rights and the conditions and order for exercising of those rights established by the state, are also the social relations related to the order of the production and distribution of the material objects containing objects of copyright and related rights, as well as of moulds for their reproduction.

The material objects containing objects of copyright and related rights and the moulds for reproduction of such carriers are also the object of the crime under Article 172 "a", Paragraph 2 of the Criminal Code. After these terms have been officially defined, one can use the legal definitions of the Law on the Administrative Regulation of the Production and Trading in Optical Discs, Moulds and Other Objects of Copyright and Related Rights adopted in 2005. According to the supplement provisions of this law, "other carriers" (besides the optical discs) are all permanent material media, in which objects of copyright and related rights are fixed, allowing for these objects to be brought to the attention of the public with the help of suitable means. "Optical discs" are media, on which information can be fixed or stored in a digital form, readable with the help of an optical mechanism using a laser or some other high-frequency light source, where this category includes CD, CD-DA, CD-I, CD-P, CD-ROM, CD-R, CD-RW, CD-WO, DVD, DVD-RAM, DVD-ROM, LD, MD, VCD, CVD, SVCD, SACD. In practice, there is a wide range of material media, which could contain objects of copyright or related rights. These include portable carriers, such as magnetic discs and diskettes, optical discs, external memory (flash memory), various types of memory cards for mobile phones and so on, as well as media, which are parts of other devices, such as the hard disk of the computer, the integrated memory of mobile phones, etc.

The Law on Administrative Regulation of the Production and Trading in Optical Discs, Moulds and Other Objects of Copyright and Related Rights defines the term "mould" as the

[89] The Criminal Code Amendment Bill put forward in August 2006 proposed that Article 172 "a", Paragraph 2 of CC be dropped out, but the proposal was rejected.

prototype of an optical disc containing information, from which a limited copies of optical discs can be produced using a special technology.

The executive act is indicated in the law as holding, which means exercising of factual possession of the respective material carriers or the moulds used for their reproduction.

From an objective point of view, it is necessary for the holding to be implemented with the lack of a consent required by law. In this part, the provision is not very precise, since it does not indicate who should give this consent. Article 172 "a", Paragraph 1 of the Criminal Code explicitly mentions the consent of the holder of the respective right. Under Paragraph 2, however, the holder of the copyright or related rights is not explicitly mentioned, which allows for a broader interpretation of the definition of consent.

In all cases, if the consent of the holder of the respective right required by law is missing, the act shall be qualified as a crime under Article 172 "a", Paragraph 2 of the Criminal Code. The disputable matter in this case is whether the provision of Article 172 "a", Paragraph 2 of the Criminal Code will be applicable, if some other consent required by law is missing.

The interpretation of this point of view is of significance, since the production and trading in optical discs, moulds and other media is the object of a special legal framework and is subject to various regimes (registration – in the case of reproduction of objects of copyright on optical discs and other carriers without recording, license – for the production of optical discs and matrixes, notifying – for the import and export of matrixes, raw materials and equipment for the production of optical discs and so on). In its present version, the provision of Article 172 "a", Paragraph 2 of the Criminal Code must also be applied in these cases, since in practice this is the case of holding of a material carrier or a matrix without obtaining the necessary consent of the competent state body. Similar interpretation, however, can create certain difficulties in the practice. In this way, for example, a license is necessary for the production of optical discs and moulds for their production. The lack of such license, therefore, could be accepted as a lack of the consent required by law. The import of discs and moulds, on the other hand, is subject to a notification regime, while in practice there is no act of the respective state body, which could be accepted as equivalent to consent. The only consequence of the notifying is the filing in a special register, which, however, could hardly be qualified as consent.

When the object of the crime is a material carrier, the law requires the presence of one more element from an objective point of view. This is the value of these carriers, which the Criminal Code determines as "value in large sums". According to case law, large sums are present when the cash equivalence of the object of the crime exceeds the minimum salary in the country seventy times.[90] As of 1 January 2008, the minimum salary in Bulgaria is BGN 220.[91] This means that in order to be in large sums, the value of the object of the crime must exceed the amount of BGN 15400.

The wording of the text brings us to the conclusion that only the value of the media must be taken into consideration for the qualification of the act, regardless of the information contained in them, and the value of some carriers (optical discs, diskettes) is extremely low. In this way, in order for a crime to be present, the perpetrator must be holding a considerable amount of such media. For example, if the object of the crime are optical discs, the court will take into consideration only the value of the discs disregarding their contents. Considering that the price of these discs is approximately BGN 0.5 per disc, the act will be qualified as a crime if there are 30000 discs containing foreign objects of copyright. The normal capacity of such optical disc, however, is 650 MB, which means that 30000 discs are equal to approximately 20 TB of information. In order for the law to be precise, it should also consider other indications for the qualification of the act as a crime, for example, the capacity of the information contained on the respective carriers, the market value of the respective object of copyright, the amount of the damages caused by the act (stipulated only as a qualifying circumstance under Article 172 "a", Paragraph 3 of the Criminal Code), and so on.

The subject of the crime is any criminally liable person with the exception of the holder of the copyright or related rights, to whom the object of the crime is not characterized as foreign object of copyright.

[90] See Interpretative Ruling № 1 dated 30.10.1998 of the General Part of the Criminal Code as per interpretative criminal case № 1/98.
[91] See Decree № 1 of the Council of Ministers dated 11.01.2008 for determination of the new amount of the minimum salary for the country, published in State Gazette, issue 6, 18 February 2008.

From a subjective point of view, there is a malice – the perpetrator is aware that he/she does not have the consent for the holding of the respective material medium or mould required by the law.[92]

The punishment stipulated for committing a crime under Article 172 "a", Paragraph 2 of the Criminal Code is imprisonment for two to five years and a penalty of BGN 2 000 to BGN 5 000.

2.9.3. Qualified Corpora Delicti

The qualified *corpora delicti* of the crimes against intellectual property are envisaged in Article 172 "a", Paragraphs 3 and 4 of the Criminal Code. The qualifying circumstances are the subject of the crime and the criminal result, and for the act under Article 172 "a", Paragraph 2 of the Criminal Code – the graveness of the act as well. After the changes of 2006, all qualified *corpora delicti* of the infringements of copyright and related rights are now grave crimes within the meaning of Article 93, Item 7 of the Criminal Code.

2.9.3.1. Qualified corpora delicti in relation to the subject

The Criminal Code stipulates only one qualified *corpus delicti* of the crimes under Article 172 "a", Paragraphs 1 and 2 of the Criminal Code from the point of view of the subject and that is the case when the act is performed repeatedly (Article 172 "a", Paragraph 3 of the Criminal Code).[93] The stipulated punishment is imprisonment for one to six years and a penalty of BGN 3000 to BGN 10000.

Repeatability will always be present when the perpetrator has committed a crime envisaged by one of the first two paragraphs of Article 172 "a" of the Criminal Code, after he/she has been sentenced with an effective verdict for some other crime under the same paragraph, regardless of the executive act. For example, if a person is sentenced with an effective verdict for illegal

[92] Upon the acceptance of the changes in CC it was discussed as an element of the subjective point of view of the crime under Article 172 "a", Paragraph 2 of CC whether to add a special objective of the perpetrator, defined as "commercial". Such an objective is not present in neither of the other provisions of CC and therefore was dropped out of the final variant of the changes accepted by the Parliament. For analysis and criticism of this proposal see E-Bulgaria 2006, Foundation "Applied Studies and Communications", Sofia, 2006, page 82.

[93] For more detailed information on the acts committed under conditions of repeatability see the analysis of Article 319 "a", Paragraph 3 of CC (item 3.2.1 above).

recording of foreign object of copyright and subsequently is accused of distribution of copies of such object, the act will be qualified as committed repeatedly.

However, the question arises whether this principle will apply to acts falling within the applicable field of the two different paragraphs. For example, if a person who has been sentenced for illegal recording is subsequently accused of holding a mould. The answer to this question depends most of all on case law and on whether it interprets Paragraphs 1 and 2 as „different *corpora delicti* of the same crime" or as *corpora delicti* of different crimes. In the first case, the person shall be liable under the qualified *corpus delicti* for repeatability, and in the second – under the main *corpus delicti*.

2.9.3.2. Qualified corpora delicti in relation to the criminal result

The crimes under Article 172 "a", Paragraphs 1 and 2 of the Criminal Code are more severely punishable (imprisonment from one to six years and a penalty from BGN 3000 to BGN 10000) when considerable harmful consequences have been caused by the act. The harmful consequences cover material and non-material damages. The consequences must be a direct and immediate result of the act. Whether they are considerable will be decided on a case by case basis by the court, which must take into consideration mainly the amount of the damages suffered by the holder of the respective copyright or related right.

2.9.3.3. Other qualified corpora delicti

With the amendment of the Criminal Code of 2006 one more qualified *corpus delicti* was added, only for the crime under Article 172 "a", Paragraph 2 of the Criminal Code. According to Article 172 "a", Paragraph 4 of the Criminal Code, the crime is more severely punishable (imprisonment from two to eight years and a penalty from BGN 10000 to BGN 15000) when "the act under Paragraph 2 is in considerably large sums". According to case law, considerably large sums are present when the cash equivalence of the object of the crime exceeds the established minimum salary one hundred and forty times.[94] With a minimum salary of BGN

[94] See Interpretative Ruling № 1 dated 30.10.1998 of the General Part of the Criminal Code as per interpretative criminal case № 1/98

220, this means that considerably large sums are present in case of a value of no less than BGN 30 800.

The wording of the text is not precise and may create difficulties when applied. It is evident that the act itself has no value, therefore there is no way it can be "in considerably large sums". Only its individual elements such as caused damages, benefits, the object, etc. can be in considerably large sums. If the text is interpreted only in relation to the main *corpus delicti* under Article 172 "a", Paragraph 2 of the Criminal Code, one can come to a conclusion that this is a matter of the value of the object of the crime. The main *corpus delicti* requires that the object of the crime when committed with material media amount to large sums. When these carriers are in considerably large sums, the act will be qualified as more severely punishable. It is logical that the same approach should be used when the object of the crime are moulds for reproduction of material media, regardless of the fact that under the main *corpus delicti* they are not required to amount to large sums. As far as the damages caused by the act are concerned, the question remains open and will be decided in case law. Therefore, it must be taken into consideration in the provision of Article 172 "a", Paragraph 3 of the Criminal Code, which stipulates a qualified *corpus delicti* in case of considerable harmful consequences. On one hand, this provision seems to eliminate the damages as a criterion for the qualification of the act as more severely punishable due to considerably large sums. On the other hand, the punishments under Article 172 "a", Paragraph 4 of the Criminal Code are considerably more severe than those under Article 172 "a", Paragraph 3 of the Criminal Code; and if we assume that "considerably large sums" exceeds "considerably harmful consequences", the application of Article 172, Paragraph 4 of the Criminal Code does not seem groundless.

Thus formulated, the text of Article 172 "a", Paragraph 4 of the Criminal Code does not exclude the consideration of other circumstances in determining the considerably large sums of the act, for example – the benefit obtained from the crime. In this category of crimes, the benefit in many cases is significant and may exceed the value of the object of the crime multiple times. For example, the profit from the sale of one optical disc with software in violation of the copyright is much larger than the value of the disc itself.

In all cases, the wording of Article 172 "a", Paragraph 4 of the Criminal Code must be specified, in order to avoid a contradictory judicial practice.

2.9.4. Insignificant Cases

According to Article 172 "a", Paragraph 5 of the Criminal Code, the perpetrator is punished for insignificant cases under the administrative order of CRRA. The administrative punishments stipulated in CRRA are penalties of BG 300 to BGN 5000.

According to Article 93, Item 9 of the Criminal Code, an insignificant case is such a case, in which the committed crime with a view to the lack or the insignificance of the harmful consequences or with a view to other mitigating circumstances constitutes a lower level of public hazard compared to the general cases of crime of the respective type. The decree stipulating an administrative punishment for the insignificant cases of intellectual property infringements is of significance considering the increasing number of cases of illigal distribution of objects of copyright or related rights through the Internet.[95] Many of these cases are about the exchange of certain works between a limited circle of persons, which can be effectively counteracted by means of administrative or criminal liability. In practice, it is impossible and unnecessary to sanction every single violation of copyrights or related rights using the slow, clumsy and expensive mechanism for realization of criminal liability. However, the question remains whether it is not more expedient to formulate the corpora delicti of the crimes against intellectual property more precisely so that they covered the really serious encroachments constituting a high level of public hazard and thus requiring a more severe sanction on behalf of the state. Under the present wording of the texts, the assessment of the insignificance of each act remains in the competence of the judicial bodies, which on one hand burdens them, but on the other hand can lead to groundless increase or decrease of the threshold for the insignificance of the act.

2.9.5. Confiscation of the Subject Matter of the Crime in Favour of the State

Article 172 "a", Paragraph 6 of the Criminal Code stipulates the confiscation in favor of the state and the destruction of the subject matter of the crime regardless of whose property it is.

[95] Despite the initial ideas, the amendments of CC 2006 did not affect the decree stipulating the imposing of administrative punishment for the insignificant cases of encroachment against copyrights and related rights. The preliminary variant of the draft approved at first reading stipulated that this text be dropped out. Such a change would have left as the only alternative to criminal liability the lack of criminal act due to its insignificance under Article 9, Paragraph 2 of CC. For criticism of such a change, see E-Bulgaria 2006, Foundation "Applied Studies and Communications", Sofia, 2006, page 83.

Before the amendments to the Criminal Code of 2006, the same Article stipulated that the subject matter of the crime shall be confiscated in favor of the state only when it belongs to the guilty perpetrator and was not explicit on the matter of destruction.

In its new wording, the decree brings up a few disputable questions regarding the confiscation in favor of the state, the most important of which concerns the scope of the term "subject matter of the crime".

As per Article 172 "a", Paragraph 1 of the Criminal Code, an object of the crime is foreign object of copyright or related right or a copy thereof. In order to be confiscated, that foreign object of copyright must be materialized in a certain medium. In practice, what can be confiscated is the carrier itself – magnetic or optical disc, diskette, magnetic tape and so on. The same applies to the copies of that foreign object of copyright.

Under Article 172 "a", Paragraph 2 of the Criminal Code, the subject matter of the crime are material media containing foreign object of copyright or related right, such as moulds for reproduction of such carriers. The material media may be various – optical discs, magnetic tapes, external memory and others. When a material medium is a part of a larger device, for example a hard disk of a computer or a memory card of a mobile phone, the medium itself must be subjected to confiscation, not the whole device. It is still disputable how to proceed when the material carrier cannot be physically separated from the respective carrier without damaging it. Such would be the case, for example, with some devices with integrated memory, such as mobile phones, MP3 players and others.

As far as the confiscation of moulds for reproduction of such media is concerned, the strict interpretation of the text of the law requires the confiscation in favor of the state only of the mould itself (the original of the optical disc), but not the technology for reproduction. The technology may be eventually confiscated in favor of the state by virtue of Article 53, Paragraph 1, Item "a" of the Criminal Code, if it belongs to the guilty perpetrator and has been designed or has served for the commitment of the crime. Other devices belonging to the guilty perpetrator, which have been designed or used for the commitment of the act (computers, servers, modems, printers and others), may also be confiscated on the same grounds.

It is disputable to what extent it is justified to confiscate and destroy the object of the crime, when it is not the property of the guilty perpetrator. This new addition of 2006 was met with contradictory reactions. On one hand, is understandable that the legislator strives to avoid subsequent encroachments with the use of the same instrument of crime, regardless of whose property it is. On the other hand, however, the non-precise definition of the object of the crime may lead to confiscation in favor of the state of belongings of significant value that do not belong to the perpetrator of the crime, which creates a hazard of unjustified impairment of the rights of third scrupulous parties.

The compulsory requirement for the object of the crime to be destroyed also brings up certain questions. A more expedient decision would be to obliterate foreign object of copyright from a material medium and to resort to the destruction of the medium itself only as a measure of last resort and if the obliteration is technically impossible. Such a decision was adopted with the changes to CRRA in 2005 for cases where the object of the crime are computer programs. Thus, according to § 1a, Paragraph 3 of the Supplementary Provisions of CRRA, obliteration from an electronic medium of a software when it is a subject matter of crime is recognized as confiscation in favor of the state.

2.10. Crimes Related to Pornographic Materials

Article 159. (1) Whoever creates, exposes, presents, broadcasts, offers, sells, rents or in any other manner disseminates pornographic materials shall be punished by imprisonment for up to one year and a penalty from one thousand to three thousand leva.

(2) Whoever disseminates pornographic materials through the Internet shall be punished by imprisonment for up to two years and a penalty from one thousand to three thousand leva.

(3) Whoever exposes, presents, offers, sells, rents or in any other manner disseminates pornographic materials of a person who has not reached 16 years of age shall be punished by imprisonment for up to three years and a penalty of up to five thousand leva.

(4) For the acts under Paragraphs 1 - 3 the punishment is imprisonment for up to six years and a penalty of up to eight thousand leva if the creation of the pornographic materials involves a person who has not reached 18 years of age or a person who looks like a person who has not reached 18 years of age.

(5) When the act under Paragraphs 1 - 4 has been performed by order or in execution of a decision of an organized criminal group the punishment is imprisonment from two to eight years and a penalty of up to ten thousand leva and the court may decree confiscation of the whole or a part of the property of the perpetrator.
(6) Whoever holds or obtains for himself/herself or for somebody else through a computer system or in any other manner pornographic materials shall be punished by imprisonment for up to one year and a penalty of up to two thousand leva if the creation of the pornographic materials involves a person who has not reached 18 years of age or a person who looks like a person who has not reached 18 years of age.
(7) The object of the crime shall be confiscated in favor of the state and if it is missing or expropriated its equivalence shall be adjudicated.

The crimes related to pornographic materials, just like the crimes against intellectual property, are not typical computer crimes. Due to the wide distribution of information technologies however the distribution of such materials electronically happens more and more often. This form of distribution constitutes a very high level of public hazard, because in contrast to the distribution on paper the use of new technologies makes it possible for the materials to reach a practically unlimited number of persons. On account of that with the amendments of the Criminal Code from April 2007 the old framework of the crimes related to pornographic materials was amended by introducing new and more severely punishable corpora delicti related to the dissemination of such materials via the Internet.

2.10.1. Main Corpora Delicti

The Criminal Code provides two main corpora delicti of crimes related to pornographic materials. However, on both main corpora delicti the law does not make a difference whether computers or other information technologies have been used for the commitment of the act or not.

The first main corpus delicti includes the creation, exposure, presentation, broadcasting, offering, sale, renting or distribution in any other manner of pornographic materials (Article 159, Paragraph 1 of the Criminal Code).[96]

[96] For more details on the main corpus delicti under Article 159, Paragraph 1 of CC see Kopcheva, M., *Computer crimes*. Publisher Sibi. Sofia, 2006, page 120-123.

With the amendments to the Criminal Code from April 2007 a legal definition of the term "pornographic material" (Article 93, Item 28 of the Criminal Code) was introduced for the first time in Bulgarian legislation. According to this definition "pornographic material" is a material, which is indecent, unacceptable or incompatible with public morality and expresses explicit sexual behavior. The definition consists of two elements. First, it is about a material, which explicitly expresses sexual behavior. Article 93, Item 28 of the Criminal Code gives examples when an action can be accepted as explicitly sexual behavior. These are the cases when behavior expresses real or simulated sexual contacts between persons of the same or different sex, sodomy, masturbation, sexual sadism or masochism or lascivious showing of sexual organs.[97] The listing is exemplary and in every concrete case the court must assess whether a specific action is explicitly sexual behavior or not. The second element of the definition contains the public assessment of this material, namely that it is indecent, unacceptable or incompatible with public morality. Case law determines when a specific material is indecent, unacceptable or incompatible with public morality. What is of significance in this case is the fact that the two elements of the definition must be present at the same time, in order for a certain material to be qualified as pornographic. If a certain material expresses explicitly sexual behavior, but in its nature it is not indecent, unacceptable or incompatible with public morality, it will not be categorized as pornographic. Examples of such materials are the various textbooks for educational purposea, science literature, works of art and others. When a material is indecent, unacceptable or incompatible with public morality, but it does not express explicitly sexual behavior, it will not be categorized as pornographic either.

The main corpus delicti of the crime under Article 159, Paragraph 1 of the Criminal Code is formulated in a technologically neutral manner and covers the creation and dissemination of pornographic materials in any manner whatsoever. The listing of the various manners of distribution is exemplary and the provision shall apply in relation to any other act, which can be categorized as dissemination, i.e. as bringing the contents of the respective materials to the attention of third parties. The applicable field of the provision covers the dissemination of pornographic materials on paper (newspapers, magazines, posters, calendars and so on), as well as on an electronic carrier (CDs, videotapes, DVDs and others) or online (e-mail, multimedia communications through mobile phones and others). Neither the material carrier, nor the

[97] In the preliminary text of the Criminal Code Amendment Bill put forward in August 2006 the exemplary hypotheses of openly sexual behavior were supplemented by actions for arousal or satisfaction of sexual desires. During the discussion of the draft in the Parliament this hypothesis was dropped out from the definition.

manner of dissemination of the materials are of significance to the indictability of the act. The stipulated punishment is imprisonment for up to one year and a penalty from BGN 1 000 to BGN 3 000.

The second main corpus delicti includes the acts of holding or obtaining for oneself or for somebody else through a computer system or in any other manner of pornographic materials, the creation of which involves a person who has not reached 18 years of age or a person who looks like a person who has not reached 18 years of age (Article 159, Paragraph 6 of the Criminal Code).[98] Despite the explicit indication of the computer system as a possible means of the crime this main corpus delicti also covers all possible acts, which can be qualified as holding or obtaining.[99] Holding means exercising factual possession over the respective pornographic material, while obtaining means acquiring the material. Whether the perpetrator holds or obtains the pornographic material for himself/herself or for somebody else is of no significance to the indictability of the act. The act is indictable only when the creation of the pornographic material a person who has not reached 18 years of age or a person who looks like a person who has not reached 18 years of age. The moment of creating the material is valid. When a person looks like a minor (under 18 years of age) is a factual matter and shall be assessed by the court on a case by case basis. The carrier of the pornographic materials is of no significance to the indictability of the act. The explicit indication of the computer system as an exemplary carrier is more like an attempt to emphasize on the public hazard of the act when such a system is used for its commitment. The act will be a crime upon holding or obtaining the said pornographic materials on any material carrier whatsoever (paper, electronic carrier other than the computer system and others). The punishment stipulated for this crime is imprisonment for up to one year and a penalty of up to BGN 2 000.

2.10.2. Qualified Corpora Delicti

The Criminal Code stipulates qualified corpora delicti only in relation to the crime under Article 159, Paragraph 1 of the Criminal Code. Qualifying circumstances are the specific manner of committing the crime (dissemination through the Internet), the object of the crime (a person

[98] The Criminal Code Amendment Bill, put forward in August 2006 stipulated the introduction of a legal definition of the term "child pornography materials" (pornographic materials expressing or describing openly sexual behavior of a junior or a minor person or a person who looks like a junior or a minor person). During the discussion of the draft in the Parliament this proposal was rejected.

[99] For more details on the term "computer system" see the analysis of Article 93, item 21 of CC (item 2.2 above).

who has not reached 16 years of age), the means of the crime (pornographic material, the creation of which involves a person who has not reached 18 years of age or a person who looks like a person who has not reached 18 years of age) and other elements from the objective point of view (act committed by order or in execution of a decision of an organized criminal group).

The qualified corpus delicti, which is the closest to computer crimes, is the dissemination of pornographic materials through the Internet (Article 159, Paragraph 2 of the Criminal Code). The stipulated graver punishment for this crime is imprisonment for up to two years and a penalty from BG 1000 to BGN 3000. The provision was introduced with the amendments to the Criminal Code from April 2007.

The manner of dissemination of the pornographic materials is defined by the expression "through the Internet". In this part the editing of the provision is not precise and may lead to groundless expansion of the applicable field of the more severely punishable corpus delicti in relation to acts, the level of public risk of which is not so high. The meaning of the text is to sanction those acts, which are expressed in the dissemination of pornographic materials to an unlimited number of persons. Such dissemination is mainly publishing of materials on generally accessible website on the Internet. A considerably high level of public risk would characterize the hypothesis when the pornographic materials are stored in the computer system of the perpetrator but the so called peer-to-peer technologies (Internet based) offer access to them for an unlimited number of persons. The global network however allows exchange of information between individual persons, for example through e-mail, ICQ, Skype and other Internet based means of communication. The use of these means for exchange of pornographic materials does not constitute a high level of public risk compared to the acts under the main corpus delicti of Article 159, Paragraph 1 of the Criminal Code and does not justify the imposing of a graver punishment. Within this meaning the provision of Article 159, Paragraph 2 of the Criminal Code should be changes and the executive act should be defined more specifically.[100]

The subjective point of view of the act is of great significance to this crime. The crime is deliberate, therefore the perpetrator must be aware that the material is pornographic and

[100] The Criminal Code Amendment Bill put forward in August 2006 offered a different solution. It stipulated a graver punishment only for the public distribution through the Internet site of works with pornographic contents. This edition of the text was more adequate since it differentiated more clearly the acts with a higher level of public hazard, namely – the cases when the distribution is public through an Internet site. The Parliament however rejected this proposal and approved the more general formulation distribution through the Internet.

disseminates it purposefully. This means that the person knows or should know the contents of the material. When a person publishes pornographic materials on an Internet site, the criminal liability shall be borne by the said person. The employees of the internet service provider presenting that person with the possibility to maintain an Internet site are not bound to check the published information and shall bear liability only if they have known about its contents, for example if they have been informed of its contents and have not undertaken the necessary measures to remove it.

The corpus delicti under Article 159, Paragraph 3 of the Criminal Code is qualified with a view to the object of the crime and covers the hypotheses when the pornographic material is exposed, presented, sold, rented or in any other manner disseminated to a person who has not reached 16 years of age. The stipulated punishment is imprisonment for up to three years and a penalty of up to BGN 5 000. The corpus delicti does not disclose specific features with a view to the use of computers or other information technologies. The executive acts are the same as per the main corpus delicti under Article 159, Paragraph 1 of the Criminal Code and cover distribution on an electronic carrier or electronically, as well as any other form of distribution.

Under Article 159, Paragraph 4 of the Criminal Code the qualifying circumstance is the means of the crime (pornographic material, the creation of which involves a person who has not reached 18 years of age or a person who looks like a person who has not reached 18 years of age) and the punishment is imprisonment for up to six years and a penalty of up to BGN 8000. Under Article 159, Paragraph 5 of the Criminal Code the act is more severely punishable when it is committed by order or in execution of a decision of an organized criminal group and the punishment is imprisonment from two to eight years and a penalty of up to BGN 10000, and the court may decree and confiscate the whole or part of the property of the perpetrator. Both qualified corpora delicti do not disclose specific features, which attach them to computer crimes, with the exception that they are also applied in relation to the cases when the pornographic materials are disseminated through the Internet.

2.10.3. Confiscation of the Object of the Crime in Favour of the State

According to Article 159, Paragraph 7 of the Criminal Code the object of the crime is confiscated in favor of the state and if it is missing or expropriated its equivalence shall be

adjudicated. The correct determination of the object of the crime is of great significance to the legal application of the provision. The object of the crime is the pornographic material itself and only it can be subject to confiscation, respectively to restoration as cash equivalence. The material carrier, on which it is reproduced, is not subject to confiscation if the pornographic material can be removed from it. In this case the confiscation shall be expressed in the removal of the material from the carrier.

2.11. Computer Crimes against the Confidentiality of Correspondence

Article 171. (1) Whoever illegally:

1. opens, forge, hide or destroy foreign letter, telegram, sealed books, package and the like;

2. takes foreign opened letter or telegram with the purpose of getting to know their contents or presents the said letter or telegram to somebody else with the same purpose;

3. learns about a message not addressed to him/her, which has been sent electronically, or diverts such a message from its recipient, shall be punished by imprisonment for up to one year or with a penalty from one hundred to three hundred leva.

(2) If the act has been committed by an official who has abused his/her business capacity, the penalty is imprisonment for up to two years and the court may also decree imprisonment under Article 37, Paragraph 1, Item 6.

(3) Whoever learns about a message not addressed to him/her, sent by phone, telegraph, through a computer network or other means of communication, by using special technical devices, shall be punished by imprisonment for up to two years.

(4) When the act under Paragraph 3 is committed with a self-interest purpose or if considerable damages have been inflicted, the punishment is imprisonment for up to three years and a penalty of up to five thousand leva.

With the amendments of the Criminal Code from 2002 the legal framework of the crimes against confidentiality of correspondence was supplemented, which was prompted by the more and more widespread use of new technologies for exchanging of information. The immediate target of these crimes is the public relations providing the privacy and confidentiality of correspondence as a whole and in particular of that transmitted through the Internet.[101]

[101] For more details on crimes against privacy of correspondence see Stoynov, Paragraph *Criminal law. Special part. Crimes against human rights.* Publisher: Siela. Sofia, 1997 , page 205 and following.

2.11.1. Main Corpora Delicti

Article 171, Paragraph 1, Item 3 of the Criminal Code incriminates two main corpora delicti, which differ in the executive act. The first case is about the illegal learning of the contents of foreign message sent electronically and the second – about the diversion of such a message from its recipient.

The immediate target of the crime is the public relations guaranteeing the confidentiality of correspondence and the security of its transmission from the sender to the recipient.

From an objective point of view the object of the crime is a message sent electronically.[102] The message constitutes specific information. In contrast to the traditional crimes against privacy of correspondence, which have two objects – the information itself on one hand and the carrier of this information on the other hand (for example a letter, telegram and other), upon the illegal learning about a message sent electronically it is possible for the perpetrator to learn about the contents of the message without the need of physical access to the material carrier of the information. For example, such will be the hypothesis when a person illegally gains access to the e-mail of some other person through the Internet.

The executive act under the first main corpus delicti is formulated in the law as learning, i.e. bringing the contents of the message to the attention of the perpetrator. The perpetrator may learn about foreign message by gaining access to the computer system of the sender or the recipient or to some other computer system, through which the message passes or in which it is stored. From an objective point of view it is necessary for the message not to be addressed to the perpetrator. In case of a message sent by e-mail however the act will be considered as addressed to a certain person when this person is copied (including blindly) from the sender. The crime is effective – the result is the perpetrator's new knowledge of the contents of the message.[103]

Under the second main corpus delicti the executive act is expressed in the diversion of the message from its recipient. The diversion of the message means impeding its receiving by the

[102] For more details on the term "electronically" see the analysis of Article 319 "c", Paragraph 1 of CC (item 4.2.2 above).
[103] For the opposite standpoint see Kopcheva, M., *Computer crimes*. Publisher: Sibi. Sofia, 2006 , page 55. According to the author the crime is formal under both main corpora delicti.

recipient, to whom it is addressed. The crime is effective and the result is expressed in the lack of the message in the respective device for receiving of messages of the recipient.

The subject of the crime under both main corpora delicti may be any criminally liable person with the exception of the titular, the author and the recipient of the message, to whom it is not foreign. Upon the diversion of the message from the recipient, as far as the law does not qualify the message as "foreign", theoretically it is possible that the subject of the crime is the titular or the recipient of the message, when he/she diverts his/her own message. Nevertheless, the intention of the legislator probably is not to sanction these specific hypotheses, so with a view to the specification of the text it is recommended that under both main corpora delicti the message be explicitly defined as "foreign".

From a subjective point of view there is malice. The perpetrator is aware that the message is foreign (that it is not addressed to him/her) and despite that he/she learns about its contents or hinders its receiving by the recipient.

The punishment stipulated under по Article 171, Paragraph 1, Item 3 of the Criminal Code is imprisonment for up to one year or a penalty from BGN 100 to BGN 300.

2.11.2. Qualified Corpora Delicti

The Criminal Code stipulates four qualified corpora delicti of encroachments against the confidentiality of correspondence when it is implemented electronically. The qualifying circumstances are the subject of the crime (an official), the means of the crime (special technical devices), the criminal purpose (self-interest purpose) and the criminal result (infliction of considerable damages).

2.11.2.1. Qualified corpora delicti with a view to the subject of the crime

The act is qualified with a view to the subject of the crime when it is committed by an official who has abused his/her business capacity (Article 171, Paragraph 2 of the Criminal Code). The stipulated punishment is imprisonment for up to two years and the court may also rule for the deprivation of the right to occupy a specific state or public position.

By virtue of Article 93, Item 1 of the Criminal Code an official is a person appointed to occupy on a salary or free of charge, temporarily or permanently, a position in a state institution with the exception of the ones performing only activity of material execution or leading work or work related to the safeguarding or managing foreign property in a state institution, cooperation, public organization, other legal entity or a sole proprietor vendor, as well as the position of a private notary, assistant private notary, private judicial executor and assistant private judicial executor.

From an objective point of view, in order for a crime under the qualified corpus delicti of Article 171, Paragraph 2 of the Criminal Code to be present, it is necessary for the official to have abused his/her business capacity, i.e. to use his/her official functions to gain access to foreign message.[104]

2.11.2.2. Qualified corpora delicti with a view to the means of the crime

The crime is qualified with a view to the used means when it is committed using special technical means (Article 171, Paragraph 3 of the Criminal Code).[105] The stipulated punishment is imprisonment for up to two years. The more severely punishable corpus delicti applies only in relation to learning about foreign message, but not in relation to the diversion of a message from its recipient.

From an objective point of view it is necessary for the message to be sent through a computer network or some other communication device.[106] With a view to the specification of the provision and standardizing the terminology with the one used in the main corpus delicti, it is recommended to use the expression "message sent electronically" in the qualified corpus delicti as well.

[104] For more details on crimes committed by an official who has abused his/her business capacity see Stoynov, Paragraph *Criminal law. Special part. Crimes against property.* Publisher: Siela. Sofia, 1997, page 36.
[105] Also see Kopcheva, M., *Computer crimes*. Publisher: Sibi. Sofia, 2006, page 56-59. According to the author the text of Article 171, Paragraph 3 of CC regulates a different main corpus delicti of a crime against the confidentiality of correspondence.
[106] For more details on the definition of the term "computer network" see the analysis of Article 93, item 25 of CC (item 2.5 above).

From an objective point of view the crime must have been committed by using special technical devices.[107] These are devices used for the implementation of specific technical activities. On order for the act to be more severely punishable the technical devices must have been used according to their specific designation. The technical devices are special when their use requires special skills. In the hypothesis of a message sent through a computer network these technical devices could be hardware or software using connection to a computer network or providing access to the information exchanged through it.

2.11.2.3. Qualified corpora delicti with a view to the criminal purpose and the criminal result

With the amendments to the Criminal Code from April 2007 two more qualified corpora delicti of encroachments against the confidentiality of correspondence were added. The qualifying circumstances are the criminal purpose (self-interest purpose) and the criminal result (infliction of considerable damages).[108] Both corpora delicti are regulated in Article 171, Paragraph 4 of the Criminal Code and the stipulated punishment is imprisonment for up to three years and a penalty of up to BGN 5000. The particular thing about this provision is that it applies only in relation to Article 171, Paragraph 3 of the Criminal Code, i.e. is concerns only the cases of illegal learning by using special technical devices of a message sent by phone, telegraph, through a computer network or other communication device.[109]

2.12. Destruction and Damaging of Foreign Property

Article 216. (1) Whoever destroys or damages illegally foreign movable or immovable property shall be punished by imprisonment for up to five years.

(2) Whoever destroys, demolishes or damages his/her own mortgaged or pledged property shall be punished by imprisonment for up to five years and a penalty of up to two thousand leva.

[107] For more details on the use of special technical devices see Stoynov, Paragraph *Criminal law. Special part. Crimes against property.* Publisher: Siela. Sofia, 1997, page 33.

[108] For more details on the infliction of considerable damages and the self-interest objective see the analysis of Article 319 "b", Paragraphs 2 and 3 of CC (item 2.4.2.1 and item 2.4.2.3 above).

[109] The Criminal Code Amendment Bill put forward in August 2006 proposed that the act of illegal interception through technical devices of foreign electronic message or other computer data not addressed to the perpetrator be incriminated as a separate crime (punishable by imprisonment for up to one year and a penalty of up to BGN 3 000) and that the qualified corpora delicti with self-interest objective or inflicted considerable damages (imprisonment for up to three years and a penalty of up to BGN 5 000) to be applied only in relation to this crime. During the discussion of the draft in the Parliament however the introduction of a new main corpus delicti was not approved and the proposed qualified corpora delicti were added, but in relation to the already existing main corpus delicti of illegal learning through use of special technical devices of a message not addressed to the perpetrator sent by phone, telegraph, through a computer network or some other communication device.

(3) Whoever gains illegal access to a computer, which is of significance to an enterprise, institution, legal entity or natural person and thus destroys or damages foreign property shall be punished by imprisonment from one to six years and a penalty of up to ten thousand leva.

(4) In insignificant cases the punishment is imprisonment for up to six months or a penalty from one hundred to three hundred leva.

(5) If significant damages are inflicted or other grave consequences have occurred and if the act has been committed by a person under Article 142, Paragraph 2, items 6 and 8, and if the act is related to the destruction or damaging of elements of the communication network, the punishment is imprisonment for up to ten years and the court may also rule deprivation of rights under Article 37, Paragraph 1, Items 6 and 7.

(6) If the act under Paragraphs 1, 2, 3 and 5 has been committed due to carelessness the punishment if imprisonment for up to two years or a penalty from one hundred to three hundred leva.

The destruction and damaging of foreign property by gaining illegal access to a computer is provided for in Article 216, Paragraph 3 of the Criminal Code.[110]

From an objective point of view the executive act of the crime includes two elements. The first element is the gaining of illegal access to a computer, which is of significance to an enterprise, institution, legal entity or natural person. The computer constitutes a computer system within the meaning of Article 93, Item 21 of the Criminal Code.[111] When a specific computer is of significance to an enterprise, institution, legal entity or natural person is a factual matter, which shall be assessed by the court on a case by case basis. For this assessment the court should consider the properties of the computer itself, as well as the information and data stored in it. Illegal access is any access, which is not justified lawfully (normative act, provision from internal rules or procedures, private legal transaction and others).

The second element of the executive act is the same as under the main corpus delicti of destroying and damaging under Article 216, Paragraph 1 of the Criminal Code – destroying and damaging foreign property.[112] It should be taken into consideration that in order for a crime under Article 216, Paragraph 3 of the Criminal Code to be present from an objective point of

[110] The Criminal Code Amendment Bill put forward in March 2006 proposed that Article 216, Paragraph 3 of CC be dropped out but due to the withdrawal of the draft the provision remained unchanged.

[111] With the amendments to CC from April 2007 the legislator failed to correct the terminology in the text of Article 216, Paragraph 3 of CC. Everywhere else the term "computer" was replaced by "computer system".

[112] For more details on the crimes against privacy of correspondence see Stoynov, Paragraph *Criminal law. Special part. Crimes against property.* Publisher: Siela. Sofia, 1997 , page 115 and following.

view between the two acts, there must be a functional relationship – the gaining of illegal access is the manner, means for destruction of damaging of foreign property.

According to Article 216, Paragraph 5 of the Criminal Code the act is more severely punishable (imprisonment for up to ten years and the court may also decree deprivation of the right to occupy a specific state position or to exercise a specific profession or activity) if a specific criminal result is present (inflicted considerable damages or other grave consequences occurred), if it has been committed by a special subject (a person engaged in security, an employee at an organization performing security or insurance activity, a person acting by order of such organization or pretending to be acting by such order, a person from the members of the Ministry of Interior or a person who pretends to be such a member, a person who acts by order or in execution of a decision of an organized criminal group or organization or a group, which uses force of strikes fear to conclude transactions or gain benefits) or if it is with a special object (related to the destruction or damaging of elements from the communication network).

There are also two privileged corpora delicti stipulated – when the act is insignificant the punishment is imprisonment for up to six months or a penalty from BGN 100 to BGN 300 (Article 216, Paragraph 4 of the Criminal Code), and when it has been committed due to carelessness the punishment is imprisonment for up to two years or a penalty from BGN 100 to BGN 300 (Article 216, Paragraph 6 of the Criminal Code).

2.13. False Documenting

Article 313. (1) Whoever confirms an untruth or conceals the truth in a written declaration or message sent electronically, which by virtue of a law, decree or ordinance of the Council of Ministers are given before a regulating body to certify the authenticity of specific circumstances, shall be punished by imprisonment for up to three years or a penalty from one hundred to three hundred leva.

(2) When the act under Paragraph 1 is committed with the purpose of avoiding payment of due taxes the punishment is imprisonment from one to six years or penalty from one hundred to two hundred and fifty leva.

(3) The punishment under Paragraph 1 is also imposed on whoever confirms an untruth or conceals the truth in a private document or message sent electronically, in which by virtue of an explicit provision of a law, statute or

ordinance of the Council of Ministers he/she is specially bound to certify the truth, and uses this document as proof of the falsely certified circumstances or statements.

(4) Whoever uses false favorable data or conceals such that is of great significance to the decision for acquisition of securities in relation to public offering of securities in a prospect or review of specific economic status, shall be punished by imprisonment for up to three years and a penalty of up to five hundred leva.

With the amendments to the Criminal Code from 2002 the electronically sent message was added to the corpora delicti of false documenting under Article 313, Paragraphs 1 and 3 of the Criminal Code as the object of the crime.[113] The corpora delicti incriminate the confirmation of an untruth or the concealment of the truth in various types of documents and the only relation to computer crimes is the possibility of these documents being messages sent electronically.[114]

The changes in the corpora delicti of false documenting are practically unnecessary. The electronically sent message will be a document within the meaning of the Criminal Code only if it complies with the requirements for an electronic document under EDESA. In this case however by virtue of Article 3, Paragraph 2 of EDESA this message will be equalized to a written document thus falling within the applicable field of Article 313 of the Criminal Code before the change. On the other hand, if the electronically sent message does not comply with the requirements for an electronic document it shall have no legal significance, because it does not authenticate the statement.

[113] For more details on the definition of the term "electronically" see the analysis of the provision of Article 319 "c", Paragraph 1 of CC (item 4.2.2 above).

[114] For more details on false documenting see Kopcheva, M., *Computer crimes*. Publisher: Sibi. Sofia, 2006 , page 125-127.

3. LEGAL PROVISIONS ON CYBERCRIME IN ROMANIA

3.1. Introduction

According to the data made public by the National Authority for Communications of Romania (ANC), Romania has witnessed a significant increase of the access to Internet during the last years reaching a penetration rate estimated at 27% of the population, while 10% has access to broad-band solutions.

Naturally, with the increase of the access to the Internet, an entire national industry was developed in relation to the new communication mean, so electronic commerce or online advertising no longer represent anything uncommon. According to EuroStat statistics, the local e-commerce market was estimated at Euro 120 million, although 3% of the population in Romania has bought goods or services online.

The electronic payment means have also become a daily routine with 10 million cards issued and 29 banks with electronic banking systems. However, a large part of the economy is still based on cash having in view that 78% of the population uses the cards only to withdraw cash from Automated Teller Machines (ATMs). Unfortunately, some people have tried to profit from certain security weaknesses of the computer applications or only tried to use some new communication methods for classical legal offences. We notice that, along with the absolutely spectacular development of the Internet and of the related applications during the last 10 years, the methods of infringing the law by means of the Internet have also development and improved, from the standpoint of the people involved as well as of the technology used.

In this context, this chapter is meant to briefly approach the main legal terms related to cybercrime as they are regulated by the Romanian legislation. As it is a continuously developing environment, we believe the legislation must be updated from time to time to keep pace and therefore, we have introduced Chapter 4.

3.2. The Romanian Legislation on the New Technologies

We have to reckon that most part of the Romanian legislation on information technology represents the implementation of the *aquis communautaire* and actually, in most cases, it is just a translation of the directives. The positive side of this process is the similarity with the European directives and hence, the easiness in interpreting or comparing it to normative acts of other countries. The negative side of the process is the lack of coordination between the issued normative act and the rest of the Romanian legislation which often leads to contradictions and unclear elements between various acts. The literal translation of the text also makes it difficult sometimes to put the provisions into practice, a non-specialised person finding it hard to relate a specific case to a certain article. Therefore, we propose, inter alia, to try and identify the concrete cases when certain provisions would be applicable.

For an easier understanding and for the purpose of this study, we suggest splitting the Romanian legislation into 3 categories:

A. Legislation adopted for the implementation of the acquis communautaire including:

- Law of e-commerce – in force (Law 365/2002 with the modifications brought by Law 121/2006)
- Ordinance on the protection of consumers at contract conclusion and remote execution - in force (OG 130/2000 with the modifications brought by Law 51/2003 and Law 373/2007)
- Law on electronic signature - 455 / 2001
- Technical and methodological standards of December 13, 2001 for the application of Law 455/2001 on electronic signature
- Law for the protection of persons related to personal data processing and the free circulation of data - 677 / 2001
- Law on personal data protection and of private life in the electronic communication sector - 506/2004

- *Normative acts on communications regulation*
    - Government Ordinance 34/2002 on the access to public electronic communication networks and the associated infrastructure as well as their interconnection, approved with modifications and completions by Law 527/2002

- Government Emergency Ordinance 79/2002 on the general regulation framework for communications, approved with modifications and completions, by Law 591/2002, with further modifications and completions
- Government Ordinance 31/2002 on post services, approved with modifications and completions by Law 642/2002, with further modifications
- Law 304/2003 for universal service and the right of users regarding electronic communication networks and services
- Law 239/2005 on the modification and completion of normative acts in the domain of communications

- *Normative acts modifying the legislative framework on copyright*
  - Emergency Ordinance 123 of September 1, 2005 for the modification and completion of Law 8/1996 on copyright and related rights
  - Law 285 of June 23, 2004 for the modification and completion of Law 8/1996 on copyright and related rights

B. Romanian legislation adopted after having adhered to international conventions

This framework mainly includes:

- Provisions on the prevention and combating cybercrime (Title III of Law161 dated 19/04/2003 on certain measures to ensure the transparency in exercising public offices and positions and in the business environment, to prevent and sanction corruption - Published in Official Journal, Part I no. 279 dated 21/04/2003)
- Law 64 dated 24/03/2004 for the ratification of the Council of Europe's Convention on Cybercrime, adopted in Budapest on November 23, 2001

C. Romanian legislation adopted following national initiatives

These normative acts have a smaller influence from the point of view of this study:

- Law on temporal mark 451/2004, published in the Official Journal, Part I no. 1021, November 05, 2004

- Law on the legal regime of notary electronic activity - 589/2004 published in Official Journal no. 1227/December 20, 2004

- Order of the Minister of Communications and Information Technology no. 221/ June 16, 2005 for the approval of the technical and methodological standards for the application of Law 589/2004 on the legal regime of notary electronic activities

- Law on archiving documents in electronic format 135/2007 - published in Official Journal no. 345 of May 22, 2007

- Law on the registration of commercial operations by electronic means 260/2007 - published in Official Journal, Part I no. 506 dated 27/07/2007

- Law on the setting up, organisation and operation of the National Supervisory for Personal Data Processing -102/2005

- Law on preventing and combating pornography - 196/2003 published in Official Journal no. 342 / May 20, 2003

3.3. Cybercrime

Title III of Law 161/2003, mentioned above includes three categories of offences related to cybercrime as follows:

a) Offences related to the confidentiality and integrity of computer systems and data

- Illegal access to a computer system;

- Illegal interception of a computer data transmission;

- Data interference;

- System interference;

- Illegal operations by means of information devices or systems.

b) Cyber offences

- Computer-related forgery;

- Computer-related fraud.

c) Child pornography through computer systems

We will also study more broadly here the offences introduced by Law 365/2002 which applies sometimes to cybercrime as well:

- Art. 24: Forgery of electronic payment instruments
- Art. 25: Possession of equipment with a view of forging electronic payment instrument
- Art. 26: Misrepresentation with a view of issuing or using electronic payment instruments
- Art. 27: Fraudulent performance of financial operations
- Art. 28: Acceptance of fraudulent financial operations

For a better understanding and interpretation of these provisions, we will continue with a detailed legal analysis of each above mentioned infringement.

3.3.1 Terms and Definitions

For the beginning, defining the instruments and concepts the legislator chose to operate with is more than necessary, and has been already done in Article 35 of Law no. 161 of 2003, as follows:

a) computer system means any device or assembly of interconnected devices or that are in a operational relation, out of which one or more provide the automated data processing by means of a computer program.

Examples: personal computer (PC), two or more workstations connected by cable or wireless, computer network, ad-hoc networks consisting of a PC and the peripherals (printer, external storage devices, scanners etc.), and also the ATMs which deliver cash to the customers identified by a electronic instrument, such as a CARD.

b) automatic data processing is the process by means of which the data in a computer system are processed by means of a computer program.

Example: following a logical algorithm, the instructions for the computer are written in a "high level" programming language (such Pascal, C++, Visual Basic, Java etc.), implemented from the keyboard, interpreted by the Central Processing Unit (of the PC), and then translated into a machine-code language and further executed by the Execution Unit, each component of the PC running a certain operation.

c) computer program means a group of instructions that can be performed by a computer system in order to obtain a determined result.

Computer programs Examples: Operation Systems (Ms-DOS, Ms Windows, UNIX, Ubuntu etc.), standard applications package (Ms Office, Open Office, Star Office – which usually consist of a word processor, a database running software, spreadsheet application for calculation, graphing tools and tables, a presentation software etc.), dedicated applications (ERP – Enterprise Resource Planning – for the financial, logistics and human resources needs of a company, CRM - Customer Relationship Management – electronic instrument for a business management and organising the relations with the customers), antivirus software (BitDefender, Norton Systems Work, NOD32, Avast etc.), Internet-related programmes (Browsers – Microsoft Internet Explorer, Mozilla Firefox, Netscape etc., electronic mail –Outlook, Webmail, Eudora etc.), various other special designed applications even with destructive scope (Viruses, Worms, Trojan Horses, Logical Bombs, Keyloggers, Spyware etc.) and much more;

d) computer data are any representations or facts, information or concepts in a form that can be processed by a computer system. This category includes any computer program that can cause a computer system to perform a function.

At the user's level, data are represented in a alphanumeric form – numbers, letters, special characters, as they appear on the computer screen. At the machine level, these data can be seen as arrays of 8, 16, 32, 64 or 128 bits ("0" and "1" coded elements which, in fact, represent the controlled variations of voltage).

Practically, any data which can be found in a computer system could be regarded as computer data. Example: word processed documents, tables, images, audio-video files etc.

e) service provider means:

1. any natural or legal person offering the users the possibility to communicate by means of a computer system;

2. any other natural or legal person processing or storing computer data for the persons mentioned at item 1and for the users of the services offered by these.

One can note that the Romanian legislator did not limit the service provider's category to the one of the Internet Service Providers, the definition being comprehensive, including also a Free Internet Provider, an Internet-Cafe, the owner of a cafe-bar who offers free WiFi Internet access (hotspot), a provider of Host Services, a provider of Back-up or Electronic Archive services etc.

f) traffic data are any computer data related to a communication achieved through a computer system and its products, representing a pat of the communication chain, indicating the communication origin, destination, route, time, date, size, volume and duration, as well as the type of the service used for the communication.

Example: data recorded (logged) by a server with reference to a File Transfer Protocol access

g) data on the users are represented by any information that can lead to identifying a user, including the type of the communication and the service used, postal address, geographical address, IP address, telephone numbers or any other access numbers and the payment means for the respective service as well as any other data that can lead to identifying the user.

Noticeable is the similarity of the elements of this definition with those comprising the definition of the personal data (from Article 3 item a) of Law 677 of 2001)

> *personal data is any information regarding an identified or identifiable natural person. A identifiable person is the one who can be identified, directly or indirectly, in a particular way by reference to a identification number or to one or several specific factors of his physical, physiological, psychological, economical, cultural or social identity;*

One of the most important user data for the criminal cyber investigation is the Internet Protocol Address (or IP address). The IP address is a 32 digits number written, regularly, in a decimal format, with dots. Example: IP address 154.162.1.28 identify (for the usage of the Internet Protocol or the sent or received IP data packages) a certain PC network interface. However, this IP address could be allocated by the Service Provider to a user both ways, static or dynamic, and therefore is not simple to determine a link to a certain natural person.

h) security measures refer to the use of certain procedures, devices or specialized computer programs by means of which the access to a computer system is restricted or forbidden for certain categories of users.

Example: access system (LOGIN) based on a username and password, PKI (Public Key Infrastructure) encryption software or infrastructure for communications, electronic signature applications, SmartCard access tools, print or eye reader etc.

i) pornographic materials with minors refer to any material presenting a minor with an explicit sexual behaviour or an adult person presented as a minor with an explicit sexual behaviour or images which, although they do not present a real person, simulate in a credible way a minor with an explicit sexual behaviour.

For a detailed interpretation of this definition, related to other legal provisions, we recommend the reading of the bibliographical materials at the end.

j) For the purpose of this law, a person acts without right in the following situations:

- *is not authorized, in terms of the law or a contract;*
- *exceeds the limits of authorization;*
- *has no permission from the qualified person, according to the law, to use, administer or control a computer system or to carry out scientific research in a computer system.*

Example: It will not be the case of the crime of illegal access to a computer system if the access was approved by the legitimate user of the system (or by the owner or the legal beholder). Moreover, accessing the computer system belonging to both spouses by one of them cannot be regarded as illegal while the respective system is being commonly used by each of the spouse (regardless the period spent in using the system) and the computer data stored are not personalized and signalled accordingly by encryption or protection against the opening, re-writing, modification or access restriction.

Also the interaction with a computer system which allows free and open access to its resources from the users (public).cannot be considered as a crime.

To the definitions provided by Law 161 of 2003 (Title III – prevention and combating cybercrime), we must add those detailed in Law 365 of 2002 regulating the electronic commerce, Chapter I – General Provisions, Article 1, for a better understanding of the cyber-environment we are referring to.

a) *information society service – any activity of providing services or that involve the creation, modification, transfer or termination of a real right on a fixed or non-fixed asset, activity carried out by electronic means, that shows the following characteristics:*

- *it is performed considering a patrimony interest provided to the supplier usually by the recipient;*
- *the supplier and the recipient do not have to be physically present simultaneously at the same place;*
- *it is carried out by transmitting the information at the individual request of the recipient; electronic means – electronic equipment and cable networks, optic fibre, radio, satellite and others, used to process, store or retransmit information*

This definition caused several debates in practice. We consider that the interpretation of the definition has to be done according to the European practice. Thus taking into account that the Law 365 of 2002 is a direct implementation in the national legislation of EU Directive on electronic commerce (2000/31/EC), it is essention to consider the above-mentioned provisions in relation with the 18th Recital of E-commerce Directive with reference to what should be regarded as information society services:

> *Information Society (IS) services consist of a large scale of online economic activities. These activities could especially be online sales of goods. Other activities, such as delivering goods or providing off-line*

services, are not covered. Information Society services are not exclusively bound to services concluded with online contracts, but, in the way they represent an economic activity, they are extended to free of charge services (such as online news and information, commercial communications, online searching engines, search and retrieve data etc.). Information Society services are also cover information transmission in a network, providing access to a communication network or hosting the information provided by a beneficiary. In the light of Directive CEE/89/552, TV and Radio services are not IS services because they are not provided upon individual request. On the other hand, point-to-point transmitted services (such as video on demand or commercial electronic mail) could be regarded as IS services. The use of Email or of equivalent communication means by individuals not acting in their commercial or professional capacities, including the use of such means to conclude any form of contract, is not considered as being an IS service. Also, the contractual relationship between an employer and its employees is not an IS service, and neither are the activities which, by their nature, cannot be fulfilled remotely using electronic means, such as the authorized control of the accounts of a company or the medical examination.

Electronic Means – electronic equipment and cable, Optic Fibre, radio, satellite based networks used to process, store and transmit the information;

Domain – an area of an information system owned as such by a natural or legal person or by a group of natural or legal persons with a view of data processing, storing or transfer;
For example: regarding the webpage hosted at URL http://www.legi-internet.ro, the domain is legi-internet.ro

Commercial communication - any form of communication meant to promote, directly or indirectly, the goods, services, image, name or denomination or logo of a company, trader or a person exercising a regulated profession. The following do not constitute commercial communications themselves: information allowing direct access to the activity of a natural or legal person, especially a domain name or an electronic mail address, communications related to the products, services, image, name or brand of a natural or legal person made by a third party, independent from the respective person, especially when they are made free of charge;

Electronic Payment Instrument – an instrument allowing the owner to carry out the following types of operations:

- *fund transfers others than the ones ordered and performed by financial institutions;*
- *cash withdrawal as well as charging and discharging of an electronic money instrument;*

Owner – person owning an electronic payment instrument on the basis of a contract signed with an issuer, under the conditions of the law;

Identification Data – any information allowing or facilitating the types of operations mentioned at item 10, as well as an identification code, name and denomination, residence or headquarters, telephone, fax numbers, electronic mail address, registration number or similar identification means, fiscal code, personal numerical code and other similar.

One has to note that, presently, the Romanian legislation is passing a transition period. A large reform of the criminal law is however envisaged, which primarily targets the Criminal Code. As regarding the computer-related crimes, a new Title will be added (Title X – Crimes against Data and Computer Systems) with all the provisions (even modified or updated) of Law 161 of 2003 regarding cybercrime.

3.3.2 Illegal Access to a Computer System

Article 42 of Law 161 of 2003

(1) The access without right to a computer system is an offence and is punished with imprisonment from 3 months to 3 years or a fine.

(2) Where the act provided in paragraph (1) is committed with the intent of obtaining computer data, the punishment is imprisonment from 6 months to 5 years.

(3) Where the act provided in paragraphs (1) and (2) is committed by infringing the security measures, the punishment is imprisonment from 3 to 12 years.

Protected Legal Interest

Is represented by the social value called *computer system* and by the social relationship which emerges with reference to the use of automated data processing systems in society. At the same time, the legal provisions assure the inviolability of the "cyberspace". Other specialists are also talking about the protection of the „cyber home". There is no doubt that the definition for „cyberspace" also includes the computer data, as they will be described further on.

The protected legal interest could also be that of the owner or legitimate user of the computer system, as well as of the owner, beholder or legitimate user of the computer data stored or transmitted within the respective computer system.
It is also worth mentioning that the cyber offence is a type of crime that, to the extent of the legal provision in force, has the characteristic of affecting two (or more) social values, therefore it could be seen like having two (or more) legal objects, a main one, and a secondary one.

Subjects of the offence

The Offender

Could be any person who has criminal responsibility and is liable to punishment, the text of the law mentioning no special capacity for it.

The legal practice, however, demonstrated that, in most of the cases, this type of persons have certain IT knowledge. A high percentage of them represent high-tech, IT or network specialists, familiar with the computer or network security measures.

Researches on criminology have shown that the most active are the "enemies within", meaning both those who do not have a clue about IT or the ability of using computers thus being a real threat for the systems, and those members of organizations (employees, contractual personnel, collaborators, associates etc.) who choose to react to the management rules or to express their negative behaviour acting in a wrong way against computer systems or using them to commit crimes.

The involvement in the crime is possible in all known forms, the offender acting as principal, co-principal, instigator or accomplice.

The Victim

Is the natural or legal person owner or beholder of the illegally accessed computer system or the respective illegally obtained computer data. To some extent, there could be "collective victim" when an illegal access to a computer system generates automated illegal accesses to other computer systems inter-connected with the first one.

There could be a secondary victim when, for example, the computer data obtained by the perpetrator refer to a natural or legal person, other than the owner or the legal beholder of that data. This is the case of somebody accessing without right the database of the National Inspectorate for Persons Records and getting hold of personal data (in a digital form) regarding a certain person (with the intent to further use the data illegally).

The Materiality of the crime

It is achieved by the access without right to a computer system (workstation, server or network).

The access, in term of the law, means entering the whole or just a part of the computer system. The connection link, either direct or remote (including the use of wireless or satellite), has no relevance.

In its easiest form, the access without right to a computer system requires the interaction of the offender with the respective system through equipment or other components, such as power source, on/off buttons, mouse, keyboard or joystick).

There will be illegal access in a simple form in the situation when the offender, manoeuvring his own peripherals (e.g. keyboard), remotely finds and uses an external way to get into another computer system. This is the common case of entering another workstation of a LAN, MAN, WAN etc.

In order to get the access, de offender usually tries a large variety of technical procedures, such as: *attack of the password, free access attack, attack that exploits technological weaknesses, attack that exploits shared resources, IP attack or hijacking TCP session attack*.

An interesting type of illegal access, very often used nowadays in Romania (but not only) is the *social engineering attack*. This king of attack is more frequent and dangerous while more users get connected cu Internet or other networks (LAN, WLAN etc.). An usual example of social engineering is when the offender sends email messages to a category of users (or even by phone) pretending to be the administrator of the local computer, network or telecommunication system and asking them to be provided with personal data, as well as

passwords, falsely claiming that the system ”just recovered from a failure or unexpected interruption of the services”.

The access to another person’s e-mail

3.3.2.1 As regarding he access to the electronic mail, from a criminal perspective we have different situations and therefore multiple indictment possibilities, as follows:

- When the electronic mail is accessed from the computer system the victim uses and beholds irrespective of the legal situation in place (owner, based on a contract, as fulfilling service duties or considering other legal provisions). Under the circumstances, any access to that system by another individual (who does not have the same rights) will be considered unlawful (illegal) and the provision of Article 42 Paragraph 1 of Law 161/2003 could be regarded as the legal charge.

- When the usual access to the electronic mail is done through a specialized interface called e-mail Client. This web-based application facilitates the owner of an e-mail account the sending/receiving or storing of electronic messages (in a digital format). Usually, after the exchange of data between the local system and the dedicated servers (mail servers), both the received and the sent messages are stored on the Hard Disk of the system (in the special memory area reserved to the application).

3.3.2.1.1 The E-mail software (e-mail client) is not protected against unlawful access by security measures. In the case of an individual entering this application we cannot cross the legal conditions of an illegal access to a computer system, because, taking into consideration the definitions of Article 35 of the law, the ”system” is a device or assembly of devices and not a computer program or an application. Simply, entering the e-mail software could not be legally charged by using the present provisions.

If the offender accesses the e-mail client with the intent of obtaining messages already/previously received, sent or stored by the victim, then the correct indictment would be illegal access to a computer system with the intent of obtaining computer data (Article 42 paragraph 2) – just with reference to the computer system access (conditions presumed at item 1), and violation of the secrecy of correspondence (as stated in Article 195 paragraph 1 of the Criminal Code), in real concurrence.

The opinion that, using a email client, there is an illegal access to the mail server, is false, because, at the opening of the application, it automatically and independently communicates with the mail server and stores locally (for reading) all the new messages. In other words, we do not have the form of guilt (no *mens rea*), necessary for the existence of the crime.

3.3.2.1.2 Email software is protected by security measures, and the offender acts for infringing those measures. In this case we could only charge the offender for illegal access to a computer system, eventually with the intent of obtaining computer data (Article 42 paragraph 2) and violation the secrecy of correspondence (Article 195 paragraph 1 Criminal Code) in real concurrence. Any other mention or reference to Article 42 paragraph 3 of Law 161/2003 (the illegal access to a computer system by infringing the security measures) is from the start erroneous.

3.3.2.2 The Email is directly accessed from the (remote) Mail Server of the service provider, using the facility offered by WEBMAIL application (remotely email accessing tool), possible with the help of another software (incorporated or not in the operating system) called Browser. Being an external resource and taking into account that Server is a electronic device (interconnected with other similar devices) it is clear that we have the conditions of accessing a computer system.

The authentication of the user into the system (web application and the Mail Server) is compulsory and is usually done by inputting a *username* and a *password*.

3.3.2.2.1 Accessing the Email account through Webmail is accomplished by the offender following a correct authentication in the system using the real username (ID) and the real password.

In this case, the appropriate indictment would be: a crime of illegal access to a computer system (Article 42 paragraph 1) – with the reference to the access without right of the PC (workstation) belonging to the victim, a crime of illegal access to a computer system with the intent of obtaining computer data (Article 42 paragraph 2) – with the reference to the remote access of the Mail Server, and a crime of violating the secrecy of correspondence (Article 195 paragraph 1 Criminal Code), the later two in ideal concurrence, because the

offender did not have the capacity or the right to access the email account, created and used by the victim.

Taking into consideration the legal provisions of Article 42 paragraph 3 (illegal access to a computer system by infringing the security measures) would be false, because technically speaking the authentication into the system (even fraudulent) is done correctly. The data (username and password) filled in are real and thus known by the system. Accepting just this two security elements (account name/username and password), the system has no other possibility to verify the identity of the real/pretended user and therefore consider the access as being legitimate.

3.3.2.2.2 Accessing the email account through Webmail facility is done by the offender by infringing of the security measures. In order to get access, the offender will eventually try a variety of technical proceedings, such as: attack of the password, attack of free access, attack that exploits technological weaknesses, attack that exploits shared resources, IP attack or the hijacking of TCP session attack.

In this case, the correct indictment would be: a crime of illegal access to a computer system, simple form (Article 42 paragraph 1) – with the reference to the access without right of the computer system owned, belonging to or used by the victim, a crime of illegal access to a computer system with the intent of obtaining computer data, by infringing the security measures (Article 42 paragraph 3) – with the reference to the forced access of the Mail Server, and a crime of violation the secrecy of correspondence (Article 195 paragraph 1 Criminal Code), these later two in ideal concurrence.

3.3.2.3 The Email messages are read on a computer system of free access (or public access, unrestricted). Access to email is done through an Email Client.

3.3.2.3.1 The access to email messages is done through an Email Client unprotected by security measures. Under the circumstances, the correct indictment would be just violation the secrecy of correspondence.

3.3.2.3.2 The access to email messages is done through a protected Email Client, and the offender acts against the security measures. In this case, also, the correct indictment would be just violating the secrecy of correspondence.

3.3.2.4 The access to email messages is done through Webmail facility, by remote access of the Mail Server (a computer system in the terms of Law 161/2003)

The offender succeeds the authentication into the Mail Server by inputting the real username (account name) and password. In this case, the correct indictment would be: the crime of illegal access to a computer system with the intent of obtaining computer data (Article 42 paragraph 2) and violation the secrecy of correspondence (Article 195 paragraph 1 Criminal Code), in ideal concurrence.

The offender succeeds the authentication into the Mail Server by infringing the security measures. In this case, the correct indictment would be: a crime of illegal access to a computer system with the intent of obtaining computer data, by infringing the security measures (Article 42 paragraph 3), and a crime of violating the secrecy of correspondence (Article 195 paragraph 1 Criminal Code), in ideal concurrence.

In all these situation and cases we introduced in the analysis the crime of violating the secrecy of correspondence (mentioned in and punished by Article 195 of the Criminal Code). Although, at a first glance, using just the legal provisions from Article 42 paragraphs 1, 2 or 3 of Law 161/2003 would be sufficient, we must note that the attention of the offender is rather pointed to a special category of computer data – those which represent electronic mail messages.

The legal practice demonstrated that, in most of the situations of illegal access, the offender acts with the intent of obtaining computer data, which could mean (in technical terms):

- visual caption of data on the screen;
- getting hold of a printout (printed document);
- running special software and applications (e.g. for administering databases in a organization, e-mail programmes etc.).

Obtaining computer data could also mean copying/pasting that data onto external storage media (Floppy disks, CDs, Memory Flash, Memory Stick, DVD, Card etc.). If only a copy action takes place, we could refer to the provisions of Article 42 paragraph 2 of Law 161/2003. But, if the offender transfers the data onto an external storage medium (in the sense of a migration, a movement of the data on the respective medium), the provisions of Article 44 of the law will be applied accordingly (those referring to the alteration of the data integrity), because the simple copy of data from the Hard Disk to external media cannot affect in any way the integrity of that data, while during the transfer or the migration of data, this could be relocated or even deleted.

Usually, the owners, beholders or users choose to protect their computer systems by security measures.

That protection could be *physical* (protecting the workstation by mechanical means with keys or ciphers, manual control of the power source etc.) or *logical* (using passwords, access codes or encryption processes).

Under the conditions of Article 42 paragraph 3, the offender will act on the computer system by infringing the security measures, but the real interest of the legislator is only in those protection measures which could directly affect the safety or the access to the system.
The attacks of the passwords are, historically speaking, preferred by the hackers approaching the network safety. At the beginning, the hackers tried to enter the networks by introducing so called login identifiers and passwords. They were trying passwords one by one until they got the real one. However, hackers realized that they had the possibility of writing down simple programmes to try breaching good passwords or to enter the systems. In general, those simple programmes were running a dictionary of words trying to get the genuine one. Thus, this kind of attacks rapidly became known as *dictionary-based attacks*. UNIX operating systems seem to be very vulnerable in front of dictionary-based attacks, because Unix does not reject automatically the one who repeatedly and unsuccessfully tries to enter the system, as compared to other Oss which make a certain user inactive following a fixed number of unsuccessful attempts of introducing passwords.

The local legal practice consists of various examples when hackers had success in using Unix-based services such as Telnet or File Transfer Protocol in order to get access to password files (from public areas of the system). Usually, the operating system encrypts the passwords within those files. However, because Unix codes the password file using the same algorithm (a mathematical function), a hacker could ignore the encoding of such a file by using certain applications or software from the Internet.

A special requirement for the existence of the crime is that the offender acts *without right* (see the definition and the explanations above).

Mens Rea

The crime of illegal access is committed with *direct or indirect intent*. In case of obtaining computer data (paragraph 2) *the intent is qualified by the aim*.

Forms

The preparatory acts, although possible, are not criminalised, thus not punished. Certain preparatory acts are incriminated as standalone offences, such as the case of Article 46 "Illegal operations with electronic devices and computer programs".

The attempt of the crime is punished according to the provisions of Article 47 of the law.

Criminal Proceedings

The criminal action starts *ex officio*.

3.3.3 Illegal Interception of Computer Data Transmission

Article 43 of Law 161/2003

(1) The unauthorised interception of a non-public transmission of computer data to, from or within a computer system is a criminal offence and is punished with imprisonment from 2 to 7 years.

(2) The same punishment shall sanction the unauthorised interception of an electromagnetic emission from a computer system carrying non-public computer data.

Protected Legal Interest

Is represented by the social relations related to telecommunications and computer communications, in general, and to non-public computer data transmissions, in particular.

Subjects of the offence

The Offender can be any natural person with criminal responsibility and liability for punishment. Generally speaking, this is a common request for all the cybercrimes. In this case, the offender must directly use certain types of electronic equipment specially designed for interception (eavesdropping) in the IT environment, and irrespective of the technical knowledge of the perpetrator. With other words, this could be the case of a State employee who has the task to intercept an electronic communication, but exceeds the limits of its authorization and illegally uses a software application which captures and recomposes IP packets in a network (thus getting hold of an electronic conversation), while he does not have a clue about the topology of the network, the routing of IP packages or even on how the application runs.

The involvement in the crime is possible in all known forms, the offender being principal, co-principal, instigator or accomplice.

The Victim will be the natural or legal person owner or beholder in any way of the computer system targeted (a simple workstation or an entire network) or of the link components (elements of the transmission) between two or more computer systems.
In addition, the secondary victim will be the beholder of the intercepted computer data or the person directly affected by the processing of such data.

The Materiality of the crime

Technically, interception means the action of capturing, by means of a specially designed electronic device or of a computer, the electric impulses, the variation of the electric potential (voltage) or electromagnetic emissions (radiations) which are present inside a computer system, come as an effect of its functioning or exist on the connection way between two or more computer systems.

Packet interception means one of the most difficult actions to be accomplished and is also a real threat to the electronic communications between the networks (LAN, Internet etc.). Each data packet sent over a network could transit a large number of workstations and other small networks before reaching its destination. By means of a *packet interceptor*, the hackers could intercept and capture the data packets (including those containing login messages, credit card information, email etc.) which travel between different locations within the network. After the interception of a packet, a hacker could then open it and take over the name of the host, the name of the user, as well as the password associated to it. The IT security experts called this package interception as *network snooping* or *promiscuous monitoring*.

Directly, the computer data interception could be achieved through the interaction of the offender with the external components of the computer system (cables, switches, routers, workstations etc.). For example, the communication between two workstations of a local network (LAN) belonging to an organization could be intercepted by an intruder after he makes some physical connections to the cables of the network, by cutting and inserting its own wires, and then being ready to "listen" to the traffic.

Indirectly or remotely, the interception could take the form of using specialized software applications (so called *Sniffers*) which are capable to monitor the package traffic in a network and save the data of interest in *log* files. Basically, the sniffers are used by the network administrators or Internet Service Providers (ISP) for traffic analysis or maintenance of the network. At the same time, such applications (or devices) are often used by the system administrators of certain institutions or organizations to monitor the communications channels (both internal and external) in order to discover any breach of security, leakage of sensitive information or even the misuse of the network resources (downloading forbidden software or applications, copyright infringements, exposing child pornographic materials etc.) or just for the management of the institution to have a clear view of what the employees are doing on the Internet or locally (LAN) while they are on duty.

Newly, the targets of the hackers are the Wireless networks (Wi-Fi networks or Hotspot Access Points), most of them being unprotected by encryption (although the IP Routers which offer Access Point Services have already implemented cryptographic solutions from the factory).

In order to discover what is inside a computer system (or network), the perpetrators have to their disposal another tool which manages to remain undetectable even by a Firewall, Antivirus programme or any other IT security application. It is about the capturing and decoding the sound made by the computer keyboard. So far, no such case was recorded.

Another powerful and sometimes undetected tool for the interception of computer data is the device or application called *keylogger.* Sometimes they are present as Adware or Spyware. This programme uploads automatically into the system when a certain webpage is visited. Their task is to record and send back to the sender (usually marketing and advertising companies, online commerce entities etc.) the online history, itinerary and Internet preferences of a user.

A keylogger programme is a very powerful tool, a specially designed application or electronic device, which logs (records) every key stroken by an user and then sends that information back to the person who previously has installed it. This type of programme (device) can extract very useful and sensitive information a user is writing down every moment, such as passwords, credit card numbers, classified documents, personal data, financial reports etc. The usage of keyloggers is at the medium scale in Romania, but it manifests both at the individual and organizational level.

In the same group of interception applications we can also include e-mail monitoring programmes, such as Websense, MIMEsweeper, FastTrack etc.

Paragraph 2 of the Article enlightens a new type of fulfilling the crime, by intercepting without right an electromagnetic emission from a computer system that stores non-public computer data. This means the caption of the compromising emanations (unintentional information-bearing signals which, if intercepted and analysed, may disclose the information transmitted, received or processed within the system) which can be easily found around every electrical device, in our case the computer system. Today, well known is the modern way in which interested persons can capture, by special means, those compromising emanations (radiations) existing for example round the screen of the targeted computer. Those captured data are "translated" into electric impulses and then in alphanumeric characters. The technology of preventing the interception of the compromising emanations is called TEMPEST (Transient ElectroMagnetic Pulse Emanation STandardizing) and is in the course of being implemented to

all civil and military institutions where sensitive or classified information is stored or processed by means of computer systems.

The main requirement for the existence of the crime is that the offender acts *without right*. The legal practice showed that the act is legitimate if the person who commits the interception:

- has the right to use the data comprised in the transmitted packages (the case of the owners or legal beholders of computer systems);
- acts based on a contract, following a legal order or with the consent of the participants to the correspondence (case of the system or network administrators, Internet Service Providers etc.);
- if the data is for private purpose;
- if, based on legal provisions, the electronic surveillance is authorized in the national security interest or to allow security services, law enforcement agencies or public prosecutors to bring forth offences or felonies (it is the case of state authorized agents who operate special monitoring devices and act lawfully).

Any other action besides those mentioned above or which exceeds the legal provisions will be automatically considered as illegal.

Mens Rea

The offence of illegal interception is only committed with *direct intent*. From the analysis of the material element of the crime comes the conclusion that it is almost impossible that the offender, foreseeing the result of his own action, captures and records the data packages of a electronic communication within a computer system without the intent to do so, just accepting the possibility of obtaining the result.

Forms

The preparatory acts, although possible, are not criminalized, thus not punished. Certain preparatory acts are incriminated as stand alone offences, such as those covered by Article 42 – illegal access to a computer system or Article 46 – illegal operations with devices and computer programs.

The attempt of this offence is punished according to Article 47 of the law.

Criminal Proceedings

The criminal action starts *ex officio*

3.3.4 Altering the Integrity of Computer Data

Article 44 of Law 161/2003

(1) The alteration, deletion or deterioration, without right, of computer data or the unauthorised restriction of access to such data, is a criminal offence and is punished with imprisonment from 2 to 7 years.

(2) The unauthorized transfer of data from a computer system is punished with imprisonment from 3 to 12 years.

(3) The same punishment as in paragraph 2 shall sanction the unauthorized transfer of data from a computer data storage media.

Protected Legal Interest

This is represented by the social relations arising in relation with computer data and information stored or travelled in a digital form. The protected legal interest will also be that of the owner or the legitimate beholder of the computer data targeted, because he (she) is the only person who can use effectively the respective information.

Subjects of the Offence

The Offender (author) could be any natural person who has criminal responsibility and is liable to punishment. Generally, as we have seen, the perpetrator is an IT&C knowledge-based individual, although there are situations when this capacity has no direct relevance.

The involvement in the crime is possible in all known forms, the offender being principal, co-principal, instigator or accomplice.

The Victim of the crime is the natural or legal person, owner or legitimate beholder of the altered, modified, transferred or restricted to access computer data.

The Materiality of the crime, in the case of the first paragraph, is achieved by multiple alternative acts of modifying, deleting or deterioring computer data, restricting the access to such data or transferring data without right.

All those acts shall have negative effects on the status of the data (in terms of integrity), especially as regards their capacity to have the meaning designed by the person who created or possesses them. Therefore, we have to eliminate from the analysis the possibility of the data being modified, altered or deleted with no direct consequences on their functionality or with a better outcome (a perfectionated new data with the same meaning/value or a programme perfectly compatible with the original one).

The modification consists of the action of the perpetrator who inputs new digital sequences (01001101 etc.) or deletes certain such digital sequences, having as outcome new computer data, entirely or partially different and with other value/meaning as compared to the original.

The deletion means the elimination (the whole or just parts) of the binary representation of the data stored on specific media such as Hard Disks, CDs, DVD, FloppyDisks, Memory Flash, Sticks etc., that drives inevitably to the vanishing of that data.

The deletion of data could be regarded as the equivalent of the destruction of goods. There could also be the case of alteration, destruction or making useless the media support of the data, the re-writing on the media (magnetic surface, optical disks, flash memory etc.). The deletion of the binary representation of data means the modification of the "0"and "1" values, which technically, is about the modification of the respective voltage values.

We shall note that the deletion of computer data does not automatically mean their definitive erasure. More often, the deletion of the data is the outcome of the sofware commands DELETE or FORMAT. In that case, the data – which is internally organized in files, continue to physically exist on the media (HardDiskDrive, Memory Flash etc.), but the operating system will mark those areas as "available" for future re-writing. Until the system occupies all those "free" locations with other data (in binary), the original/initial data (supposed to be deleted) could be retrieved. Although people usually consider that by means of the FORMAT

command, a disk (storage media) is actually formatted and the data vanishes, technically, this happens after executing nearly 7 such Format commands.

The deterioration means the alteration of the binary content of the computer data, by controlled or random insertions of „0" and „1" sequences, so the new sequence (Byte) cannot have a logical correspondent in reality.
In a far more serious way, the destruction of data could be the result of a damage caused to IT&C installations or facilities by elaborate terrorist acts or simple sabotage, as well as the deletion of data using powerful magnets or by running various specific destructive programmes, such as logical bombs.

There is a restriction of the access to data when the offender makes data disappear but not as a result of a DELETE or FORMAT command. The data is no more accessible to authorized persons and, consequently, are of no use.

Data access restriction could also be the result of various manoeuvres undertaken by the offender against the computer systems or storage media, in a way that the legitimate user cannot find them as in the original form or perform specific SEARCH processes. In the case of *physical restriction* the offender acts directly in order to block the access to the system resources by making the peripherals such as keyboard or mouse useless. In the case of *logical restriction*, the offender could modify the entries in the File Allocation Table (FAT) – a component of the operating system which assigns to each file one or more logical areas on the disk, memorizing the locations by specific addresses.

An example of data access restriction is the cyber attacks against the web pages, which make the sites unreadable or blocked, for all the category of users, even for the owner or legitimate beholder of data.

Unauthorized data transfer means the unauthorised movement of the binary representation of computer data from the current media storage to an external one, or within the same computer system but to another location.

The data migration from a computer system with a certain Hardware and Software configuration onto another one with a different configuration could determine a malfunctioning or the change in the original format of the data or of the format projected by the legitimate user. However, generally, this kind of incidents is accidental and refers to the professionalism of the person who performs the migration than an eventual criminal activity or attempt.

The relocation of data could have a significant impact on the integrity of computer data. It is the case of *relational databases*, where the final information is structured following a specific logical order and, at the physical level data are retrieved depending on their location on the storage media and using well defined algorithms. An eventual relocation of such data could provoke data misidentification with effect on the final data integrity in the way the legitimate user expects to find them.

The respective legal practice shows that the most dangerous tools that affect computer data are programmes like Viruses, Worms or Trojan Horses, which have the capacity of reproducing and run in other programmes, applications or data files as destruction software.

The basic condition for the existence of the offence is that the offender acts *without right*.

Case Study:

On 01.09.2003, mass-media reported that a new virus was launched and was spreading fast in Romania. Based on this information, local IT company Softwin, specialized in antivirus programmes, succeeded in identifying the source of the virus and further noticed the Combating Organized Crime and Antidrug General Division of the General Inspectorate of Police.

The specific investigation showed that a young Romanian, CD, 25 years old, a Master student with the Hydrotechnics Faculty, Iasi University, downloaded a virus from the Internet and modified it, by introducing a text in Romanian with a defamatory content related to one of his professors and the faculty, then spreading it within the faculty LAN.

The search and seizure procedure at the student's home produced computer systems, Floppy Disks, CDs, as well as documents. Police officers in charge made specific cyberforensic investigations of the systems seized and of the

faculty's systems, which led to the identification of relevant criminal evidence with reference to the criminal activity of the accused.

Mens Rea

The offence of altering the integrity of computer data is done with *direct or indirect intent*.
In most of the cases, the offender intends to format/damage. The intent of getting an illegal profit is not necessary and is not typical to this form of criminal behaviour. There is a possibility, however, for a specific but indirect motivation to harm someone.

The legal practice demonstrated that, in many cases, computer data damages are motivated by the desire for revenge of a certain frustrated employee. Political, as well as ideological motivations could also be taken into consideration, especially when the act comes in the form of terrorism (cyber terrorism). And finally, this intention to draw the attention of the large public or of certain institutions is not seldom.

Forms

The preparatory acts, although possible, are not criminalized, thus not punished. Certain preparatory acts are incriminated as standalone offences, such as those mentioned by Article 42 – illegal access to a computer system or Article 46 – illegal operations with devices and computer programs.

The attempt of this offence is punished, according to Article 47 of the law.

The crime is considered as being committed when the offender modified, deleted or deteriorated in any way the computer data in a system or managed to restrict de access of the legitimate users to such data or succeeded the illegal transfer of the binary representation of data from the system/storage media.

Criminal Proceedings

The criminal action starts *ex officio*.

3.3.5 Computer System Interference

Article 45 of Law 161/2003

The act of causing, without right, a serious hindering of the functioning of a computer system by inputting, transmitting, altering, deleting or deteriorating computer data or by restricting the access to such data is a criminal offence and is punished with imprisonment from 3 to 15 years.

The Protected Legal Interest consists in the good (normal) functioning of the computer systems in the society and their reliability in terms of the social need they have been implemented for.

Subjects of the Crime

The Offender (author) could be any person with criminal responsibility and liability for punishment (in the sense of the already made assumptions).
The involvement in the crime is possible in all known forms, the offender being principal, co-principal, instigator or accomplice.

The Victim is the natural or legal person owner or legitimate beholder of the computer system the functionality of which has been hindered.

The Materiality of the crime is achieved by any form of a serious hindering of a computer system normal functioning. The legal provisions also mention the type of the acts – *inputting, transmitting, modifying, deleting, deteriorating* or *access restriction to computer data*.

Inputting computer data. Data can be directly input from the keyboard or by transfer from an external storage media. From the keyboard (or mouse), the offender can access certain reserved areas of the system, such as BIOS – Basic Input Output System which controls the Central Processing Unit activity, or the operating system.

Wrong data can progressively attack and hinder the functioning of other components, especially in the case of a network. This can be the case of a computer system operator who controls the activity of a hydro power plant, inputting from the keyboard various parameters which are wrongfully understood and misinterpreted by the software application, with a

damaging outcome: chaotic functioning of the entire plant or even blocking of certain processing elements.

The transmission of computer data is done remotely, using the facilities offered by the connection of the system targeted to a computer network (LAN, WAN, W-LAN etc.).
Often, it is the case of inputting or downloading viruses, worms or Trojan horses into the system. The transmission could be achieved by:

- the transfer (copy) into the targeted system of the infected files or programmes from external storage media;
- the transmission/reception of email messages with infected attachments;
- downloading malicious code-bearing files and programmes from the Internet or un-trusted senders.

Most often it is the case of the person who, regardless of his (her) motive, sends over the Internet a large amount of messages (possibly without dangerous payload) towards a certain computer system or network, overloading data ports and thus blocking its access to exterior.

An example is the Denial of Service (DoS) attack, when a resource on the Internet, such as a server or a website, doesn't work normally because a group of people launch a co-ordinated attack which overloaded the targeted system with so many false requests that cause the breakdown of the system. The most common DoS attack has as outcome preventing users to access a certain website, which could lead to possible financial losses for the owner of the site (if the site is the interface for an electronic commerce company).

Another way an attacker could takeover the control of a computer system is by inputting malicious applications through a Mobile Code. This is a special category of code (written in Java, JavaScript or ActiveX) implemented in HTML-based documents. Whenever the user's browser uploads the specific webpage, the hidden mobile code is downloaded automatically and executed.

The basic condition for the above mentioned acts to be considered as crimes is that they have been committed *without right*. For example, the person who, based on a contract, executes an

Ethical Hacking operation which means some „hacking procedures" in order to assess the vulnerabilities of a network, possibly causing a hindering of the respective system during the process, will act lawfully.

We also have to clarify the term „serious" with reference to the offence itself. This is not mentioned in the legal provision we analyse, but somehow let to the decision of the prosecutors and judges to evaluate the value of the damage and the level of the threat to society. We appreciate that the distinction could be made taking into account the importance of the computer system to the social life (for example: the computer network of 112 Unique National Emergency System is vital to the society whereas a certain Local Area Network of a school isn't).

Mens Rea

The offence of system interference could be committed with direct or indirect intent. Often, the difference between these two forms of guilt is made by the nature of the data input, transmitted, modified, deleted, deteriorated or restricted to access.

For example, there could be direct intent in the case of an employee from an organization, who, during a break, sends to all his colleagues a non-offensive joke as an e-mail message, but having attached to it an infected file or a virus. Technically speaking, the outcome of such an action would be a temporary blockage of the internal mail service and thus a hindering of the Mail Server functioning in the entire organization, result foreseen and accepted by the would-be offender.

Forms

The preparatory acts, although possible, are not criminalized and thus not punished. Certain preparatory acts are incriminated as stand alone offences, as by Article 42 – illegal access to a computer system, Article 43 – illegal interception of a computer data transmission or Article 46 – illegal operations with devices and programmes.

The attempt of the offence is punished, according to Article 47 of the law.

The offence is considered as being fulfilled when the targeted computer system shows the very first signs of weakness, malfunctioning or blocking. If those signs are not present, we can consider the offender as doing preparatory acts or committing other offences (e.g. illegal access, altering the integrity of data etc.).

Criminal Proceedings

The criminal action starts *ex officio*.

3.3.6 Illegal Operations with Devices and Computer Programs

Article 46 of Law 161/2003

(1) It is a criminal offence and shall be punished with imprisonment from 1 to 6 years:

a) the production, sale, import, distribution or making available, in any other form, without right, of a device or a computer program designed or adapted for the purpose of committing any of the offences mentioned by Articles 42 to 45;

b) the production, sale, import, distribution or making available, in any form, without right, of a password, access code or other such computer data allowing total or partial access to a computer system for the purpose of committing any of the offences mentioned in Articles 42 to 45;

(2) The same punishment shall sanction the unauthorised possession, of a device, computer program, password, access code or any other computer data, referred to in paragraph (1) for the purpose of committing any of the offences mentioned in Articles 42 to 45.

The Protected Legal Interest is represented by the social relations related to the confidence in computer data, devices and programmes, in the sense of correct and legitimate use, as well as to the correct and legitimate development of the associated commercial operations.

The Subjects of the Offence

The Offender (author) could be any person with criminal responsibility and liability for punishment.

The involvement in the crime is possible in all known forms, the offender being principal, co-principal, instigator or accomplice.

The Victim of the offence is the natural or legal person owner or legitimate beholder of the computer system, possibly targeted by the cyber offences mentioned above (Articles 42-45), as well as the owner or beholder of the copyright for the modified or adapted hardware and software products, with criminal intent. A victim will also be the natural or legal person legitimate beholder (and not necessarily the owner) of the passwords, access codes or any of such computer data which have been used, without right, to grant the access to a computer system.

The Materiality of the offence is represented by the action of producing, selling, importing, distributing or making available of one or more devices or computer programs, special designed or adapted with the purpose of committing any of the cyber offences mentioned above.

The production of an electronic device means carrying out some technical activities by which certain electronic components are combined and interconnected so that the new product may (directly or remotely) interact with a computer system or become a part of it. For example, the fabrication of a device capable of packets interception of a transmission between two or more workstations.

The creation of a computer program means the elaboration of a logical algorithm based on the requested purpose and the translation of the instructions into a programming language (machine code – such Assembler, or higher level language - C++, Pascal, Visual Basic, Java etc.) in order to be „understood", correctly interpreted and processed by the targeted machine (computer system). An example could be the creation, with the help of Borland C++ programming language, of a programme which, under execution, grants the access to the computer system resources or to the whole network to an unauthorized person by bypassing the username and password operation. As we have already seen, the most dangerous programmes are those generating viruses, worms, Trojan horses or „logical bombs".

The legislator's intention is also that of criminalizing the action of the person who, although does not have any implication in the creation of the device or programme, *imports* it, *distributes* it or *makes it available* to the offender who directly acts against the system.

At the same time, the producing, selling, importing, distribution and availability to unauthorized persons of the passwords, access codes or any other data which grant total or partial access to a computer system will be punished

Mens Rea

The illegal operations with devices and computer programs are committed with direct intent, according to the offender's aim. Thus, the acts described in paragraphs (1) and (2) will be performed entirely for the purpose of committing the cyber offences covered by Article 42-45.

Forms

The preparatory acts, although possible, are not criminalized and thus not punished.

We note that the acts incriminated in Article 46 paragraph (1) letters a) to c) could be considered as preparatory acts for the offences in Articles 42 to 45, but the Romanian legislator chose to criminalize them separately.

The attempt of the offence will be punished, according to Article 47 of the law.

The offence is regarded as being fulfilled in the very first moment of producing, selling, importing, distribution, making available or possessing, without right, a device, programme, password, access code or any other type of data with the purpose of committing the cyber offences mentioned in Articles 42 to 45.

Criminal Proceedings

The criminal action starts *ex officio*.

3.3.7 Computer-Related Forgery

The unauthorised input, alteration or deletion of computer data or the unauthorised restriction of the access to such data, resulting in untrue data with the purpose to be used in obtaining a legal advantage, is a criminal offence and is punished with imprisonment from 2 to 7 years.

The Protected Legal Interest is refers to the social relations related to the public trust in the safety and reliability of computer systems, to the validity and authenticity of computer data, and

the whole modern automatic way of officially or privately processing, storing and transacting computer data.

Subjects of the Offence

The Offender can be any natural person with criminal responsibility and liability for punishment.

However, generally, this kind of offences is achieved by initiates in IT&C science or by people who, by the nature of their duty/job, have access to computer systems and data.
The involvement in the crime is possible in all known forms, the offender being principal, co-principal, instigator or accomplice.

The Victim

In the case of this offence, the victim is the natural or legal person who suffered a legal or (patrimonial, moral or social) interest harm following a counterfeit (forgery) of the data belonging to him (her).

A secondary type of victim is the owner, legitimate beholder or authorized user of the computer system.

The Materiality of the crime is achieved by an alternative action of inputting, modifying or deleting computer data or restricting the access to such data. Note: these situations have already been addressed in the analysis of the "altering the integrity of computer data" offence.
The acts by which the material element of the offence is achieved have negative effects on the status of the data, in what regards their capacity of properly functioning and certifying facts or situations in the manner designed by the person who created or manage them. This is similar to fabricating false documents or forging some true ones.
As an example, computer-related forgery could be achieved as follows:

- by inputting, altering (modifying) or deleting the data from certain database fields of a Centre for Personal Records, Police, banks, insurance companies etc. – through the offender's direct action on the keyboard or by transferring data from an external storage media;

- altering the electronic form of documents, by the modification or direct deletion of words, figures etc. resulting in new documents but with another legal value.

From the legal practice, we learned that computer-related forgery could take one of the following forms:

- E-mail Spoofing;
- Hyperconnections Spoofing;
- Web Spoofing.

The most encountered methods of achieving computer forgery in the Romanian legal practice are Hyperconnections Spoofing and Web Spoofing. Ingeniously used along with the social engineering, these methods are very well known in the cyberspace as „PHISHING attacks". What is interesting is that the primary victims of these attacks are not the organizations or financial institutions, but the Internet users who, due to their ignorance or lack of knowledge, fall in the trap of these scams and provide their personal, financial as well as confidential data to unknown individuals.

Case Study:

In March 2007, the local authorities learned that in Constanta County a criminal group was running illegal activities with regard to financial operations, using counterfeited (forged) electronic payment instruments and personal data belonging to other persons, the amount of money being retrieved from Western Union payment system. Later on, in April 2007, a financial institution reported to the law enforcement agencies that it had been under Phishing attack.

The police surveillance upon the group revealed that the individuals were specialized in committing cybercrimes and had advanced IT knowledge.

The investigation further established that the data used in the illegal financial transactions or necessary for re-writing of the blank cards had been obtained through Phishing attacks against certain foreign financial institutions and their clients. After the offenders created the spoofed web pages of those banks and hosted them on controlled servers, they usually transmitted fake e-mail messages to different users (clients), containing notices or warnings apparently from the security admins of the institutions about the cancellation or restriction of the respective clients to their own account. In order to get back the initial status of the account, clients were urged to access a certain link and fill in an electronic form with all the requested data (full name, card number, account

number, card expiry date, PIN code etc.). Once the form validated, it has been transmitted automatically to an e-mail address special created for the criminal activity. The data related to clients and their payment instruments thus collected have further been used to buy online service, such as: hosting, domain names, phone services, objects, transferring money through Western Union or forging blank cards (by re-writing the magnetic strip on the back) with the purpose to withdraw cash from ATMs.

The total economic prejudice caused by the related offences amounted to 60 000 USD.

The dismantling of the group and the apprehension of the offenders was the result of the co-operation between the US Justice Department with the help of the Federal Bureau of Investigations (by its attaché in Bucharest), along with Romanian police officers from Combating Organized Crime and Antidrug General Division.

Mens Rea

Computer-related forgery is committed only with *direct intent*, due to its illegal purpose.
In the case of inputting, altering or deleting computer data, there will be an offence even if the offender altered the content of the data with a "legitimate" purpose (for example, in order to create a legal evidence in course of a real judicial situation). There is also no need to effectively use that forged data, but only to get them tin order o further achieve the criminal aim.

The offender's purpose is to use the obtained forged data in order to produce a legal advantage (interest). In this case, data are supposed to produce the legal advantage only if they are capable to initiate, modify or terminate legal relations, by creating another legal rights and obligations.

Forms

Preparatory acts, although possible, are not criminalized and thus not punished.
The attempt to this offence is punished, according to Article 50 of the law.

Criminal Proceedings

The criminal action starts *ex officio*.

3.3.8 Computer-Related Fraud

Article 49 of Law 161/2003

Causing loss of property to another person by inputting, altering or deleting computer data, by restricting the access to such data, in any way, or by any interference with the functioning of a computer system with the intent of obtaining an economic benefit for oneself or for another is a criminal offence and shall be punished with imprisonment from 3 to 12 years.

The Protected Legal Interest consists of the social relations safeguarding one person's property, when the presence of that person in the cyberspace is quantifiable in a certain volume of data stored in a computer system or transmitted within a network.

Subjects of the Offence

The Offender (author) could be any person with criminal responsibilities and liability for punishment. Fraudulent acts of this type are, like in the situations above, usually achieved by initiates in informatics or by persons who, by the nature of their activity, have access to data and computer systems.

The involvement in the crime is possible in all known forms, the offender being principal, co-principal, instigator or accomplice.

The Victim will be the person whose property or economic interest was harmed by the action of the offender. In this case, there is also a secondary victim – the owner, legitimate beholder or user of the computer system.

The Materiality of the offence is achieved by alternative actions of inputting, altering or deleting computer data, of restricting the access to such data or of interfering in any way with the proper functioning of a computer system.

"Interference with the functioning of a computer system" means any act or action taken in order to prevent the system from properly and normally, partially or totally, temporary or permanently functioning,. For example, at a certain date and time, the offender enters and hinders the Stock Exchange computer network paralysing the electronic financial transactions and thus causing serious harm to businesses and the companies during the selling-buying process.

In the cyberspace environment, computer-related fraud can take various forms and usually can be mixed-up with the traditional criminal offence of fraud.

Case Study:

In July 2008, the prosecutors from the Direction for the Investigation of Organized Crime and Terrorism – County Office Valcea, along with specialized police officers from the General Division for Combating Organized Crime and Antidrug, have undertaken 34 domiciliary search and seizure actions in various locations of Rm Valcea, Dragasani, Bucharest, Alexandria, Sibiu and Hunedoara.

Following those search and seizure actions against 26 offenders, numerous goods have been identified in connection with the case, such as: laptops, PC units, HDDs, mobile phones, memory flashes, modems, SIM cards, receivers, switches and a large amount of money in local and foreign currency.

The modus operandi of the group members was that of posting selling advertisings for goods they did not have in possession on specialized electronic commerce websites, like eBay.com, Equine.com or Craigslist.com.

The access to those websites was done using identification and other data of other persons, including data related to credit cards belonging to these persons, information that had been obtained beforehand through special designed e-mail messages luring them to unveil and communicate personal data (Phishing).

Data obtained this way were then used to illegally login onto those electronic commerce websites.

By the selling adverts, the offenders determined many victims to acquire (buy) those inexistent goods and to make the payment through fast money transfer systems like Western Union and MoneyGram or through cash deposits in accounts opened in false names. All these false names were then used to withdraw the money from the victims.

The amount of money resulted from this criminal activity was sent back home, in Romania, with the help of fast financial transactions services and using a false sender identity and true receiver one, with some similarities with the purpose to falsely create de idea of a transaction between family members.

Mens Rea

Computer-related fraud is committed only with *direct intent*, due to its illegal purpose. The offence is also committed with the intent of obtaining an economic benefit for oneself or another.

For the existence of the guilt of this offence is not necessary for the prejudice or loss to be effectively created, but to exist as a possibility sought for by the offender.

Forms

The preparatory acts, although possible, are not criminalized, thus not punished.

The attempt to this offence is punished, according to Article 50 of the law. In this case, usually, there is no attempt to computer-related fraud, but the stand alone offence of computer-related forgery.

Criminal Proceedings

The criminal action starts *ex officio*.

3.3.9 Child Pornography through Computer Systems

Article 51 of Law 161/2003

(1) It is a criminal offence and shall be punished with imprisonment from 3 to 12 years the production with the purpose of distributing, offering or making available, disseminating or transmitting, procuring for oneself or another child pornography material through a computer system, or the unauthorised possession of child pornography material in a computer system or computer data storage media.

(2) The attempt to this offence shall be punished.

The Protected Legal Interest consists of the social relations established with regard to the protection of the minors.

According to Article 35 item 2 letter i) of Law 161/2003, *pornographic materials with minors* means any *material presenting a minor with an explicit sexual behaviour or an adult person presented as a minor with an explicit sexual behaviour or images which, although they do not present a real person, simulates in a credible way a minor with a explicit sexual behaviour.* Article 35 also uses the term "images" which, although

does not depict a real person, simulate in a credible way a minor with an explicit sexual behaviour, and therefore we consider that the audio recordings could not be regarded as "pornographic materials with minors" in the absence of the respective video attachments.

In defining the term "pornographic materials with minors" there are references to an *explicit sexual behaviour*. This behaviour could easily mean a sexual position as well as a sexual intercourse or any other attitude which could be interpreted as a sexual behaviour. The behaviour has to be *explicit*, so it has to come out directly from the image presented, not in the form of suggestions or possible interpretations of someone's own imagination. A minor's sexual behaviour has also to be clearly depicted in the respective material for the offence to exist. It must be noted that a picture a writing or a photo should only be considered as pornographic if "decadent" details are deliberately used to emphasize an obscene character and in order to open the way to pornography or bents for sexual abnormalities.

Subjects of the Offence

The Offender (author) could be any person with criminal responsibility and liability for punishment.

In the case of producing materials with the purpose of distribution, the offenders are all the individuals who took part, at different stages, in the elaboration or making of pornographic materials with minors, even those adults who acted as minors (models/actors in photo shootings, film makings etc.).

The involvement in the crime is possible in all known forms, the offender being principal, co-principal, instigator or accomplice.

The Victim is the minor whose pornographic situations have been recorded, stored or transmitted by means of computer systems. In some cases, however, there will be no victim, just the trespassing of the law.

The Materiality of the crime is achieved by multiple execution acts, such as:

- producing with the purpose for distributing;

- offering;
- making available;
- disseminating;
- transmitting;
- procuring for oneself or another (the pornographic materials with minors);
- possessing, without right, pornographic materials with minors in a computer system or in a computer data storage media.

The production with the purpose of distributing of pornographic materials with minors implies the confectioning, extracting and combining of those materials. For the existence of the crime in this case, these materials have to have been produced with the intent to be distributed. If the intent was not the distribution, but for one's own private purpose, those acts will not be considered as material element of the respective offence. In this case, there will be the offence but under the circumstances of the unauthorised possession of pornographic materials with minors.

Offering pornographic materials with minors means the offender shows or presents the respective materials to someone else.

Making available pornographic materials with minors means to give someone else access, in any way, against an economic benefit or for free, to such materials or to grant to those persons the possibility of using the materials.

The distribution of pornographic materials with minors takes place whenever such materials are broadcasted or disseminated in any way to the requesting people or to amateurs. Whether the person who distributes the materials is the same with the one who produced them or another individual is irrelevant. It must be noted that the act of making such materials public, with or without any economic purpose, will be an offence, in the sense of distributing pornographic materials with minors. In this case of distribution of pornographic materials, we consider there are multiple acts of transmitting, which could eventually occur at the same time or successively. The action of *transmitting* the materials, in terms of the law, implies electronically sending or delivering objects (video files, digital photos etc.) containing pornographic images with minors.

Procuring for oneself or another consists of any act by means of which a person obtains the pornographic materials with minors (through buying, renting, receiving in custody etc.).

The unauthorised possession of pornographic materials with minors simply represents the situation of a person having, owning, beholding, holding or keeping them in any way, against the law. *Per a contrario*, the legitimate possession (for example in the case of a prosecutor or police officer investigating the offence) eliminates the criminal responsibility.

For the existence of the offence the criminalized acts must be related to pornographic materials with minors. Without this condition, there will be no content of the crime, and thus no material element of the related offence.

Mens Rea is characterized by both *direct and indirect intent*.

Forms

The preparatory acts, although possible, are not criminalized, and thus not punished.

The attempt to this offence shall by punished according to paragraph (2) of the article, but the legal provision does not specify the nature and the period of the punishment.

Criminal Proceedings

The criminal action starts *ex officio.*

3.3.10 Forging Electronic Payment Instruments

Art. 24 of Law 365/2002

Forging an electronic payment instrument is punished with imprisonment from 3 to 12 years and the denial of certain rights.

The same punishment is used to sanction the issuing into circulation, in any way, of forged electronic payment instruments or their possession with the intention to put them into circulation.

The punishment is imprisonment from 5 to 15 years and the denial of certain rights if the acts stipulated in paragraph (1) and (2) are performed by a person who, by reason of his (her) job attributions:

- performs technical operations necessary to issue the electronic payment instruments and to carry out the types of operations stipulated art. 1 item 10 or
- has access to security mechanisms involved in issuing or using electronic payment instruments, or
- has access to identification data or security mechanisms involved in carrying out the types of operations stipulated in art. 1 item 10

The Protected Legal Interest refers to the entire social relationships referring to the public trust (*fides publica*) in the safety and reliability of the electronic payment instruments, to the validity and authenticity of computer data, to the entire processing, storing and automatic transaction process of data and values.

The protected legal interest is also that of the owner of the forged electronic payment instruments issuer, financial institution etc.), of the owner or rightful user of the respective electronic means, identified by the identification computer data stored or circulated in the issuer's computer system as well as the accepting trader or bank.

The Subjects of the Offence

The Offender

It can be any legally responsible person – case of paragraph (1) and (2). The legal practice has demonstrated that, in most of the cases, such persons have knowledge of information technology. Amongst these, a significant percentage is represented by experts in computing systems and networks, familiar with "breaking" the security measures of computers or computer systems.

In terms of paragraph (3), the offender has to be employed by the issuing financial institution or in a contractual relationship with it, and, by reason of his (her) job attributions has to be involved in technical or financial operations with electronic payment instruments (issuing cards, configuring identification data, establishing security measures etc.).

The participation is possible in all its forms: principal, co-principal, instigation or complicity.

The Victim

It is a natural person rightfully owning the forged electronic payment instrument or the identification computer data.

There is also a secondary passive subject which is the legal person owning the electronic payment instrument (the issuing financial institution respectively), the accepting trader or bank.

The Materiality of the crime

In terms of paragraph (1), it is achieved by forging an electronic payment instrument. According to the criminal code theory, forgery is in general achieved either by an *alteration*, or a *counter faking* of a certain object.

In its simplest form, forging an electronic payment instruments means *an interaction of the offender with black cards* by means of equipment specially meant for card configuration.

A very tough problem for attorneys is to obtain the necessary data for the configuration (forgery) of the electronic payment instrument, case when the offender will try a rage range of technical procedures such as attack by social engineering or attack by using hand-made devices imitating standard locations where electronic payment instruments are used (skimming) etc.

An attack by *social engineering* is mostly based on the users' ignorance regarding computers and information society. Most often, the social engineering attack is done by means of an information infringement (information forgery), PHISHING variant. The best recipe against these attacks is the users' education.

Once the necessary personal or financial data obtained, the offender will proceed to the manufacturing of the electronic payment instrument.

SKIMMING occurs most often amongst the displeased employees of financial institutions or those willing to get illicit gains or accepting traders. However, the most targeted places are bars

and restaurants where the clients choose to pay the services or products with bank cards and, out of commodity, give the cards to the serving personnel to process the transaction.

In some cases, the skimmer creates special devices imitating the interface of ATMs that he attaches to them in order to capture (register, obtain, copy) the identification data of the cards introduced by the users. These devices are accompanied by mini-video cameras that will record the introduction of the PINs of the respective cards.

The legal practice has also shown that the forgery of an electronic payment instrument cannot take the form of *alteration* as any modification brought to the object makes it unusable and therefore there is no case of infringement.

Counterfeiting means the manufacture, production or imitation of an electronic payment instrument. Whether the imitation is perfect or bad has no relevance as it is enough to circulate and interact with the targeted computer systems.

Counterfeiting (forgery) involves the use of devices especially conceived, similar to those used by the issuing financial institutions which impress on the card magnetic strip or store on a microchip the necessary information to create the authenticity impression so that the forgery may be accepted in the network of the financial institutions or accepting traders..

In order to achieve the material element of the infringement stipulated by (1), the forgeries achieved must have circulation power meaning they have to imitate or impersonate the electronic payment instruments on the market under the conditions of NBR Regulation no.4 of 2002, by observing at the same time the validity conditions.

As provided by paragraph 2, the offender will act to put into circulation a forged electronic payment instrument or will possess the respective forged electronic payment instruments I view of putting them into circulation.

Putting into circulation means the introduction (no matter for how long) into the economical-financial-monetary circuit of forged electronic payment instruments fulfilling the same economical functions as the real ones. The introduction into the economical circuit has the

cumulative purpose of passing the forged instrument from the offender to at least another person, the trading or making the forged instrument available to third parties.

Possessing forged electronic payment instruments will mean to receive or keep them with a view of putting them into circulation.

In case of possession, the law also imposes a second requirement that the possession should have as purpose putting the instruments into circulation. The lack of this essential requirement will remove the criminal character of the possession act, but will trigger the offender's criminal responsibility if the other elements of favouring (art. 264 Criminal Code) or concealing (art. 221 Criminal Code), the offence, as appropriated.

Paragraph (3), art.24, Law 365/2002 reveals an interesting situation from the point of view of the offender's quality. This one is an employee of a financial institution in charge with issuing electronic payment instruments or is in contractual relationship with one and his (her) job attributions include technical operation or the operations necessary for issuing cards or administrates financial transactions that are specific to this type of information society services. Basically, the offender will use the same above mentioned forgery methods but from a clearly superior position, being already in possession of the data (information) referring to the identity of the person whose electronic payment instrument is to be forged, the targeted bank account, the instrument identification name etc.

Case Study:

The prosecutors of the Direction for the Investigation of Organized Crime and Terrorism (DIOCT) – Suceava county office – have initiated the legal action and issued the 24h retaining warrants for the accused C. N., N. D – A and L. A – M, both from Constanţa county, investigated, together with other 8 persons, in a criminal file for the creation of a organised criminal group with the purpose to commit defraud with very serious consequences

De facto, the offenders C. N. and N. D – A were charges for having, starting with May 2007, contracted bank credits with forged documents, having manufactured and possessed equipment to forge electronic payment instruments and for having forged electronic payment instruments, acts committed as principal authors, but also as instigators and accomplices, the damage being presently estimated at ROL 2.5 billion. Also, by the evidence in the file, a first evaluation was made for the damage caused by committing the cyber offences, which reached 7500 euro.

The third offender, L. A – M, is accused of complicity to fraud with very serious consequences and document forgery, having solicited several persons and forged documents to fraudulently obtain bank credits, also involving in this sense SC SMART CONCEPT SRL Constanta, the company where he is an administrator and associate.

The criminal file was built in August 2007, following a disjunction from another case under the investigation of DIOCT prosecutors, were carried out for the offence of human traffic and cybercrime for which the offenders were imprisoned before trial.

In the disjunctive case, on the basis of a residence search mandated by the court, DIOCT prosecutors, together with officers form the Brigade for Combating Organised Crime and Anti-drug from Suceava and Constanța counties searched 12 residence addresses of the offenders and the defendants from where they seized a series of preparatory papers for the forgery of documents used to cheat banks as well as card cloning devices.

Mens rea

The offence of forging electronic payment instruments is committed with *direct* or *indirect intention* (for any of the causes stipulate by paragraphs 1, 2 or 3).

Forms

The preparation acts, although possible, are not incriminating and therefore not punished (see Skimming).

Certain preparatory acts can be incriminated as stand alone , such as the case of art.46 "Illegal operations with computer devices or programmes" (under certain conditions) or art.49 "Computer fraud" of Law 161/2003.

As regarding the "identify theft", this is more of a concept because, presently, there is no incriminating norm for it although it is stringently necessary.
The attempt is punished in terms of the provisions of paragraph (4) of the same article.

Criminal proceedings

The criminal action starts *ex officio*.

3.3.11 Possession of Equipment with a View of Forging Electronic Payment Instruments

Art. 25 of Law 365/2002

Manufacturing or possessing equipment, including hardware or software, with the view to forge electronic payment instruments is punished with imprisonment from 6 months to 5 years.

The Protected Legal Interest

It refers to the social relations related to the public trust in the safety and reliability of electronic payment instruments.

The Subjects of the Offence

The Offender can be any natural person with criminal responsibility and liability for punishment.

The legal person will be legally charged for the offences brought while performing its activities or in its interest if the act has been performed with the form of guilt as stipulated by the law.
The involvement is possible in all its forms: principal, co-principal, instigator or accomplice.

The Victim

The Victim will be the bank, credit or financial institution or authorised entity which, according to the legal provisions, issues electronic payment instruments or performs financial operations by means of these.

The Materiality of the crime consists in the manufacturing or possession of pieces of (hardware or software) for the purpose shown by the law.

In this context we are dealing with preparatory activities for the offences covered by art. 24, incriminated however as autonomous offences having in view the high social risk they cause.

Manufacturing implies to produce instruments in any way or to perform the proper operations in order to obtain electronic or electromagnetic devices or computer applications necessary for the forgery of electronic payment instruments.

Possession implies keeping, receiving, hiding or transporting the equipment necessary for forgery activities.

An essential requirement in order to have an offence is that the equipment created, manufactured or possessed with a view of forging electronic payment instruments should be technically able to be used for forgery activities.

Mens rea

The offence of forging electronic payment instruments is committed with direct intention, due to its illegal purpose.

If the created, manufactured or possessed equipment (applications) is used for the forgery of electronic payment instruments, in other words, if the purpose intended by the offender is achieved, there is a concurrence of offences and the criminal charging will be established for the manufacturing or possession of equipment in for the forgery as well as for the forgery activity it self.

Forms

The offence can cover all the forms of an intentional activity that is, preparatory acts, attempt, consumption, completion, the text incriminating only the consumption and completion forms.

Criminal proceedings

The criminal action starts *ex officio*.

3.3.12 Misrepresentation with a View of Issuing or Using Electronic Payment Instruments

Art. 26 of Law 365/2002

The untruthful declaration to a bank, credit or financial institution or any other legal person authorised by the law to issue electronic payment instruments or to accept the types of operations covered by art.1, item 10, in order to issue or use an electronic payment instrument, for himself (herself) or somebody else when, according to the law or circumstances, the

declaration is used to issue or use an electronic payment instrument, is punished by imprisonment from 3 months to 2 years or a fine.

The Protected Legal Interest

It refers to the social relations related to the trust in the declarations made in front of the bank, credit or financial institutions authorised to issue or administrate electronic payment instruments, declarations that may cause legal or economical consequences

The Subjects of the Offence

The Offender

Can be any natural person fulfilling the legal conditions and who is entitled to give the declaration or has the capacity to make declarations with legal consequences.
The offender can also be a legal person when the act was committed in its name or interest, by its bodies or representatives.

The involvement is possible in all its forms: principal, co-principal, instigator or accomplice.

The Victim

Will be the natural or legal person whose legal or financial interests have been damaged by the committed offence.

There will also be e secondary victim, the legal person owning the electronic payment instrument (the issuing financial institution respectively).

The Materiality of the crime consists in the declaration action which, entirely or partially, is untrue.

The declaration can be made at the author's initiative (who intends to obtain an electronic payment instrument) or at the request of the financial institution (as a standard procedure necessary for the issuing of electronic payment instrument), generally in writing and directly, in Romanian or, eventually, in of EU official languages.

If the declaration implies a certain procedure or certain conditions related to the way in which such a declaration is given, the non-observance of such requirements might exclude the applicability of cruminal legal provisions.

An essential requirement for an offence is that the declaration should be given to a bank, credit or financial institution or any other legal person authorised by the law to issue electronic payment instruments.

In terms of the law or circumstances, the declaration must also be able to cause the legal or economical consequences the offenders look for. If the false declaration cannot serve to cause consequences or is withdrawn or retracted before being processed, the act will not be considered an offence.

An example is the account takeover (getting possession of someone else's bank account). The offender will obtain enough personal data regarding a certain person (by previously getting invoices, bills, copies of receipts from card payments etc.) and then will impersonate the respective person (assumes the person's identity) in the (indirect for safety) relation with the financial institution. Under a certain pretext, the offender asks the bank to deliver all electronic communication to an e-mail address that is exclusively under his (her) control and, eventually even mentions a change of residence. Later on, he (she) announces the loss of the card and requires the issuing of a new one to the new address. Unfortunately, there are many bank, credit or financial institutions in the world which, as part of the information society services or out of concern for their clients, send the electronic payment instruments by courier, making them very accessible for offenders.

Mens rea

The forgery of electronic payment instruments is committed with *direct intention,* due to its legal purpose (the purpose does not need to be achieved).

Forms

The offence is susceptible of covering the preparation, attempt and consumption phases.
The preparatory acts and the attempt are not incriminated and therefore, will not be punished.

Criminal Proceedings

The criminal action starts *ex officio*.

3.3.13 Fraudulent Financial Operations

Art. 27 of Law 365/2002

(1) Carrying out one of the operations covered by art. 1 item 10, by using an electronic payment instrument, including of the identification data allowing its use, without the consent of the owner of the respective instrument, is punished with imprisonment from 1 to 12 years.

(2) The same punishment is used to sanction any operation stipulated by art.1, item 10, performed by the unauthorised use of any identification data or by the use of fake identification data.

(3 The same punishment is used to sanction the unauthorised transmission of any identification data to another person, with a view of carrying out any of the operations by art.1, item 10.

(4) The punishment is imprisonment from 3 to 15 years and the denial of certain rights, if the acts covered by paragraphs (1) - (3) are committed by a person who, by reason of his (her) job attributions:

a) performs technical operations necessary to issue the electronic payment instruments or to carry out the types of operations stipulated art. 1 item 10 or

b) has access to security mechanisms involved in issuing or using electronic payment instruments, or

c) has access to identification data or security mechanisms involved in carrying out the types of operations stipulated in art. 1 item 10.

The Protected Legal Interest

It refers to the entire social relationships referring to the public trust (fides publica) in the safety and reliability of the electronic payment instruments, to the validity and authenticity of computer data, to the entire processing, storing and automatic transaction process of data and values.

The protected legal interest is also that of the owner of the forged electronic payment instruments issuer, financial institution etc.), of the owner or rightful user of the respective

electronic means, identified by the identification computer data stored or circulated in the issuer's computer system.

The Subjects of the Offence

The Offender

The offender can be any person who has criminal responsibility and liability for punishment – case of paragraphs (1), (2) and (3).

Under the terms of paragraph (4), the offender has to an employee of the issuing financial institution or in a contractual relationship with it and, by reason of his (her) attributions, to be involved in technical or financial operations with electronic (issuing cards, configuration of identification data, setting up security measurements, etc.).

Involvement is possible in all its forms: principal, co-principal, instigator or accomplice.

The Victim

It can be a natural person rightfully owning the forged electronic payment instrument or the identification computer data.

There is also a secondary passive subject which is the legal person owning the electronic payment instrument (the issuing financial institution respectively).

The Materiality of the crime Under the conditions of paragraph (1), it is achieved by the action of using an electronic payment instrument and of the associated identification data (PIN code, user code, other references) at one of the terminals mentioned by NBR Regulation no. 4/2002, without the rightful owner's consent. The relationship between the electronic payment instrument and the identification data is an associative one in terms of the technical details of the location (terminal) where the respective instrument is used. There are situations when certain accepting traders use POS terminals for instance thus set not to require the identity of the card user by the introduction of the PIN code.

Under the terms of paragraph (2), the material element refers to the transfer of funds, withdrawal of cash or charging/discharging an electronic payment instrument, if the offender uses fictitious identification data or real identification data without authorisation.

Paragraph (3) stipulates the unauthorised transmission of any identification data to another person, with the express requirement that there is dissemination of the information for a transfer of funds, a cash withdrawal or charging/discharging a value unit stored on electronic payment instrument.

The material element under the terms of paragraph (4) is similar to the already presented ones, in this case with the aggravation of the offender's participation in the crime.

An example of fraudulent financial operation with electronic payment instruments is carding. This is generally a term used to define the validation of identification data associated with an electronic payment instrument (card). Thus, the offender offers the card data on a specialised website with real time processing facility. If the electronic payment instrument is recognised by the system, the offender will be sure that the instrument is valid and can be used. Generally, small value online services or products are chosen or online payments (donations) are made on electronic commerce sites in order to avoid signalling the fraud at the level of the issuing financial institution.

Most fraudulent electronic financial operations occur however on the Internet. The electronic mail and the Internet are the main ways to commit frauds against traders selling or transporting products by benefiting of the facilities offered by electronic (online) commerce. The term used in the profile industry for catalogue type orders or other similar transactions is CNP – Card Not Present, meaning the physical check of the electronic payment instrument is not necessary. Under the circumstances, the trader relies exclusively on the information supplied by the card holder (or the person claiming to be the card holder) by means of the phone, electronic mail or online forms on the websites, when the possible buyer is not in front of a POS. It is difficult for the trader to instantly check if the card holder legally authorises the transaction and the shipping companies for example guarantee only the delivery of products under good conditions to the specified addresses without being required to check the identity of the person receiving the products.

Furthermore, it is good to know that the small value electronic transactions are not automatically checked by the bank institution or the accepting trader, especially because of the cost difference between the possible fraud and the value of the financial investigation it self.

Mens rea

The offence of fraudulent financial operations is committed with *direct* or *indirect intention.*

Forms

The attempt is punished, in terms of paragraph (5) of the same article.

The offence covered by paragraph (1) is consumed when the offender has achieved a first interaction of the electronic payment instrument with the computer system (including cashier desk operations, standard terminals such as imprinter, POS, ATM etc.) of the back, credit or financial institution.

In terms of paragraphs (2) and (3), the offence is consumed when the real identification data have been used or transmitted without authorisation or when the offender chooses to use the false identification data.

In terms of paragraph (4), the offence is consumed when the data to which the offender has access by reason of or charge/discharge an electronic payment instrument.

Criminal proceedings

The criminal action starts *ex officio*.

3.3.14 Accepting Fraudulent Financial Operations

Art. 28 of Law 365/2002

The acceptance of one of the operations covered by art.1 item 10 while acknowledging it is performed by means of a forged electronic payment instrument or used without its user's consent will be punished with imprisonment from 1 to 12 years.

The same punishment will be applied for accepting one of the operations covered by art. 1 item 10, while knowing the operation is done by the unauthorised use of identification data or by the use of assumed identification data.

The Protected Legal Interest

Refers to social relations related to public trust into the safety and reliability of the entire modern process of processing, storing and automatic transferring data and values within bank, credit or financial institutions or accepting traders.

The Subjects of the Offence

The Offender

Will be a natural person employed by a bank, credit or financial institution or having a contractual relation with it and who, based on his (her) job description or labour contract is responsible for the good development of the financial operations using electronic payment instruments.

The involvement is possible in all its forms: principal, co-principal, instigator or accomplice

The Victim

Will be the natural person rightfully owning the forged electronic payment instrument or the identification computer data used without authorisation.

There is also the secondary victim which is the legal person owning the electronic payment instrument (the issuing financial institution respectively).

The Materiality of the crime refers to the acceptance of an electronic financial transaction (fund transfer, cash withdrawal etc.), with the knowledge that the transaction has been performed by using a forged electronic payment instrument, without the consent of the rightful owner of the genuine instrument or by using fictitious identification data or real data without authorisation.

Acceptance involves the initiation, continuation or approval of the transaction operation. For accepting traders, it is the case when a cahier operator *accepts* to handle the card susceptible of being forged and makes the interaction between the card and the POS device, *accepts* the introduction of the identification data (knowing they are used without authorisation or that they are false) or *does not stop the transaction.*

In the case of the bank, credit or financial institutions, we have the situation of authorised operators with the attribution to administer (to approve as good for payment) electronic financial transactions.

Mens rea

The forgery of electronic payment instruments s committed only with *direct intention*.

Forms. The preparatory acts, although possible, are not incriminated and therefore, they are not punished.

The attempt is punished according to the provisions of paragraph (3) of the same article.

The offence is susceptible of being committed with the real concurrence of offences such as favouring the offender (provided and sanctioned by art. 264 Criminal Code), and fraudulent administration respectively (provided and sanctioned by art. 214 Criminal Code).

Criminal proceedings

The criminal action starts *ex officio*.

An interesting element of these offences is, more recently, their organised and complex character. The legal practice has shown that most often, the offences typical for the electronic commerce come in real concurrence with cibecrimes or organised crimes.

3.4. Controversial Aspects. *De Lege Ferenda proposals*

The legal practice in the domain of cybercrime shows that, presently, Romania has adopted and applies a complex set of criminal regulations covering several anti-social acts related to cybercrime.

However, it appears from the analysis of certain cases that, generally, Law 161/2003 or 365/2002 is questionably interpreted by some prosecutors or judges who understand less the

technical details of the act, fact which has a negative impact upon the accuracy of the legal trial and often these situations can mean "a way out" for the cyber offenders.

3.4.1 Skimming

As regarding SKIMMING, a close analysis shows that this act could be (rather forcibly) covered by the provisions art. 24 of Law 365/2002 on electronic commerce, as a prior form to the forgery of electronic payment instruments but any reference to illegal access to a computer system (art.42 of Law 161/2003) as it results from the analysis of the following case:

The High Court of Cassation and Justice, Criminal Division, Decision no. 5288 of September 15, 2006
By criminal sentence no. 21/2006 of Hunedoara Court, the defendants C.C., G.M., T.I. and I.F. were condemned for braking the confidentiality and integrity of the computer data and systems mentioned in art.42 paragraphs (1) and (3) of Law no. 161/2003, for the forgery of electronic payment instruments covered by art.24 paragraphs (1) and (2) of Law no. 365/2002, for performing fraudulent financial operations covered by art.27 paragraph (1) of Law no. 365/2002 and for aggravated theft covered by art.208 paragraph (1), art.209 paragraph (1), letters a) and e) Criminal Code, all with the application of art.41, paragraph (2), art. 3, letters a) and b) and art.34, paragraph (1) letter b) Criminal Code

The court noted that in May 2005, the defendants C.C., G.M., T.I. and I.F. agreed together to use reading devices for card magnetic strips (skimmers) with a view of obtaining the data necessary for cloning several cards and to withdraw cash.

For this purpose, for several data, the defendants travelled to different locations, mounted the skimmers and the mini-camera on several ATMs and obtained the data on the cards used at these ATMs that they downloaded and stored in a computer at I.F.'s residence.

After all the data obtained had been stored in the computer, the defendants acquired blank cards and stuck on each of them adhesive labels on which they wrote the PIN or PINs previously read by the mini-camera. By means of an electronic printing device attached to I.F.'s computer the magnetic strip of each blank card was inscriptioned with the previously copied account corresponding to the PIN code inscriptioned on the label.

On June 28, July 7, July 8, July 11 and July 21 2005, the defendants withdrew cash by means of the cloned cards from the ATMs of several banks.

By Decision no. 197/A of June 22, 2006, Alba Iulia Appeal Court, criminal division, accepted the appeals declared by the defendants, changed the criminal charge mentioned by art.2,7 paragraph (1) of Law no.365/2002 and art.208, paragraph (1), art.20, paragraph (1) letters a) and e) Criminal Code, with the application of art.41, paragraph (2) of the same code, into one offence mentioned by art.27, paragraph (1) of Law no.365/2002, with the application of art.41, paragraph (2) Criminal Code, convicted the defendants on the basis of the latter legal texts and reduced the punishment of the defendants.

The appeal declared among others by defendant C.C., invoking the cassation case covered by art.385,[9] paragraph (1), item 12 C. Criminal Procedure, is unjustified.

It can be noted that defendant C.C.'s request of discharge on the basis of art.11, item 2, letter a) reported to art.10, paragraph (1), letter d) Criminal Procedure Code, for the offences mentioned in art.42, paragraphs (1) and (3) of Law no.161/2003 with the application of art.41, paragraph (2) Criminal Code and art.24, paragraph (2) of Law no.365/2002, in the variant of putting forged electronic payment instruments into circulation with the application of art.41, paragraph (2) Criminal Code, is unjustified

The provisions of art.24 paragraph (1) of Law no.365/2002 stipulate that the forgery of an electronic payment instrument is punished with imprisonment from 3 to 12 years and the denial of certain rights art.24, paragraph (2) of the same law incriminate the circulation, in any way, of forged electronic payment instruments and their possession with a view of entering them to circulation.

From the examination of the objective side of these acts, two distinct offences appear, one related to the forgery of electronic payment instruments and the second to the circulation or possession with a view of circulating forged electronic payment instruments.

In this case, the circulation of the electronic payment instruments was achieved by withdrawing cash, the transmission of the possession of the forged cards to another person being unnecessary.

On the other hand, the facts of the four defendants who, on the basis of the same criminal resolution, forged about 200 electronic payment instruments, meet the constitutive elements of the offence of forging electronic payment instruments covered by art.24, paragraph (1) of Law no.365/2002, with the application of art.41, paragraph (2) Criminal Code.

Also, on the basis of the same criminal resolution, the defendants' acts by which they possessed with a view of putting into circulation and circulated forged electronic payment instruments meet the constitutive elements of the offence of forging electronic payment instruments covered by art.24, paragraph (2) of Law no.365/2002, with the application of art.41 paragraph (2) Criminal Code.

The provisions of art.42, paragraph (1) of Law no.161/2003 incriminate the acceess without right to a computer system which is punished with imprisonment 3 months to 3 years or a fine and paragraph (3) of the same article stipulates that if the act mentioned by paragraph (1) is committed by breaching the security measures, the punishment is imprisonment from 3 to 12 years.

It must be noted that the ATM is a mean of collecting, processing and transmitting computer data represented by the owner's account number which is stored at level 2 of the black magnetic strip.

On the other hand, by mounting the skimmer in front of the ATM where the card is introduced and where, the security measures meant to provide the confidentiality of the account numbers and of the operations performed and to prevent the use of the cards by other people for forgery, were breached.
Or, from the evidence of the file, it appears that the defendants accessed a computer system without authorisation thus breaching the security measures.

Therefore, the acts of the defendants who, on the basis of the same criminal resolution, mounted a skimmer on various ATMs as well as a mini-camera thus, by breaking the security measures, accessing without authorisation the bank ATMs which, in terns of the law, are considered information systems, meet the constitutive elements of the offence of breaching the confidentiality and integrity of computer data and information, as per art.42, paragraphs (1) and (3) of Law no.161/2003, with the application of art.41, paragraph (2) Criminal Code.

As, in this case, the acts committed by defendant C.C. include the elements constituting offences according to art.42 paragraphs (1) and (3) of Law no.161/2003, with the application of art.41, paragraph (2) Criminal Code and art.24, paragraph (2) of Law no.365/2002 on electronic commerce, in its variant of putting forged electronic payment instruments into circulation, with the application of art. 41, paragraph (2) Criminal Code, there are no causes for the acquittal as requested.

For these considerations, the defendant's appeal was denied.

In this case, we consider that the High Court of Cassation and Justice unduly dismissed the appeal of the defendants as concerning the indictment of their act in terms of the provisions art. 42 paragraph (3) of Law 161/2003, Title III – prevention and combating cybercrime, which sanctions with imprisonment 3 to 12 years, the access without right to a computer system in order to obtain computer data by forcing the security measures.

We agree that ATM type of systems have to be included into the category of computer systems as from the technical standpoint they meet the conditions to be considered as computer systems. However, the only security elements of ATMs are of a logic type, computer applications that establish the validity or validity of a card on the basis of on a mathematical introducing the values "true" or „false" for the set of information stored on the magnetic tape of the card or obtained by pressing the PIN code by the holder. Forcing the security measures associated to such a computer system (ATM) would involve a direct interaction of the offender with this device or upon the mathematical function, which, from the point of view of a skimmer is almost impossible.

Or, in the analysed case, the offenders attached to the plastic or metal interface of the ATM a device especially created to mislead the users letting them believe they were in front of the genuine ATM and thus, making them use their own cards. The extraction of the data from the cards, including their processing and the combination with the images taken by the micro video-camera including the introduction of the PIN, occurred later on.

We believe that in this case there is rather an application of the *social engineering* concept or, at the most, a preparatory form of the offence of forging an electronic payment instrument and in no case, illegal access to a computer system by forcing the security measures.

Referring to the same Skimming act, some specialists even came with the idea of an offence of "illegal interception of an information data transmission", under the terms of art.43 of Law 161/2003. We consider this solution wrong as well because, from the technical point of view, there is no computer data transmission in the sense considered by the Romanian legislator. The chapter related to "Cybercrimes" explains what happens in the case of data transmission interception.

With Skimming, the capture and "reading" of the data of the magnetic tape are practically done before the respective card enters the ATM slot and the transmission of data between the card and the ATM is achieved. If, for instance, the Skimming device would be placed inside the ATM and would capture the data transfer between the magnetic strip and the ATM reader, an interception of the transmission could be considered and reference could be made to art. 43 of Law 161/2003 and even illegal access to a computer system (ATM), covered by art.42 of the same law.

Under the circumstances, we believe that, presently, in Romania, with the existing legal instruments, simple Skimming cannot easily be legally indicted and hence cannot be sanctioned accordingly (certain preparatory acts of this illegal act can have constituent elements of a different offence). However, the extremely large number of acts of this type requires the introduction of an indictment norm under art. 24 of Law 365/2002 (which is the basic legal provision).

Therefore, for the improvement of the application of Law 365/2002 we can suggest the following text which, in our opinion, would undeniably incriminate any form of skimming:
Obtaining by fraud, including by using technical devices especially created for this purpose or by using electronic communication means (telephone, facsimile or computer systems), any data or information associated to an electronic payment instrument or a bank account is a crime and is punished by imprisonment from 6 months to 1 year.

3.4.2 „Identity Theft"

As in other countries, Romania faces more and more an exceptionally severe phenomenon which needs special attention from the legislator: „*identity theft" through electronic communication means.*

As term, *the identity theft* is an inappropriate denomination as the identity of a person is not actually stolen but only doubled (tripled etc.).
However, illegally obtaining (sometimes personal) information that could directly identify a person, without the person's consent, by misleading or by the infringement by the operators mentioned Law 677/2001 (on personal data processing and free circulation) of their

obligations, would bring important mainly financial damages to the respective person but not only.

For instance, we can consider the act well know in practice as PHISHING. Presently, this act is punished in terms of the provisions of art.48 of Law 161/2003 regulating *computer-related forgery*.
Study case:

The prosecutors of the Direction for the Investigation of Organized Crime and Terrorism received on May 16, 2008, from USA legal authorities a rogatory commission request to identify the members of a criminal group on Romania's territory, to identify certain IP addresses, to perform residence search (that took place on May 19, 2008) in seven locations in Bucureşti, Craiova, Caracal and Buzău).

Actually, the Californian Prosecutor's Office – The Central District and the Federal Investigation Bureau have carried out an investigation on the activity of an organised crime group with offences such as identity theft, fraud and cyber offences.

Thus, the American prosecutors have indicted on May 15, 2008, the named S. A. P., Ş. S. I., M. C., I. N. S., P. B. B. and others for the crimes of the creation of an organised criminal group forgery of electronic payment instruments possession of equipment for fraudulent operations by means of electronic payment instruments and access *without right.*

This criminal group was performing fraudulent financial operations by using counterfeited electronic payment instruments to generate financial transfers. The members of the criminal group have obtained thousands of accounts and data associated to credit and debit cards by sending through the Internet e-mail messages to fraudulently attract account owners towards web pages that had the appearance of the pages of some legal bank and financial institutions. The account owners were invited to introduce access devices and other personal information on or through these web pages.

The accomplices of the offenders having created and operated the „pshishing" pages and sent the e-mail messages, spam or other fraudulent messages are located in Romania and other states and have worked together with accomplices in the USA, including with the suspect leaders, in this case, S. W. L. and H. T. T respectively. The latter have used information supplied by the defendants in Romania to create access cards and to access and withdraw funds from the victim's accounts, acting as "cashiers" and coordinators of the fraudulent access devices

and identities to withdraw cash form ATMs and to buy goods and services by means of POS systems. As a general rule, the goods thus obtained were split in equal percentages with the accomplices in Romania having supplied the information of the access devices.

The total estimated damage caused in the case would have exceeded USD 1 million.

However, a careful analysis of the act shows that only one of the Phishing stages can be really indicted as computer fraud wand that is the creation of a counterfeit web page with the purpose to mislead the users of the real page.

Yet, in Phishing cases, a significant component is the communication of data by e-mail when the potential victims are lured (by e-mail messages well drafted from the point of view of the inter-personal communication techniques) to access counterfeited websites or reveal their personal and financial data. Presently, from the legal point of view, this act (luring the users of electronic communication means) is included in the materiality of the cyber-related fraud offence, but we support the idea that the existence (creation) of a distinct indictment norm could be useful and would offer the legal investigation authorities a broader legal basis in combating cybercrime.

Therefore, we are making the following proposals of legal norms (broader):

Obtaining any information about a person by means of which he (she) can be identified directly without his (her) agreement or by misleading, if the act has been done by using communication techniques or by using computer or telecommunication systems is considered a crime and is punished with imprisonment from x to y years.

Or

Obtaining any information by means of which a person's electronic payment instrument can be directly identified without the person's agreement or my misleading, if the act has been done by using communication techniques or by using computer or telecommunication systems is considered a crime and is punished with imprisonment from x to y years.

If the act in paragraph 1has been done by using electronic or electromagnetic devices especially conceived to capture or store data in audio, video or electronic (skimming), the punishment will be imprisonment from x to y years.

For the point of view of the legislative technique, we believe the introduction of such a new article or a combination between the 2 mentioned in Law 161/2003 would be preferable.

3.5. Conclusions

When investigating infringements in a domain that is so rapid in its evolution, such as that related to cybercrime, it is clear that not only the institution in charge with applying the law must be familiar with the latest news in the domain but also any player on the public scene interested in the subject. The law, even if it observes the neutrality principle, must be able to cover the mail illegal actions that occur in the virtual space. In this sense, the authors openly support the idea of the necessity of frequent debates on topics related to this subject, with the participation not only of those directly involved in fighting cybercrime but of the private, academic sectors and the civil society that can bring a different perspective on this domain at national, regional or international events.

4. International Responses for Counteraction to Computer Crime

On account of their specific target of encroachment or means of perpetrating the act – information technologies - computer crimes quite often have a cross-border character. The fast development and dissemination of such technologies allows perpetrators of crimes in one country to perpetrate encroachments against targets located in one or more other countries. The cross-border character of computer crime impedes its detection and punishment only through the national legislations of separate states, and necessitates the focusing of still more efforts on the creation of international instruments for prevention of and counteraction to this phenomenon.

4.1. Initiatives of the Organization for Economic Co-operation and Development (OECD)

The first steps in the sphere of international co-operation in counteraction to computer crimes are initiated within the framework of the Organization for Economic Co-operation and Development (OECD). In the early 80s of last century OECD already starts seriously dealing with problems concerning information inviolability, and in consequence, several recommendations and declarations regarding data protection upon automatic processing and cross-border exchange of data have been adopted. In 1983, within the framework of the organization, an expert commission is formed to study computer crimes and the related necessity of changes to the national legislation of the member states. In 1986, the commission publishes the report *Computer-Related Crime: Analysis of Legal Policy*, which analyses the various approaches to computer-related crime used by the national legislations of separate member states, and proposes a list of acts recommended to be criminalized in all member states. [115] At the end of XX century and the beginning of XXI century, OECD focuses its efforts on the security of information systems, illegal and harmful contents on the Internet, encryption, security of data in global networks, and consumer protection in online trade.

4.2. Initiatives of the United Nations (UN)

[115] See Computer-Related Crime, Analysis of Legal Policy, OECD, Paris, 1986.

The first UN initiatives for counteraction to computer crime are also related to problems concerning inviolability of data and data protection upon automatic data processing and exchange, as well as to the legal meaning and value of computer recordings as evidentiary material (including in criminal proceedings), and the fight against racist and xenophobic contents on the Internet.

In 1990, within the framework of VIII UN Congress on prevention of crime and treatment of perpetrators, a special resolution is adopted regarding computer-related crimes, in which the member states are called on to improve their national legislation (both material and procedural law) by way of providing measures for effective detection, investigation, and punishment of computer crime. In pursuance of this resolution, in 1994, the UN publishes *A Manual on the Prevention and Control of Computer-Related Crimes*, which examines several groups of issues – nature of computer crimes, material law protection of inviolability of data and their confidentiality, procedural law issues related to investigation and punishment of computer crimes, prevention of computer-related crime and international co-operation.[116]

4.3. Initiatives of the Council of Europe (CE)

The Council of Europe has made the most significant contribution to the development of international co-operation in counteraction to computer crime. Like most other international organizations dealing with prevention of and counteraction to computer crime, the first initiatives of the CE are also in the field of inviolability-of-data protection. Thus in 1981, Convention No. 108 of 28.01.1981 of the Council of Europe for the Protection of Individuals with regard to Automatic Processing of Personal Data is adopted.[117] Along with other provisions, the convention binds each party to establish the relevant sanctions and compensations upon violation of the internal law provisions which enforce the data protection principles of the convention. At the end of last century and the beginning of the present one, recommendations are also adopted which pertain to data inviolability protection in different

[116] See United Nations Manual on the prevention and control of computer-related crime, International review of criminal policy, № 43 и 44, 1994.
[117] Convention No. 108 of 28.01.1981 of the Council of Europe for the Protection of Individuals with regard to Automatic Processing of Personal Data, ratified by an act adopted by the Thirty-ninth National Assembly of 29 May 2002, promulgated in SG, issue 56 of 7 June 2002, issued by the Ministry of Interior, promulgated in SG, issue 26 of 21 March 2003, enforceable since 1 January 2003

spheres of public life (medical data, data for the purpose of science and statistics, etc.). The CE also adopts a series of recommendations related to illegal and harmful contents in the electronic media and on the internet, such as violence, instillation of hatred, etc.

In 1989 the CE adopts Recommendation No. R(89)9, which contains a list of the minimum encroachments which shall be incriminated by the member states for the purpose of adoption of a general criminal policy with regard to computer-related crimes, as well as a list of other encroachments on the incrimination of which consensus has not been achieved.[118] In 1995, a second recommendation is adopted pertaining to the criminal procedural aspects of the creation and use of information technologies, which recommends that the member states should provide for rules in their internal legislation regulating the searching of computer systems and confiscation of computer data.[119]

In 1997, an Expert Commission on Cybercrime to the CE is formed to examine and define new crimes, jurisdiction of states, and criminal liability in relation to online communication. On the basis of the results from the expert group's work, a draft for a Convention on Cybercrime is prepared, and adopted at the 109th meeting of the Committee of Ministers on 8 November 2001, and is open to signing at the meeting in Budapest, Hungary, on 23 November 2001.[120]

The Convention on Cybercrime of the Council of Europe provides definitions of essential concepts related to computer crime, and provides for the specific steps that the member states shall take on the national level in the field of material and procedural criminal law. Four main concepts are defined – a computer system, computer data, a service provider and traffic data.

The Convention provides definitions of four basic categories of crime: infringements of the secret, inviolability and possibility of use of computer data and systems (unauthorized access, illegal interception, encroachments on inviolability of computer data and computer systems, misuse of devices), computer crime (computer forgery and computer fraud), contents-related

[118] See Recommendation No. R (89) 9 of the Committee of Ministers to Member States on Computer-Related Crime (adopted by the Committee of Ministers on 13 September 1989 at the 428th meeting of the Ministers' Deputies).
[119] See Recommendation No. R (95) 13 of the Committee of Ministers to Member States Concerning Problems of Criminal Procedural Law Connected with Information Technology (adopted by the Committee of Ministers on 11 September 1995 at the 543rd meeting of the Ministers' Deputies).
[120] See Convention on Cybercrime, adopted at the 109th meeting of the Committee of Ministers of the Council of Europe, and open to signing in Budapest on 23 November 2001, ratified by an act adopted by the Thirty-ninth National Assembly on 1 April 2005, promulgated in SG, issue 29 of 5 April 2005, issued by the Ministry of Justice, promulgated in SG, issue 76 of 15 September 2006, enforceable in the Republic of Bulgaria since 1 August 2005.

crime (child pornography), and copyright infringement (piracy of protected works, etc.). Provisions therein regulate the incrimination of participation in and attempt at a computer crime, as well as the introducing of liability, including criminal liability, of legal entities where the crime is perpetrated in favour of a legal entity by a related natural person.

With regard to criminal procedure, the Convention provides rules pertaining to efficient retention of data in computer systems, and of traffic data, the procedure of data provision, search and confiscation of the computer data retained real-time collection of traffic data and contents-related data.

With regard to international co-operation, the Convention introduces a few new forms of co-operation, in addition to the traditional instruments provided by the European Convention on Extradition and the European Convention on Mutual Assistance in Criminal Matters. The formation of a 24-hour network of contact points (the so-called 24/7) is also provided to ensure co-operation upon investigation of computer crimes.

Through an Additional Protocol to the Convention on cybercrime, concerning the incrimination of acts of a racist and xenophobic nature committed through computer systems.[121] The Additional Protocol provides a definition of the concept "racist, or xenophobic material", and indicates four groups of crime – distribution of racist and xenophobic material through computer systems, threat with racist and xenophobic motives, offence with racist and xenophobic motives, denial, extenuation, approval, or justification of acts of genocide or crimes against humanity. The Protocol also contains provisions concerning incrimination of accessory and inducement to such crimes.

4.4. Initiatives of the European Union

In the late 80s and early 90s, computer crimes become an object of attention on the part of the European Union as well. In 1987, at the request of the European Commission, the Report on *the Legal Aspects of Computer Crime and Security*[122] is drafted, and in 1998 the European

[121] See Additional Protocol to the Convention on cybercrime, concerning the incrimination of acts of a racist and xenophobic nature committed through computer systems, Strasbourg, 28 January 2003.
[122] See Sieber, Kaspersen, Vandenberghe, Stuurman, *The Legal Aspects of Computer Crime and Security - A Comparative Analysis with Suggestions for Future International Action*, document prepared for the Commission of the European Communities, 1987.

Commission presents to the Council the results from a study on the subject of *Legal Aspects of Computer-Related Crime in the Information Society*[123] (popular as the COMCRIME-Study). The first EU legislative acts pertaining to computer crimes are mostly in the area of personal data protection, intellectual property, and counteraction to illegal and harmful contents on the Internet. Most of these documents do not provide for specific measures in the field of criminal law, instead, they only focus on the necessity of sanctions on infringements in these spheres.

In October 1999, at the meeting in Tampere, Finland, the Council of Europe makes the conclusion that high-tech crime shall be included in the efforts for unification of definitions and sanctions. The European Parliament also calls up for adoption of unified definitions of computer crimes, and for effective harmonization of legislation, especially in the field of material criminal law. In the course of drafting the Convention on Cybercrime of the Council of Europe, the Council of the European Union adopts a General Position concerning the negotiations on the Convention, and includes some of its elements as part of the Union's strategy for counteraction to high-tech crime.[124]

On 26 January 2001, the European Commission adopts a proposal to the Council of European Parliament under the title *Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-Related Crime*.[125] The proposal summarizes the kinds of computer crime incriminated in the EU member states – crime against personal data inviolability, crime related to distribution of illegal contents, economic computer crime, and intellectual property crime. On 6 June 2001, the European Commission adopts a second proposal under the title *Network and Information Security: Proposal for A European Policy Approach*.[126] The same month a Recommendation of the Council of 25 June 2001 is adopted, concerning contact points maintaining 24-hour service for combating high-tech crime.[127]

---

[123] See *Legal Aspects of Computer-Related Crime in the Information Society (COMCRIME-Study)*, prepared for the European Commission by Prof. Dr. Ulrich Sieber, University of Würzburg, 1998.

[124] See General Position of 27 May 1999, adopted by the Council on the grounds of Article 34 of the Contract of the European Union on the negotiations conducted at the Council of Europe, regarding the draft of the Convention on Cybercrimes (1999/364/JHA), Official Journal n° L 142 , 05/06/1999, page 0001 – 0002.

[125] See Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions *Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime* (COM(2000)890).

[126] See Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions *Network and Information Security: Proposal for A European Policy Approach* (COM(2001)298).

[127] See Council Recommendation of 25 June 2001 on contact points maintaining a 24-hour service for combating high-tech crime, Official Journal C 187, 03/07/2001 P. 0005 – 0006.

A year later, on 19 April 2002, Commission proposal for a Council framework decision on attacks against information systems is also published.[128] The decision is adopted on 24 February 2005 for the purpose of improvement of co-operation among judicial and other competent authorities, including the police and other specialized law enforcement authorities of the member states, by drawing closer the rules of criminal law in the sphere of attacks against information systems.[129] That is the most important EU legislative act in the sphere of computer crimes. The framework decision provides definitions of concepts, such as "information systems", "computer data", and "unauthorized access", and binds the EU member states to incriminate at their internal legislation particular crimes, such as unauthorized access to information systems, and unauthorized interference in the system or data. Furthermore, the proposal binds the member states to incriminate inducement, accessory to, participation in as well as attempt at such crimes. Other rules are provided concerning punishment, liability of legal entities, and jurisdiction.

4.5. Other International Initiatives

Various initiatives on various problems related to computer crime have been undertaken by a series of other international institutions and organizations.

In 1997, the high-tech subgroup of the Group of Eight's (G8) chief experts – the organization of the seven most developed industrial states in the world (USA, the United Kingdom, France, Germany, Canada, Japan, and Italy) and Russia – adopts ten principles and an action plan for combating computer crimes, and in March 1998 a network of experts is also formed (working non-stop - 24 hours a day, 7 days a week) to further investigation of high-tech crime. That network aims at ensuring that perpetrators of computer crimes are not protected anywhere in the world, and law enforcement authorities have the necessary technical and legal instruments for detection of the perpetrators of such crimes and duly indicting them. It is accepted that the principles apply by way of conclusion of international contracts as well as by adoption of national laws and policies. Many other states outside G8 also join the newly-formed network.

[128] See Commission proposal for a Council framework decision on attacks against information systems, presented by the Commission on April 19, 2002 (COM(2002)173).
[129] See Framework decision 2005/222/JHA of the Council of 24 February 2005, regarding the attacks against information systems, Official Journal n° L 069, 16/03/2005 page 0067 – 0071.

In 2004, within the framework of intellectual property, the World Trade Organization (WTO) adopts an Agreement on Trade-Related Aspects of Intellectual Property Rights binding the states which are parties to the agreement to take measures for the incrimination of particular kinds of encroachment on intellectual property.[130]

Initiatives for counteraction to computer crime are also undertaken within various forms of international police co-operation. For instance, the European Working Group on Computer Crime to Interpol, formed in 1990, is the author of a *Manual on Investigation of Crimes against Information Technologies*.

The International Association of Penal Law – a non-governmental organization within the framework of the UN and the Council of Europe [131] – is another organization which has contribution to the development of international law regulations for counteraction to computer crime.

[130] See Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), WTO, 1994.
[131] See more about the work of the International Organisation of Penal Law in the sphere of computer crime at: http://www.penal.org.

5. COPYRIGHT ON THE INTERNET AND ONLINE COPYRIGHT INFRINGEMENT

Copyright is considered one of the major juridical problems related to the Internet. As long as the Internet is used as an instrument for selling and delivering information and intellectual work results with no paper and borders, matters concerning copyright protection of intellectual property the Internet will be of growing importance.

Copyright is an important form of intellectual property protection on the Internet which is due primarily to the following two reasons.

Firstly, most of the materials published on the Internet (written and visual materials, sound recordings) are works in the juridical sense, thus being subject matter of copyright.

Secondly, since the nature of electronic communication requires multiple data copying in the process of their transmission via the web and their delivery, hereby arises the question of copyright protection of such copies.

Every form of behaviour of the Internet users affects the right of authors and their assignee. In other words, it is impossible when working on the Internet not to potentially infringe anybody's copyrights. Surfing on the Net, storing part of the web pages contents in computer memory, forwarding e-mail messages – all these actions comprise reproduction of works subject matter of copyright.

Before analysing the problems concerning copyright protection on the Internet, it is necessary to define copyright protected materials published on the Internet and the requirements for the works subject matter of copyright.

5.1. Copyright Protection for Materials Posted on the Internet

In all countries copyright (where it exists) protects a variety of literary, scientific and artistic works. As a rule, national copyright laws and international conventions define the works subject matter of copyright descriptively. Usually they comprise the following categories:

literary, musical and audiovisual works, photographs, pictorial and graphic works, illustrations, maps, charts, plans, etc.[132]

At the same time, copyright protection is not available for materials such as reports of daily news or current events being customary media information, folklore works, as well as state documents, symbols and insignia.[133]

A large amount of the above mentioned literary and artistic works can be found on the Internet and all of them can be copyright protected, but belonging to one category of works or another as defined in the law is not enough.

5.1.1. Copyright Protection Criteria

In order to be protected under copyright law, the above mentioned works should meet specific criteria. Firstly, they should be "original" in the juridical sense and secondly, they should be expressed in an "objective form".

5.1.1.1.Originality

Different countries interpret the first criterion approximately the same. The courts in the countries of the Anglo-Saxon tradition interpret the criterion "originality" broadly: the work should be simply a result of independent work and talent of the author, i.e. not copied from other works – copyright of another author, and, according to Justice O'Connor, a judge at the U.S. Court of Appeal, it should "possess at least some minimal degree of creativity."[134]

Except for this criterion, courts in the continental countries of Western Europe also take into consideration whether the works bear the personality of the author or they are marked by his/her individuality. Although, nowadays these requirements are becoming more flexible due to the introduction of new forms of works whose creation includes automated elements.[135]

---

[132] *See,* US Copyright Law 1976, 17 U. S. C. §102 (a); Copyright and its related rights law (State gazette No. 59/20.07.2007), Art. 3(1); Berne Convention for the Protection of Literary and Artistic Works; Paris Act of 24.07.1971, revised on 2 October 1979 – p. 2 (1).

[133] *See,* §105, Art. 4.

[134] Feist Publications, Inc. v. Rural Telephone Service Co, 499 U. S. 340, 111 S. Ct. 1282, 1287 (1991).

[135] T. K. Drier. La qualitй d'auteur et les nouvelles technologies du point de vue des traditions de droit civil/ Symposium de l'OMPI, Paris, 1994.

In Bulgaria, the criterion of originality does not have legal definition. Only the "creative character" is mentioned as a feature of the activity resulting in the endeavour. Defining legally the term "author", the law states that this is "the physical person whose creative activity results in a work".[136] Therefore, the law acknowledges the results of a creative work as a subject matter of protection.

The "originality" in copyright does not imply "artistic value" and does not presuppose high aesthetical level of the works and impeccable artistic taste of their creation. According to Justice Posner, a judge at a U.S. Court of Appeal, "artistic originality is not the same thing as the legal concept of originality in the Copyright Act".[137]

"Originality" is neither a synonym of "novelty". "The work may be original even though it closely resembles other works so long as the similarity is fortuitous, not the result of copying".[138] Thus, two identical works, created by different authors, each ignorant of the other, shall be copyright protected even if the later created one is not novel. The fact that the protected works shall result from some kind of creativity does not imply that the level of the creativity should be high. In fact, the requisite "level of creativity" is extremely low; even a slight amount will suffice. The vast majority of works make the grade quite easily, as they possess some creative spark".[139]

The above mentioned fully concerns materials posted on the Internet. Even the simplest of them, such as e-mail messages, might easily meet the legal requirements for "originality".

Although the standard is actually very low, there is a range of materials which do not meet it. U.S. copyright legislation comprises a list enumerating materials, such as blank forms, works containing entirely public information, i.e. calendars, measure and weight tables or sport schedules.[140]

---

[136] Copyright and its related rights law (State Gazette No. 59/20.07.2007), Art.5;
[137] Gracen v. Bradford Exchange, 698 F. 2d 300 (7th Cir.1983).

[138] Feist Publications, Inc. v. Rural Telephone Service Co., 499 U. S. 340, 111 S. Ct. 1282, 1287 (1991).

[139] Ibid.
[140] *See* 37 C. F. R., § 202.1 (a), (c) and (d).

A large amount of such materials which are not protected are available on the Internet and most of them comprise simple facts. Copyright law of most jurisdictions does not extend its protection to simple facts, "even if they have been expressed, described, clarified, or illustrated in the works".[141]

If copyright protected data comprising simple facts, it would limit a free flow of information and exchange of opinions. "Copyright assures authors the right to their original expression, but encourages others to build freely upon the ideas and information conveyed by works. It is the means by which copyright advances the progress of science and art".[142]

On the basis of these considerations, copyright does not protect domain names and e-mail adresses, as well as code keys used in cryptography and electronic signatures being simple facts.

5.1.1.2. Fixation

The approaches to the second criterion are not the same in countries of different legal traditions. In the USA, for instance, copyright protected are materials "fixed in any tangible medium of expression now known or later developed, from which they can be perceived, reproduced or otherwise communicated either directly or with the aid of a machine or device".[143] Moreover, a work is considered "fixed" if the tangible medium appears to be "sufficiently permanent or stable to permit it to be reproduced or otherwise communicated for a period of more than transitory duration". [144]Copyright is not so much concerned with "the temporal duration of the copies as it is with what they are capable of doing while they exist".[145]

As a result of this approach, in accordance with the U.S. legislation, spoken, oral and choreographic works, not fixed on film or on any other information medium in "the real world", works transmitted in "real time" mode without being simultaneously recorded, such as

[141] Ukrainian copyright and its related rights law of 14 July 2001, Ukrainian Voice, 16. 08. 2001, Issue 146, p. 8, p. 3.

[142] Feist Publications, Inc. v. Rural Telephone Service Co., 499 U. S. 340, 111 S. Ct. 1282, 1287 (1991).

[143] US Copyright Law 1976, 17 U. S. C. §102 (a).

[144] §101(Definition for „fixed").

[145] Triad Systems Corporation v. Southeastern Express Co.), 31 U.S.P.Q. 2d (BNA) 1239, 1243 (N.D. Cal. 1994)

sport events program, in the "virtual" world of Internet, shall not be considered "fixed" and shall not be protected by copyright. [146]At the same time, there are original materials digitally fixed on a floppy, laser disk or in the computer memory (even in the operative memory, even if "just for a millisecond") available on the Internet. The other countries with Anglo-Saxon legislation follow the same approach. It fully complies with the requirements of the Berne Convention for the Protection of Literary and Artistic Works (briefly called Berne Convention) which preserves for the legislation in the countries of the Berne Union "the right to prescribe that literary and artistic works or any specified categories of works shall not be protected unless they have been fixed in some material form".[147]

In the countries of continental Europe, the copyright laws require the protected work to be fixed in some form, but not necessarily in a "material" one. Thus, the Bulgarian law spreads its protection over works expressed in "objective form", i.e. such form that allows perceiving the works by the perceptive organs. Along with oral, drama and choreographic works placed on the Internet, they meet the established legal requirements for representations in an objective form and are protected by copyright law in Bulgaria regardless of their copy on a material information medium.

5. 1.1.3. Formalities

In the countries of the Berne Union comprising states parties to the Berne Convention, including Bulgaria and Romania, the protection of the materials published on the Internet meeting the criteria of originality and fixation, occurs automatically at the moment of their creation as it is the case with all other materials. This means that "the registration of the materials or any other specific form and the fulfilling of other formalities are not necessary" for the occurrence and the establishment of copyright in these materials.[148]

---

[146] *See* U.S. Department of Commerce, Information Infrastructure Task Force, Intellectual Property and the National Information Infrastructure: The Report of the Working Group on Intellectual Property 32 (1995).

[147] Berne Convention for the Protection of Literary and Artistic Works; Paris Act of 24.07.1971, revised on 2 October 1979 – p. 2 (2).

[148] Ukrainian copyright and related rights law of 14 July 2001, Ukrainian Voice, 16. 08. 2001, Issue 146, p. 11, p. 2.

However, the legislation of most countries encourages authors to keep to some formalities, such as placing the copyright protection logo © on every copy of the works, state registration and deposition.[149]

5.2. Internet Materials and the Specifics of Their Copyright Protection

Below, the Internet materials will be presented in turn, as well as the specifics of the copyright protection of each of them.

5.2.1. Literary Works

All types of literary works appear to be typical subject matter of copyright protection in most countries. This category of works includes books, brochures, articles, and other written works.[150]

Defining the term "literary works", the U.S. Copyright Act states that these are works "expressed in words, numbers or other verbal or numerical symbols or indicia, regardless of the nature of the material objects, such as books, periodicals, manuscripts, phonorecords, films, tapes, disks".[151]

However, the Bulgarian law does not comprise a legal definition of literary works which can specify the works categorized as "scientific and technical literary works, publicistic works and computer programs".[152] Nowadays most of the materials available online, disseminated by mailing lists and discussion groups are literary works in the sense of copyright law.

Special attention should be paid to computer programs representing a peculiar form of intellectual property to which the Internet owes its existence and being considered as literary works by copyright law.[153] They control not only computers, but also the information exchange

[149] *See,* Copyright and related rights law (State gazette No. 59/20.07.2007), Rider clauses (1);
[150] *See,* US Copyright Law 1976, 17 U. S. C. §102 (a) (1); Copyright and related rights law (State gazette No. 59/20.07.2007), Art. 3(1); Berne Convention for the Protection of Literary and Artistic Works; Paris Act of 24.07.1971, revised on 2 October 1979 – p. 2 (1).
[151] *See,* US Copyright Law 1976, 17 U. S. C. §101 (definition for "literary works").
[152] Copyright and its related rights law (State gazette No. 59/20.07.2007), Art. 3(1), p. 1
[153] *See,* Copyright and its related rights law (State gazette No. 59/20.07.2007), Art. 3(1); Agreement on Trade-Related Aspects of Intellectual Property Rights, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade

between them uniting them in information nets. In fact, computer programs make possible the search and presentation of materials exchanged on the Internet and "translate" other works on the Internet from a computer language into a human one and vice versa. At the same time, they themselves are transmitted in large amounts via the Internet as individual works as well as parts of composite works. In fact, the simplicity of the momentous dissemination of computer programs on a global scale is the major threat for authors of programs and their lessees, in comparison, with which the threat for their rights by CDs fades.

In the U.S. Copyright Act the term "computer program" is defined as "a set of statements or instructions to be used directly or indirectly in a computer in order to bring about a certain result".[154]

The Bulgarian law does not comprise a legal definition of a computer program or software, while the legal theory assumes that a computer program is "a set of instructions capable of making the machine (computer) process the information, assign and accomplish a specific function and/or bring about a certain result".[155]

The protection of computer programs as literary works shows certain specificity in relation to the general regulations. A special exclusion is made for the free use of the computer programs according to Art. 71, item 1 of the Copyright and Related Rights Act, i.e. the person who legally acquired the right to use a computer program can, without the author's consent and without paying additional fee, make a backup copy of the program if it is necessary for the respective use of the program. At the same time, the law prohibits reproducing computer programs on any medium by a physical person for the purpose of his/her personal use even on the condition that this is not made for commercial purposes (Art. 25, Paragraph 2). Otherwise, we may face an infringement copyright in the form of reproduction of works unauthorized by the author for purposes beyond those stated by the law.

Organization, Annex 1C, Legal Instruments – Results of the Uruguay Round vol. 31//33 I. L. M. 81 – 1994 – Art. 10 (1)

[154] US Copyright Law 1976, 17 U. S. C. §101 (definition of "computer program").

[155] Markova, M. Computer programs and data bases in the system of intellectual property and the fight against their piracy, Periodical „INSO", 2002, Issue. 9, p. 21

Art.70 of the Copyright and Related Rights Act states the limits within which a legitimate user of the computer program can use it. He/She can start the program, open it on a screen, execute it, transmit over a distance, store it in the computer memory, translate it, process it, and make other changes in it, if it is necessary for the accomplishment of the purpose for which the right of use of the program is acquired including error elimination. In practice, these are the property rights on the computer program, which, except otherwise agreed between the parties, the user acquires as per license agreement with the author.

Two specifics of the computer program as a subject matter of copyright protection should be pointed out. Firstly, the program comprises algorithm, and secondly, it is, in a sense, its equivalent. This means that some of the features of the algorithm are typical for the program as well. At the same time, the program may be considered as a method for the realization of the algorithm and as such it is characterized by specific features; according to them, for the purpose of analysing the program as a subject matter of legal protection, it is possible to point out the following: unlike the algorithm being a sequence of logical and mathematical operations for transforming information, the program contains sequence of commands describing a process of realization of the algorithm and securing the control of this process.

An objective form of the program expression is the record of formalized language for same-type computers.

In fact, this expression appears to be the subject matter of copyright protection. Ideas implemented in the computer program, expressed in it and described by it are not copyright protected. Their protection is a prerogative of another branch of intellectual property law – patent law.

According to Art.6 of the Bulgarian patent law, patents are issued to inventions in all technical spheres, which are novel, innovative and practical for the industry. It is expressly stated that computer programs are not considered as inventions. It is pointed out that the exclusion of the above works is applied as far as the legal protection is necessary for them. This regulation is borrowed from Art. 52, Paragraph 2 of the European Patent Convention, parties to which are Bulgaria and Romania, and should be interpreted in the way it is interpreted by the European Patent Office.

The above said means that a computer program in itself is not subject matter of patent law, unless it meets all requirements of Article 6 of the Patent law and possesses the quality of a "technical contribution", in which case the program is defined as "a computer-implemented invention". Computer-implemented inventions include such devices as mobile phones, intelligent household appliances, engine control devices, and inventions concerning computer programs.

What is the source of the dual mode of protection of computer programs – as subject matter of copyright and as patent inventions?

The regulations stating that the computer programs "as is" are not eligible for protection under the Patent Act points out that they are copyright automatically. Copyright protects like literary works the form, the code strings written by the programmer and offers the possibility to prohibit copying or commercializing the code by third parties. At the same time, copyright does not protect the ideas behind software, what the software does in the machine or how the machine communicates with the environment under the control of the software. If such a process includes solving of a technical problem in an inventive way (i.e. a novel and non-obvious way), then we can have a patentable invention. This is implied by computer-implemented invention. Granting such a patent is completely compatible with the principles of the European Patent Law. Nowadays, around 15% of all patent requests submitted in the European Patent Office are related to computer-implemented inventions. This means that of more than 110 000 requests submitted to the European Patent Office, more than 16 000 have been related to innovations in computer technologies. In the course of time, the practice in the European Patent Office has been liberalized concerning the patentable criteria and, as a result, current patents are granted to computer-implemented inventions provided they have "technical contribution".

The concept of protection of computer programs by Patent Law has not only many supporters, but also many adversaries. The following practical hindrances arise in the patenting of computer programs:

1. The patenting procedure is very long – from 2 to 5 years, and the lifespan of the program might be shorter. It is well known that computer programs become obsolete very fast.

2. A register of the programs is non-available; therefore, there is no possibility for finding out those analogues and prototypes, which could serve as a basis for comparison with the new decision at the time of the patent examination.
3. Because of the difficulty in discovering the infringement of rights in such works, the complete publication of the description of the works as defined in the patent documentation, on one hand, is inexpedient, and on the other hand, it might prove extremely bulky for a patent application, which fits more a scientific publication than a patent description.

Therefore, even in its current form, copyright is capable of dealing with the new task – the protection of computer programs. Thus, scientists and practitioners direct their views to its institutions in the search of appropriate methods for such protection.

Under the program boom conditions and the possibility for lightning spread of "pirate" program copies on the Internet that knows no state borders, there is no doubt that the more attractive is the protection method which does not require many formalities and much time for examination. In this respect, the most effective is the method of computer program protection based on copyright which lacks an inspection procedure and has practically no special formality requirements. We should also take into consideration the fact that the establishment of legal copyright protection on national level automatically covers international program protection as well, provided by the international conventions concerning copyright; thus, this protection is valid in almost all countries in the world.

5.2.2. Photographs and Other Static Images

According to the degree of the information load of the works placed on the Internet, literary works take the first place, followed by photographs and other static representations on the computer screen (maps, charts, diagrams, etc.).

Moreover, the representations in question can be created on the monitor by special programs designed for facilitating the users in their computer use (operational systems) and for Internet provision (programs designed for web surfing – browsers and other applications) or for being uploaded on the Internet and having a character independent of the users.

In the first case, the image on the screen represents a part of a computer program, its interface, which is protected along with the whole program; in the second case, the image is a digital photography and is protected as ordinary photography[156], or is a result of transferring into the digital form (scanning) of an ordinary photography or other two dimensional (pictorial, graphic) or three dimensional (sculpture architecture) works, and in case they meet the originality criterion are protected as works derivative from the same. We will discuss derivative works in more detail below.

5.2.3. Musical Works and Sound Recordings

Musical works, those containing text, as well as those without text, are traditionally copyright protected.[157] There is a difference between the terms "musical work" and "sound recording". The latter is also a result of creative activities, but represents a secondary result of the fixation in a material form of the performance of the former. The rights in a musical work held by its author, the rights in the performance – by the performer, and those in the sound recording – by its producer. The two last groups of subjective rights are called related rights in the countries of continental law and according to their legal character they are analogous to copyrights.

The Bulgarian law, following the rules of the Convention for the protection of sound recording producers against unauthorized reproduction of their sound recordings of 1971, according to which a sound recording is "every recording of sounds designated for exclusively aural perception"[158], defines "sound record" as "a result from sound recording"[159], and "sound recording" – as "fixing on a permanent tangible medium of a string of sounds in a way allowing for their perception, reproduction, copying, wireless, cable or other means of transmission".[160]

In the U.S. Copyright Act the term "sound recordings" is defined as "a series of musical, spoken or other sounds, but not including the sounds accompanying a motion picture or other

---

[156] *See,* US Copyright Law 1976, 17 U. S. C. §102 (a); Copyright and its related rights law (State gazette No. 59/20.07.2007), Art. 3(1); Berne Convention for the Protection of Literary and Artistic Works; Paris Act of 24.07.1971, revised on 2 October 1979 – p. 2 (1).

[157] *See,* US Copyright Law 1976, 17 U. S. C. §101 (definition for "pictorial, graphical and sculptural works"); §102 (a) (1) – Art. 33(1) Item. 7, p. 2 (1).

[158] Convention for the protection of sound recording producers against unauthorized reproduction of their sound recordings as of 1971 - Art. 1 (a).

[159] Copyright and its related rights law (State gazette No. 59/20.07.2007), Rider clauses Art. 2(8);

[160] Copyright and its related rights law (State gazette No. 59/20.07.2007), Rider clauses Art. 2(7);

audiovisual works".[161] Therefore, the sound recording can represent sound recording of not only musical, but also other – oral, drama, musical and drama, choreographic works, as well as practically all sounds capable of being recorded.

More and more musical works and sound recordings appear on the Internet and while live performances of musical works are still limited to particular events, the dissemination of these works via the Internet in the form of sound recordings, saved in such digital formats as WMA and MP3 has become commonplace.

The popularity of the dissemination of sound recordings via the Internet is explained by the fact that this form of dissemination lacks the necessity for the provision of traditional media containing sound recordings, such as vinyl discs, tapes, CDs, etc., which considerably complicate the process of delivery of the sound recordings to listeners and lead to higher costs.

5.2.4. Audiovisual Works

With the introduction of cinema, motion pictures have been included in the scope of copyright followed by other audiovisual works in the process of technical development. The Bulgarian law defines this category as "films and other audiovisual works".[162] "Audiovisual works" usually means works "consisting of a series of related images with or without sound track, designed for reproduction expressly and only by specific technical means".[163] Part of the audiovisual works is the motion pictures, as well as the works "expressed in a way analogical to the cinematographic one".[164]

As an example of works belonging to this category, the Ukrainian law mentions "motion pictures, television films, video films, slides, etc., which can be fiction films, animation, non-fiction, etc."[165]

---

[161] *See,* US Copyright Law 1976, 17 U. S. C. §101 (definition for "sound recordings").
[162] Copyright and its related rights law (State gazette No. 59/20.07.2007), Art. 3(1), Item 4
[163] *See,* US Copyright Law 1976, 17 U. S. C. §101 (definition for "audiovisual works").; Ukrainian copyright and its related rights law of 14 July 2001, Ukrainian Voice, 16. 08. 2001, Issue 146, p. 1
[164] Berne Convention for the Protection of Literary and Artistic Works; Paris Act of 24.07.1971, revised on 2 October 1979 – p. 2 (1).
[165] Ukrainian copyright and its related rights law of 14 July 2001, Ukrainian Voice, 16. 08. 2001, Issue 146, p. 1

While the U.S. Copyright Act states that audiovisual works are designed to be represented by "machines or such devices as a film projector or electronic equipment regardless of the character of the material forms, such as tapes or cassettes being public".[166] Taking into consideration this regulation, US copyright adds motion pictures, video films, television programs[167] and video games[168] to the category of audiovisual works.

Audiovisual works, especially those saved in the digital form, pave their way through to the Internet. Such types of them as video films, video conferences, commercials, musical video clips, and animation films[169] are widely spread on the Internet. Undoubtedly, a larger amount of higher quality audiovisual works are going to appear on the Internet along with larger traffic capacity of communication channels and the improvement of TCP/IP protocols.[170]

5.2.5. Derivative Works

Works resulting from the creative recast of the works in all above mentioned categories are copyright protected as derivative works on equal terms with the works on the basis of which they have been created without prejudice to the rights of the authors of the pre-existing works.[171]

The following derivative works are mentioned in the Bulgarian law:

1. Translations and revisions of pre-existing works and folklore works;
2. Musical and folklore works arrangements.[172]

In the U.S. law, derivative works are listed in detail, namely these are "works based upon one or more pre-existing works": "translations, musical arrangements, dramatization, fictionalization, motion picture version, sound recording, art reproduction, abridgment, condensation, or any other form in which a work may be recast, transformed or adapted."[173]

---

[166] *See,* U.S. Copyright Act 1976, 17 U. S. C. §101 (definition for "audiovisual works").
[167] WGN Continental Broadcasting Co. v. United Video, Inc., 693 F. 2d 622, 626 (7 Cir. 1982).
[168] Midway Mfg. Co. v. Artic Int'l, Inc.), 704 F. 2d 1009, 1011 (7 Cir.), *cert. denied,* 464 U. S. 823 (1983).
[169] See, www.mult.ru.
[170] *See*: www.korrespondent.net/main/68092/.
[171] *See,* U.S. Copyright Act 1976, 17 U. S. C. §103; Ukrainian Copyright and Related Rights Act of 14 July 2001, Ukrainian Voice, 16. 08. 2001, Issue 146, Art. 1, p. 8, p.1, p. 14; Berne Convention for the Protection of Literary and Artistic Works; Paris Act of 24.07.1971, revised on 2 October 1979 – p. 2 (3).
[172] Copyright and its related rights law (State gazette No. 59/20.07.2007), Art. 3(2), Item 1, 2
[173] *See,* U.S. Copyright Act 1976, 17 U. S. C. §101 (definition for "derivative works").

It is obvious that there are a lot of translations, art reproductions, new computer program versions and derivative works of the same on the Internet. However, a large number of the Internet works are derivative because of the fact that many original works cannot be placed on the web.

The point is that most of the works due to their character and form of expression cannot be exchanged on the Internet directly, because the web allows for only one form of fixation – the digital one. This applies to oral, drama, choreographic works, pantomimes, artistic works, such as paintings, graphics, engravings, sculptures, etc., and architecture, scientific works, such as illustrations, maps, schemes, charts, etc, and applied arts.

Moreover, literary (computer programs including), musical, audiovisual, and photographic works, after being saved in the digital form or easily transferred into such form by means of technical tools, are placed as such on the Internet.

The same works which are fixed in traditional two or three dimensional forms are available to Internet users only thanks to images resulting from photographing them, shooting them on video, or scanning. These representations are classified as derivative works.

Moreover, if the processed photo, video or audiovisual materials are not saved in the digital form, then the results of transferring them into the digital form can also be derivative works provided they meet the originality criterion. Originality of derivative works resulting from transferring of other works into digital form is found in the creative recast of images, correction of the original defects, or change in colours (colouring) used in the restoration of old photographs and films.

5.2.6. Collection and Other Compiled Works

Collection of works of all of the above categories, including derivative works, provided they meet the originality criterion are subject to copyright protection "as such without infringing the rights of the authors of each work being part of such collections".[174] The originality of

[174] Berne Convention for the Protection of Literary and Artistic Works; Paris Act of 24.07.1971, revised on 2 October 1979 – p. 2 (5).

collections is due to the fact that they result form the creative work resulting in the selection, coordination or arrangement of the materials included into their contents.[175]

According to the Bulgarian law, this category comprises "periodicals, encyclopaedias, collections, anthologies, bibliographies, data bases, etc. consisting of two or more works or materials."[176]

The U.S. Act calls collection "compilation" defining it as "a work formed by the collection and assembling of pre-existing materials or data" and includes the term "collective works" in this definition. [177]And the latter is "a work such as a periodical issue, anthology, or encyclopaedia, in which a number of contributions, constituting separate and independent works in themselves, are assembled into a collective whole".[178]

As it can be seen from the quoted provisions of copyright acts, collections are copyright protected regardless of the fact that the materials they comprise are subject matter of legal protection. Such materials along with the protected works can be also the works that are not protected, simple facts included.

As it has already been pointed out above, data, such as names, addresses, numbers of spare parts, currency exchange rates, security quotes, etc. are simple facts and as such are not subject to copyright protection. This applies to all facts, such as scientific, historical, biographical, and news of the day. Like all other works, which are not protected, they are also treated as works in public domain and can be freely used by everyone.[179]

However, collections of works available for public use can be copyright protected. Such collections on the Internet are usually data bases. These works considerably facilitate the processes of storing, transferring and searching for information stored electronically.

---

[175] *See,* U.S. Copyright Act 1976, 17 U. S. C. §101 (definition for "compilation"); Ukrainian Copyright and Related Rights Act of 14 July 2001, Ukrainian Voice, 16. 08. 2001, Issue 146, Art. 8, p. 1, p.1, p. 15; Berne Convention for the Protection of Literary and Artistic Works; Paris Act of 24.07.1971, revised on 2 October 1979 – p. 2 (5).
[176] Copyright and Related Rights Act (*State Gazette* No. 59/20.07.2007), Art. 3(2), Item 3
[177] *See,* U.S. Copyright Act 1976, 17 U. S. C. §101 (definition for "compilation").
[178] *See,* U.S. Copyright Act 1976, 17 U. S. C. §101 (definition for "collective works").
[179] Ukrainian copyright and its related rights law of 14 July 2001, Ukrainian Voice, 16. 08. 2001, Issue 146, p.30, p. 2; Feist Publications, Inc. v. Rural Telephone Service Co., 499 U. S. 340, 111 S. Ct. 1282, 1287, 1288, 1289, 1290, 1293 (1991).

According to the Bulgarian law, a data base is a "compilation of independent works, data, or other materials, arranged systematically or methodically, and individually available via electronic or other means; computer programs used for the creation or functioning of data bases, records of separate audiovisual, literary, or musical works, as well as collection of sound recordings of musical performances on a CD are not data bases according to this law".[180]

Based on this definition, it is absolutely obvious that according to the law data bases comprise not only electronic systems, but also those systems which are controlled by mechanical devices and search in them is provided by such devices.

Therefore, more precise is the definition in the copyright legislation of the Russian Federation, according to which a data base is an "objective form of presenting and organization of data, such as articles, accounts, etc. so systemized that these data can be found and processed by means of Electronic Computing Machine (ECM)".[181] Thus, according to the Russian copyright legislation data bases are expressly and only electronic data bases.

The U.S. law does not provide a definition of data bases, but undoubtedly includes traditional, as well as electronic collections of "materials or data" in the term "compilation" as can be seen from the above quoted definition.

It is obvious that the scope of copyright protection for data bases comprising works which are not protected, or ordinary data, is smaller than the scope of the protection provided for data bases comprising protected works. In the case of data bases comprising works, which according to the legislation are public domain, the copyright protects only the selection, coordination and arrangement of the materials included in the contents of such data bases. However, copyright does not prohibit free use of the same materials.

Moreover, a large number of data bases are not subject to copyright protection, since they do not meet the originality criterion despite possible considerable efforts and investments necessary for their compilation. An example of such data bases can be telephone directories

[180] Copyright and Related Rights Act (State gazette No. 59/20.07.2007), Rider clauses Art. 2(13).
[181] Russian Federation Act on the legal protection of the programs for ECM and data bases of 23 September 1992, No. 3523-1.

which alphabetical order is far from original. [182] At the same time, the trend for *sui generis* protection for data bases not copyright protected is getting momentum.

Thus, in 1966, the European Union adopted a Directive[183], according to which data bases subject to legal protection are those, whose authors have made considerable investments in the obtaining, verification, and presentation of their composite elements. The process of implementation of the adopted Directive in the national legislation of the European Union member countries was prolonged: of 15 member countries at the beginning of 2000, its implementation became a fact only in nine countries.[184] A draft law of a similar content has been introduced in the U.S. Congress.[185] The law prohibits reproduction and commercial use completely or of essential (as an amount or quality) part of "selected information" which has been comprised, arranged and preserved by another party through investment of considerable monetary and other resources in a way that it harms the available or potential placement market of the other party in question. The proposed term for protection is 15 years. The methods of the protection of the rights of authors of collections include damage compensation and judicial injunctions. Legal sanctions are introduced for deliberate infringements.

The Bulgarian law protects two types of intellectual property rights concerning data bases. The first one is copyright held by the person who made the selection or arrangement of the comprised works and/or materials unless otherwise stated in a contract (Art. 11 of the Copyright and Related Rights Act). The revisions in the Copyright and Related Rights Act as published in the state gazette No 77/2002 foresee the introduction of *sui generis* right of the producer of data bases. The producer of data bases is defined as "a physical or juridical person, who has taken the initiative and the risk to invest in the collection, verification, or use of the contents of the data bases, if this investment is considerable in amount and quality" (Art. 936, Paragraph 2 of the Copyright and Related Rights Act). The exclusive right of the producer of a data base is valid for 15 years.

---

[182] Feist Publications, Inc. v. Rural Telephone Service Co., 499 U. S. 340, 111 S. Ct. 1282 (1991). – P. 1291-1293.
[183] Directive 96/9/EC of the European Parliament and of the Union of 11 March 1996 concerning the rights on the protection of data bases, OJ L 077 dated 27.03.1996, p. 20.
[184] *Вижс,* Introduction and Implementation of Directive 96/9/EC concerning the rights on the protection of data bases, 379, http://ec.europa.eu/internal_market/copyright/docs/databases/etd2001b53001e72_en.pdf.
[185] Collections of Infromation Antipiracy Act (Reported in the House), H.R.354. RH; http://www.codata.org/codata/data_access/linn.html.

The right of the producer of a data base is not the right of the author or a similar one. It is the right of such producer not to allow copying of part of the contents of the data base on another medium or its repeated use in another form, including dissemination of copies or digital delivery without his/her permission. This is the right of the producer of a data base regardless of whether the base itself is novel and original, i.e. has the character of works resulting from the creative intellectual activity or whether it is subject matter of copyright. In order to be subject matter of copyright, data bases should be a result of individual selection, systematization, and arrangement; it is namely the selection and arrangement that are subject to copyright protection. The compiled works, data or other materials are protected either by copyright or the *sui generis* right, or by both. However, their contents are not subject to the same protection – it is something very different from the data bases as a collection.

The introduction of the new right has been dictated by the development of the digital recording technology which makes possible electronic copying and rearrangement of the contents of data bases without infringing any copyright. This right is valid regardless of whether a data base or parts of it are subject to copyright protection or related rights (Art. 93d of the Copyright and Related Rights Act). The specificity of the above rights of the producer of a data base is in the fact that it is not based on creativity, which is customary for the protection of intellectual property, but on the investment made.[186]

The compiled works include also websites and multimedia works. These two types of works are widely spread on the World Wide Web and websites and most of the net resources are comprised in them.

According to their physical and legal character, websites are similar to data bases. The texts on the websites usually contain links to other information resources placed on the same or another website. Websites are mechanisms for access to systemized information and, if original, are subject to protection as well as data bases.

[186] Kamenova, C. Copyright. International and national, S., 1999, p. 416.

Multimedia works are those works that result from the combination of two or more categories of works in one form.[187] The most appropriate of all current forms of such combination is the digital one.

While the possibility for copyright protection of multimedia works is undoubted, the scope of this protection cannot be easily defined. The problem is, that multimedia works are created as a result of the process of convergence of different works subject to copyright protection, which is possible thanks to modern information technologies.

As a tradition, there are several groups of copyright protected works, each comprising several types of works, thus, each group may have different scope of protection from that of the other. The reason for such division is that it allows for estimating all specifications and quality differences among all categories of protected works.

The introduction of digital technologies made possible the transformation of all copyright protected works into a digital form and their unification within one work. What is, for instance, the interactive curriculum of the history of literature and art with audio and video accompaniment, computer program, literary works, and audiovisual works? Unfortunately, modern copyright does not give adequate answers to these questions.

5.3. Using Works on the Internet

In the information age, with the opportunity to access information located in electronic networks virtually from anywhere in the world and by an unlimited number of persons, with a special poignancy we should raise the problem of an enhanced protection of intellectual property right holders. Copyrights and related rights (rights in literary, scientific and artistic works; rights of producers and performers, rights of database and software developers, etc.) are the most affected ones.

The main function of copyright as a legal instrument is to ensure the protection of copyright holders (authors or persons to whom the exclusive right of use is transferred) against unauthorized use of their works by third parties. This protection is achieved by declaring illegal,

[187] *Виж* Thomas J. Smedinghoff, The Software Publishers Association Legal Guide to Multimedia 4 (1994).

i.e. infringement, of any reproduction, public presentation, transmission and distribution of copies of work, including on the Internet, without the consent of the copyright holder.[188]
Pursuant to Art. 18 of CNRA (Copyright and Neighboring Rights Act), the author has the exclusive right to use the work created by him/her and to authorize its use by other persons. The actions to be considered as use and representing the exclusive rights of the author are listed in par. 2 of Art. 18. Amongst them are items 1, 2 and 10 that are the most significant for e-commerce and providers of online services:

- Ø reproduction of a copy of the work;
- Ø distribution of the work amongst an unlimited number of persons, and
- Ø offering an unlimited number of persons an access to a copy of the work, which can be achieved from a place and at time individually chosen by each of them.

Definitions of reproduction and distribution are contained in § 2, par. 3 and par. 4 of the Additional Provisions of CNRA. According to the new revisions of these definitions, reproduction of a copy of the work is "the direct or indirect multiplication in one or more copies of the work or parts thereof, in any manner and form, permanent or temporary, including saving it in a digital format in an electronic media". Distribution of a copy of the work is "the sale, exchange, donation, renting and storage in commercial quantities, as well as the offer for sale or rent of originals and copies of the work".

A copy of a work can be used with the consent of the author unless the law provides otherwise, whereas the author is entitled to remuneration for any kind of use of the work and any consequential use of the same kind (Article 19 and Article. 35 of CNRA). Therefore, the use of works such as software, multimedia products, music, movies, databases, etc., including their reproduction on a magnetic or optical disk, uploading through Internet to another disk (server) or storage in computer memory and their subsequent distribution or offering access to them to an unlimited number of persons should be done only after obtaining the consent of the copyright holder. This consent is given through a contract signed by the author for the use of the copy of the work (licensing agreement), whereas the author assigns to the person – user – the exclusive or non-exclusive right to use a copy of the work created by him/her under certain conditions. With the changes introduced in issue 77 of State Gazette of 2002, an addition was made to the definition of users of works in § 2 item 6 of CNRA, where it was expressly added

[188] Apostolova, R., Protection of the distribution of movies and entertainment software on the Internet, „Ownership and law" magazine, 2002, b. 6, p. 64

that these were "the individuals and legal entities, such as suppliers of Internet content and others, who bring a copy of the work to the attention of readers, viewers and listeners directly or through other persons – distributors". This text for the first time introduces into Bulgarian legislation as a legal term the concept of "providers of Internet content" (these are the online media, Internet portals, resource and information sites, etc.). Creating a positive and legal framework governing the status of these entities is crucial, since in the digital age, in the traditional chain delivering intellectual products to end users - author -> publisher (producer) -> distributor, the role of distributors (and often of publishers) is increasingly played precisely by providers of Internet content. Without a clear definition of their rights and obligations through legal and contractual instruments, there is a real danger of depriving copyright holders of the opportunity to manage their property rights, including the right to receive remuneration for any use of their works.

With the changes made in CNRA in the year of 2000, a new property right was introduced for authors to authorize or prohibit the use of their work by cable or wireless transmission or other technical means of access by an unlimited number of persons to the work or parts thereof in such a way that allows it to be achieved from a place and time individually chosen by each one of them (Article 18, par. 2, item 10). Thus there is an emphasis on the right of authors to authorize or prohibit the publication of their work on the Internet. The very presence of musical works, movies, software or games subject to copyright at a publicly accessible Web site maintained by a provider of Internet content without consent of the holder of this right constitutes a breach of the existing legislation and this should be subject to respective civil, administrative or criminal liability. This liability should be assumed by the person who has reproduced the piece of work. In case this is the provider of online services or if it has been notified of the violation and still has not taken any actions for its termination it is liable for that. Liability should also be assumed in case of unauthorized distribution of the work when a copy of a work can be ordered from a site of a provider of online services using a catalog of works prepared by the provider, for which there is no consent obtained from the copyright holders.
Without the authors' consent, free use of works is permissible only in cases specified by law, provided it does not interfere with the normal use of the work and no harm is caused to the rightful interests of the copyright holder. With the recent amendments, a new hypothesis has been added in Art. 24 of CNRA, according to which without the consent of the copyright holder and without payment of remuneration temporary reproduction of works is permissible,

if it is of transient or incidental nature, of no self-importance, constitutes an integral and essential part of the technical process and is done with the sole purpose of allowing transmission in a network through an intermediary. This exclusion is with regard to actions during transmission over the Internet, such as browsing and casheing, provided the intermediary does not alter the information. Thus, in e-commerce, Internet service providers are enabled to act as intermediaries in the transmission of electronic documents subject to copyright, without requiring the consent of the right holder for each reproduction of the work.

Pursuant to Art.25 of CNRA, without the consent of the copyright holder, but subject to payment of a compensation, it is permissible to reproduce works, regardless of the medium, by an individual for his/her personal use, provided that it is not done for commercial purposes. The compensatory payment is made not directly by the individuals reproducing the works for personal use, but by persons who manufacture or import blank audio or video media and devices for recording or playback. This remuneration is payable in the order specified in Art.26 of CNRA to organizations representing various categories of right holders under the Act.

The newly adopted Art.25a of CNRA (effective as of 01.01.2003) provides that when using works pursuant to Art.24 and 25 without the consent of the copyright holder, such use can not be done in a way that is accompanied by a removal, damage, destruction or disruption of the technical means of protection without the consent of the copyright holder. That provision is an attempt of implementation into the national legislation of the rule of Art.6 of Directive 2001/29/EU obliging the EU member states to establish conditions for effective protection against actions designed to circumvent in any way the used technological means for protection against misuse of copyright subject matter.

It should be noted that both specified exceptions do not apply to software, to which the special rules of Art. 70 and 71 of CNRA, discussed in detail above, apply.

5.4. Features of the Works Published on the Internet as a Subject of Copyright and Problems of Legal Protection Thereof

The features of the works published on the Internet as a subject matter of copyright are determined by the specific form of their fixation. The digital form of fixation of these works

makes possible their unique, earlier impossible, physical properties and causes significant problems of their legal protection.

5.4.1. Technical and Legal Aspects

Below one can find listed the technical factors, to which published on the Internet works are subject, as well as the legal issues caused by those factors.

1) No loss of quality upon reproduction. Unlike copies of works made using analog copying methods (such as photocopying machines, video and audio tape recorders, fax machines, etc.), digital copies represent perfect copies without any loss in quality. The first digital copy is absolutely the same as the thousandth copy made from the same original. Since each copy is perfect, there are no qualitative restrictions that could prevent pirates from making as many copies as they want and recipients of the copies will feel no need to look for a legal source to make a copy that will not have a quality inferior to the original.

2) Marginal costs of reproduction and distribution costs. Unlike the practice of distribution of ordinary copies of books, magazines, music cassettes or CD's, video tapes or software, the cost of a copy placed on the Internet is insignificant, and the same goes for the costs associated with the delivery of this copy to the final user through the network. Given the fact that the cost of maintaining a website does not depend on the amount of information received from this site (such are the realities of today's telecommunications market), for pirates, violations of copyright are not accompanied by any significant costs.

3) Ability to act anonymously. Using contemporary technology, pirates are capable of operating on the Internet anonymously without leaving traces of their activities. Anonymity is one of the dangers on the Internet, since, at least in theory, it allows pirates to cause damages remaining unpunished, thus denying the general principle of law, under which persons causing damage have the obligation to compensate it. This will result in a large number of violations in a situation where they will remain unpunished compared to the cases in which their perpetrators will have to bear responsibility for what is done.

Anonymous activity, however, is not a specific problem of copyright, but it affects all crimes and torts carried out on the Internet. Thus it would be more appropriate to address the

problem of damage caused by anonymity as such rather than developing activities that protect only copyright holders. Moreover, there is something like a natural limit to the areas and scales of anonymous actions, particularly when those actions are of commercial nature. At some stage, the activity could become significant enough to leave at least circumstantial evidence (both in "real" and in "virtual" worlds), allowing for identification of the offender.[189]

3) Uneducated consumers. Many, if not the majority, of consumers do not understand the existing system of protection for copyrights[190]. The problem of uneducated consumers concerns both the "real" and the "virtual" domains, but the Internet allows those users to easily disseminate works which are protected by copyright. In many cases such spreading, even unintentionally, can cause damages, such as in the case of transmission to third parties of works which are protected by copyright and are obtained by the consumer in a lawful manner from the copyright holder. Thus, we can have a series of relatively minor offenses which in total could lead to significant losses for copyright holders.

5.4.2. Sociological and Cultural Aspects

Besides technical and legal aspects that have a significant impact on the situation with the protection of works published on the Internet, it is also worth considering some key issues related to consumer attitudes towards intellectual property in general and towards copyright in particular. Below are considered certain sociological and cultural aspects of the Internet community and their possible impact on the willingness of consumers to pay for the use of works available on the Internet and, respectively, on the desire to use objects protected by copyright in accordance with its rules.

Consumer attitudes towards copyright vary from the thesis that "intellectual property should not be subject to protection at all" to the imperative of a "mandatory and maximum quality protection of copyrights". Five major segments of that spectrum of opinions can be distinguished[191]:

---

[189] *See* Lance Rose. The Emperor's Clothes Still Fit Just Fine, Wired., February 1995, p. 103, 104; Philip E. Ross. Cops Versus Robbers in Cyberspace, Forbes., 9.09.1996, p. 134, 137

[190] *See* Jessica Litman, *The Exclusive Right to Read*, 3 Cardozo Arts & Ent. L. J. 29, 50-51 (1994).

[191] *See* Lance Rose. Is Copyright Dead on the Net, Wired., November 1993, p. 112

1) "Information should be free". Supporters of this thesis believe that any intellectual property must belong to the whole society and can be freely used by all its members. And although it is not easy to find sworn supporters of this idea, it is much easier to find people who believe that everything they find on the Internet can be used free of charge.

2) "Right of reference". Supporters of this idea believe that works can be used freely, provided their sources are specified. Maybe it will still be difficult to find unreserved supporters of this idea, but it is even more difficult to find people, even amongst authors, who have not at least occasionally resorted to its implementation in practice.

Unpleasant as it is, the requirement for the binding force of the reference is contained in the legislation of far from all countries and often does not apply to all categories of works [192](in this respect Bulgarian law represents an exception[193]), although standards of ethics formed amongst Internet users, as a rule, encourage references.

3) "Limited use of works". Supporters of this idea believe that artists creating objects of intellectual property should have certain rights to protect their works, but at the same time, they deny the absolute nature of the rights in question. Supporters of the idea of limited use of works are trying to strike a balance between the need to protect the rights of artists and the admissibility of violation of copyrights determined by their lifestyle or business needs.

This viewpoint with more or less accuracy reflects the position of contemporary copyright law in many jurisdictions, whereby parallel to a firm protection of copyright holders, under certain circumstances, free use of works is also permitted.

4) "Moral rights". By author's moral rights, should be understood his rights "to require recognition of his authorship of the work and to object to any twisting, distorting or other change of the said work or any other infringement on the work capable of harming the honor or reputation of the author".[194]

---

[192] Mark A. Lemley. Rights of Attribution and Integrity in On-line Communications, J. On-line L., 1995, Art. 2.
[193] Copyright and Neighboring Rights Act (amended State Gazette Issue 59 of July 20, 2007) , Art. 24 par. 3.
[194] Berne Convention for the Protection of Literary and Artistic Works. The Paris Act of July 24, 1971 as amended on October 2, 1979

In general, moral rights are a product of the idea that author's works represent an extension of the author himself, so the author can control the way society perceives the author through his works. In the relations between the author and any potential user (including assignees and licensees), the doctrine of moral rights provides indisputable advantages to the former, and in many jurisdictions, for instance in Bulgaria,[195] the author can not transfer (assign) his moral rights.

5) "Strong rights of authors". Supporters of this idea believe that the author should have substantial powers to control the use of his work. They would even go farer than moral rights, providing the author with the right to control all cases of use of his work.

For reasons related to the formation of state policy on protection of copyrights, it would be appropriate to consider the way, in which contemporary copyright could affect the behavior of people supporting the above views. It is important to note that supporters of the idea that "there must be freedom of information" are capable of going beyond the standards of copyright with great ease, regardless of strict penalties for violating them, whereby strengthening the standards of copyright in order to influence supporters of free use of information will have no particular effect.[196] Given the fact that owing to the Internet culture, the number of opponents of strong intellectual property rights has increased, a new legislation in the sphere of copyright directed at strengthening the rights of authors is unlikely to achieve the desired results.

From a historical perspective, things have developed in such a way that the role of Internet enthusiasts was occupied by technologists and scientists, many of whom can be associated with the supporters of the idea that "there must be freedom of information" (or with the supporters of the "right of reference").[197] With the course of time, another attitude has been brought towards intellectual property. Take, for example, the generation of people under 30 years of age. Almost all their lives they have had an easy access, often in their own homes, to a large number of devices that they could use for infringement of copyright: audio- and video-recorders (and relatively cheap blank tapes), high quality and cheap printing machines, faxes and perhaps the most powerful copying means – a PC. As a result, the generation od

[195] Copyright and Neighboring Rights Act (amended State Gazette Issue 59 of July 20, 2007), Art. 16.
[196] *See* Lance Rose. The Emperor's Clothes Still Fit Just Fine, Wired., February 1995, p. 104.
[197] Kathy Rebello. Making Money on the Net, Bus. Week., 27.09.1996.

people under 30 years of age grew up having the opportunity of easy and cheap expropriation of intellectual property. As for students, few of them have bought the majority (or even any) of the software for their computer, rather than just "borrow" the necessary programs from acquaintances or neighbors in the dormitory. And how many of them have instead compiled collections of their favorite songs? How many of them have overwritten music on a tape of theirs from one's records? Do mechanisms exist or can they to be invented, which could effectively convince such people that their actions are prohibited under the existing system?

The initial users of the Internet have joined the generation of those who have not yet reached 30 and together they formed an interesting Internet psychology. The Internet society with an increasing nihilism treats the attempts to prove that, say, sending e-mail messages to mailing lists[198] or the creation of a fan site of a certain movie [199]may represent a violation of copyright.

Moreover, since a large number of copyright holders freely part with valuable intellectual property, consumers develop a habit of expecting only free materials everywhere. In these circumstances, consumers do not make haste to pay for intellectual property, because they know that somewhere there must be a free alternative. The need to fulfill even the smallest of formalities, such as completing a registration form, discourages many users. The habit of free use increasingly complicates the ambition of copyright holders to receive fees from consumers.

Although the idea of making the Internet community legally literate looks absolutely real, attempts to change the network itself in order to bring its use in accordance with the existing standards of copyright will require significant efforts. Moreover, all aspirations for creating a system to fight "small violations" are doomed, because they are ineffective in terms of the ratio between public expenditure and the benefits to society.[200] In practice, over time, this approach can prove its ineffectiveness even for copyright owners.[201]

---

[198] *See* Mitch Betts. On-line Pay Per View, ComputerWorld, 5.06.1995, p. 58

[199] *See* Constance Sommer. Film Rights Falling Through the Net, San Jose Mercury News, 10.12.1996 r., p. 10E.

[200] *See* Margie Wylie. Can Copyright Survive the Digital Age? Should It?, Digital Media: A Seybold Report, 3.07.1995 r.; Steve G. Steinberg. Seek and Ye Shall Find (Maybe), Wired., May 1996.

[201] *See* Jessica Litman, The Exclusive Right to Read, 3 Cardozo Arts & Ent. L. J. 29, 46 (1994).

Way more workable seems a complex application of copyright methods and economic factors, namely the implementation on the Internet of the cross-subsidization models similar to those existing on the radio and television, where no charge is levied on the audience of certain programs, but deductions are made from organizations that broadcast them for the use of copyrighted materials, which are taken from funds received from advertisers.

5.5. Conclusions

Over the past decade, the Internet has truly become a foundation for the "information highway" of the future. Developing at amazing rates, today this "network of networks" has turned from a way of communication in education and research circles into an arena of intense competition.

Today, the Internet has turned into a major channel of communication of a wide variety of information on a global scale. This information is often transmitted through the Internet in the form of works subject to copyright protection of each party to the Berne Union, including Bulgaria and Romania, along with works fixed in more traditional forms, subject to compliance with the statutory criteria for protection provided by the law of the country, regardless of the fulfillment of any formalities.

However, it can be concluded that copyright holders face significant risks determined by the existence of information technologies. The cross-border nature of the Internet and the digital form of fixation of works available on the web significantly complicate the process of rights enforcement by authors and their successors.

However, we have clear evidence that objects of intellectual property continue to be created, including those created for distribution exclusively over the Internet. Indeed a huge, almost beyond calculation, quantity of objects of intellectual property continues to appear and disseminate on the Internet in spite of the above-mentioned problems.[202] Thus, despite the claims of those, according to whom the threats that information technologies pose for works protected by copyright will not contribute to their further creation and distribution, such claims lack factual foundation.

[202] See Steve G. Steinberg. Seek and Ye Shall Find (Maybe), Wired., May 1996, p. 108.

At the same time, it can be suggested that the combination of Internet culture with the general implications of technical evolution changes the attitude towards copyright in society. Culture today embraces the understanding of the need to protect copyright together with tolerance to small but numerous violations of the same. In other words, we want to respect other people's intellectual property rights, but, at the same time, we do not want to change our usual lifestyle associated with numerous, albeit small, almost domestic, but still unlawful acts. Attempts to change this attitude caused by social and cultural factors exclusively by means of copyright (or even worse – to impose much more stringent penalties), will not have the desired effect.

6. ONLINE FRAUD

6.1. Introduction

There is a wide range of known online frauds, many of which are simply existing types of fraud transferred to the online environment, e.g. Ponzi schemes (pyramid selling or investment). The Internet has, however, significantly lowered the cost of carrying out many of these types of fraud, as the use of e-mail, websites and bulletin boards, instant messaging and chat rooms, replaces mail and fax solicitations. This means that fraudsters can afford to target a much wider audience, and can thus successfully operate with much lower percentages of successful responses: for example, a fraudster who sends out 1000 postal solicitations may need 1% of those to generate successful frauds to break even, whilst a fraudster who sends out 1 000 000 e-mailed solicitations may only need 0.00001% of those to generate successful frauds to break even.

Frauds requiring the widespread dissemination of false information, e.g. 'pump and dump' stock schemes, are also facilitated by the availability of chat rooms, forums, internet boards and via email. These frauds also typically require a fairly rapid response by victims to provide a window for the fraudsters to make their gains before the scam is exposed, or the stock crashes. The Internet provides a variety of cheap, rapid, and often anonymous, avenues for such fraudsters to spread their false information. The massive growth in internet auction sites, e.g. eBay, has also provided fertile ground for a range of fraudulent activities.

As online technologies have developed, specific new types of frauds relating to those technologies have been created by fraudsters, e.g. phishing, pharming and click-though frauds. The online fraud environment is an ever-changing one, and further new frauds, as well as ever more sophisticated versions of existing frauds, can be expected. As law enforcement agencies and legal systems have developed methods of dealing with online fraudsters, and the general public has become more wary of entering into online relationships/transactions, so the fraudsters have developed both ever more convincing frauds and, increasingly, frauds which are effectively automated. Some of the latter frauds may potentially fall under both national computer misuse and fraud laws. Online frauds targeting consumers are often additionally the

subject of national consumer protection laws. Table 1, below, outlines key current online frauds.

Tackling online fraud is often made more complicated by the international reach of the Internet, which allows fraudsters to more easily target victims in other jurisdictions, and reduces the likelihood of successful actions by the victims' national law enforcement and consumer protection agencies. Law enforcement agencies (LEAs) in other jurisdictions are often unable, either practically or legally (or occasionally are simply unwilling), to provide effective aid to non-nationals. LEAs may also be hampered by:

- technological issues, such as the ability of fraudsters to act pseudonymously or anonymously, or to conduct their operations through a chain of online systems and/or services;
- legal issues, such as the difficulty of categorizing particular frauds under existing national laws, obtaining the evidence necessary to bring charges or secure a conviction, or demonstrating that the evidence collected meets the requirements for admissibility to the courts;
- information issues, such as a lack of knowledge amongst investigating officers, prosecutors and judiciary about the technology used, or the technical workings of an online fraud. In complex frauds, it may be difficult to explain such issues to lay persons, such as jurors, in a manner which allows them to comprehend the nature of the criminal activity being alleged.

Recent international online anti-fraud initiatives have tended to concentrate on harmonizing legal provisions to facilitate effective cross-border enforcement, in combination with cross-border co-operation initiatives (e.g. the exchange of data between national consumer protection agencies). These have been backed up by national consumer information schemes and consumer fraud reporting systems.

Table 1: Examples of online fraud

Fraud	Type of Fraud	Technical expertise	Nature of Fraud	Purpose of fraud
Identity theft	Offline/Online	Low	Stolen credit/debit card information is used to make purchases online. The stolen information may be obtained offline or online (see phishing below). Increased use of 'Chip & PIN' credit cards in the UK has seen a decline in offline credit card fraud, but a rise in online credit card fraud, where the card is not present.	Identity theft using credit/debit cards is usually carried out with the aim of obtaining high value products that can be easily sold on by the fraudster. Stolen cards are often used to purchase goods from online stores and sellers thereby avoided the security checks available/required during face-to face transactions.
Business frauds	Offline/Online	Low	There are a large number of business frauds that use online services such as e-mail , instant messaging and websites. Many of these originated as postal or fax frauds. They are often variants of the following frauds	
			A fraudster e-mails a business, individual or auction seller seeking to purchase goods using a credit card.	Credit card is stolen/forged, and if goods are shipped, the seller will not receive payment, or payment will be charged back by the card company
			A fraudster offers goods for sale, often at very cheap prices (common on auction websites).	Buyer sends payment, or a deposit, but does not receive the goods advertised, or receives substandard, faulty, or fake goods.
			A fraudster seeks to purchase goods from a business, individual or auction seller and offers to pay with a financial instrument, e.g. a check, which is for a sum larger than the price of the goods. The fraudster requests that the seller deduct their costs (and often a fee), and send the remaining money by check or wire back to the fraudster, or to a third party accomplice.	The financial instrument is a forgery, the seller will lose both the value of the goods sold, and the money returned to the fraudster or third party accomplice.
			A fraudster requests help in transferring money from a foreign company or out of a foreign country. This may be characterized as an employment offer, business deal or charitable action. The fraudster may request wire transfers from the victim to pay customs duties/administrative fees/bribes, or may send money orders, seeking a percentage of their value to be returned by the victim.	There is no money; the fraudster will simply steal any money sent to pay customs duties/administrative fees/bribes. Similarly, financial instruments sent to victims will be forged or stolen and thus valueless, and any money sent in return stolen.
			A fraudster persuades individuals or small businesses to reship goods on their behalf. This may be characterized as a job, business relationship, or other co-operative venture. When the victim accepts they are sent pre-printed package delivery company labels to apply to the goods to be shipped. They may also receive a financial instrument, e.g. a check, to cover the cost of reshipping. They then receive goods ordered by the fraudster from online companies. The victim relabels the boxes, which	The fraudster has used stolen credit cards to buy at different Internet sites simultaneously. Usually the correct billing address for the card is used, but the shipping address is the home of the victim. Often the fraudster has gathered sufficient information about the victim to create accounts with the package delivery company, resulting in the victim being billed for the reshipment. Where a financial instrument is sent to the victim to pay for the reshipping, it will be forged or stolen.

			are picked up by the package delivery company and shipped to the criminal's real address.	
Consumer frauds	Offline/Online	Low	There are a large number of business frauds that use online services such as e-mail (spam), instant messaging and websites. Many of these originated as postal or fax frauds. These range from financial frauds, such as 'Ponzi schemes' (pyramid selling), through business to consumer (B2C) and consumer to consumer (C2C) sales frauds, including sale of substandard, faulty, or fake goods, or failure to deliver any goods/services, to provision of goods which are sold despite being unlawful/unlicensed in the countries e.g. unlicensed or ineffective medical treatments and pharmaceuticals	
Short-selling schemes	Offline/Online	Low	False and/or fraudulent information is disseminated in chat rooms, forums, internet boards and via email with the purpose of causing a dramatic price decrease in stocks of a specific company	The fraudsters wait until the price has dropped to a certain level and then buy the stock, they then wait for the price to rise as it becomes clear that the rumours are false and then sell the stock at a profit.

Fraud	Type of Fraud	Technical expertise	Nature of Fraud	Purpose of fraud
Pump-and-dump schemes	Offline/Online	Low	False and/or fraudulent information is disseminated in chat rooms, forums, internet boards and via email with the purpose of causing a dramatic price increase in thinly traded stocks or stocks of shell companies.	Having bought the stock at a low price prior to the scam, when the price reaches a certain level (Pump), the fraudsters sell off their holdings before the stock price drops again (Dump) lightly-traded stock, thereby increasing its price leaving new investors with stock of little or no value.
		Medium	A more sophisticated form of pump and dump schemes involves the fraudster taking over (by hacking or by phishing attack) several victims' trading accounts with online brokerages, such as E*Trade, selling their existing holdings and using the funds to purchase lightly-traded stock, thus increasing its price.	Having bought the stock at a low price prior to the scam, when the price reaches a certain level (Pump), the fraudsters sell off their holdings before the stock price drops again (Dump) leaving the victims with devalued holdings.
Click-through fraud or click fraud	Online	Low to Medium	Many website advertisements are part of a pay-per-click system, where payments are made by the advertiser to the system owner on the basis of the number of times users click on their advertisements. The system owner then shares the revenue with the owners of the websites displaying the adverts. Example: Google's Adsense system. Click-through fraud involves clicking on pay-per-click website advertisements with the aim of gaining an advantage other than that specified by the advertiser.	There are two main purposes behind click fraud: Competition - A rival firm clicks on a competitor's online advertisement with the intent of imposing a cost rather than obtaining information about the advertised product or service. Revenue - A website owner hosting advertisements uses software or pays individuals to click on the adverts on their site to generate a revenue-sharing payment from the syndicating search engine rather than obtaining information about the advertised product or service.
Auction frauds	Online	Medium	A fraudster hijacks a legitimate seller's account (often via a phishing attack), usually one with high positive feedback, and sets up a fake online store.	Buyers send payment, but do not receive the goods advertised , or receive substandard, faulty, or fake goods. Personal and financial details provided by victims may be used for further identity theft.
Escrow frauds	Online	Medium to High	As buyers and sellers have become more cautious, particularly with online auctions, fraudsters may suggest the use of a third-party escrow service for the exchange of money and merchandise. Sometimes a genuine escrow service website is compromised and another fake site resembling it is created by the fraudsters (see Pharming), or the escrow service is simply a sham.	Buyers sending payment to the fake escrow service do not receive the goods. Sellers who send merchandise to the fraudster do not receive payment. Additionally if the sellers have disclosed credit card details to the fake escrow service, they may also be subject to identity theft by the fraudster.
Phishing	Online	Medium to High	Use of spam e-mails usually appearing to be from a financial institution, such as a bank, asking for information about online accounts, or for other personal and financial information. E-mails may contain a link to a fake website using code and graphics from the legitimate website. This provides any data entered, to the fraudster.	The primary purpose of phishing frauds is usually to gain unauthorized access to bank/credit card/Paypal accounts. Some phishing attacks are also used to gain unauthorized access to services, such as ISP and VoIP accounts – compromised accounts may be hijacked and used for spamming, denial of service attacks, etc.
Pharming	Online	High	Redirection of a website's traffic to another fake website,	Pharming is strongly linked to phishing, inasmuch as spam e-mails

			run by the fraudster, by changing the hosts file on a victim's computer, by compromise of a local network router, or by exploitation of a vulnerability in DNS server software (DNS servers are the machines responsible for resolving internet names into their real addresses). Attacks on a victim's computer or router can be made via the victim clicking on links in, or opening attachments to, e-mails.	are a primary attack vector. As with phishing, the main objectives of pharming frauds are usually to gain unauthorized access to bank/credit card/Paypal accounts etc. or to gain unauthorized access to services.

This table is derived from a range of sources including: The US Internet Crime Complaint Center <http://www.ic3.gov/>; and the UK Metropolitan Police Sterling Initiative <http://www.met.police.uk/fraudalert/>.

6.2. International Responses

As with other areas of online criminality, supranational bodies, such as the OECD, Council of Europe and European Union, have highlighted the fact that, without cross-border co-operation, tackling online fraud will be all but impossible. As a result, there have been numerous international initiatives aimed at combating online fraud, and/or ensuring online/cross-border consumer protection. The aims of these initiatives have been to ensure that participating nations have:

- adopted adequate national legal measures to provide criminal law solutions to online fraud, including adapting existing laws so that they are technology neutral, or are capable of application to both existing forms of off-line fraud, and to frauds facilitated by new technologies;
- attempted to harmonize those national legal criminal law measures and connected provisions as far as possible , with the aim of facilitating LEA co-operation and expedited systems of extradition;
- put in place cross-border co-operation mechanisms between LEAs and other regulatory bodies, including national fraud prevention and consumer protection agencies.

There have also been numerous initiatives which, while not specifically targeted at online fraud, have an impact upon it, such as agreements relating to computer systems and network security.

6.2.1. The United Nations

In 1990, the 8th United Nations Congress on the Prevention of Crime and the Treatment of Offenders approved a resolution requesting Member States to increase their efforts to fight computer-related crimes by adopting, if necessary, the following measures:

- modernization of national criminal laws and procedures;
- improvement of computer security and prevention measures;
- adoption of adequate training measures; and,
- elaboration of rules of ethics in the use of computers.

It also recommended that the United Nations Committee on Crime Prevention and Control should promote the development and dissemination of a comprehensive framework of guidelines and standards to assist Member states in dealing with computer-related crime. In

1994, the U.N published the United Nations Manual on the Prevention and Control of Computer Related Crime. This Manual examined issues surrounding computer related crimes, substantive criminal laws protecting privacy, procedural law, and the needs and avenues for international cooperation.

A Resolution on combating the criminal misuse of information technologies was adopted by the General Assembly on December 4, 2000 (A/res/55/63), that stated:

"(a) States should ensure that their laws and practice eliminate safe havens for those who criminally misuse information technologies;

(b) Law enforcement cooperation in the investigation and prosecution of international cases of criminal misuse of information technologies should be coordinated among all concerned States;

(c) Information should be exchanged between States regarding the problems that they face in combating the criminal misuse of information technologies;

(d) Law enforcement personnel should be trained and equipped to address the criminal misuse of information technologies;

(e) Legal systems should protect the confidentiality, integrity and availability of data and computer systems from unauthorized impairment and ensure that criminal abuse is penalized;

(f) Legal systems should permit the preservation of and quick access to electronic data pertaining to particular criminal investigations;

(g) Mutual assistance regimes should ensure the timely investigation of the criminal misuse of information technologies and the timely gathering and exchange of evidence in such cases;

(h) The general public should be made aware of the need to prevent and combat the criminal misuse of information technologies;"

6.2.2. The G-8

In 1997, the G-8 created a Subcommittee on High-Tech Crime. This has focused its efforts on:

- establishing an international network of 24-hour high-tech points of contact to facilitate law enforcement communications for investigations.
- developing computer forensic principles for circumstances where digital evidence retrieved in one country required authentication in the courts of another country
- making recommendations for tracing terrorist and criminal communications across borders.

In December 1997 the G8 adopted ten Principles to Combat High-Tech Crime and ten point Action Plan to Combat High-Tech Crime (see below). Key principles included:

- development of comprehensive substantive and procedural computer crime laws at international level;
- coordination of the investigation and prosecution of international high-tech crimes;
- protection of the confidentiality, integrity, and availability of data and systems from unauthorized impairment and ensuring that serious abuse is penalized;
- co-ordination of the work of the G8 in the area of high-tech crime with the work of other relevant international fora to ensure against duplication of efforts.

6.2.3. Council of Europe

The Council of Europe adopted the *Convention on Cybercrime* (ETS 185) in 2001. The Convention aims to harmonize national criminal substantive law elements of offences and connected provisions in the area of cyber-crime (Chapter II, Section 1, Titles 1-5); to provide for domestic criminal procedural law powers necessary for the investigation and prosecution of such offences (Chapter II, Section 2, Titles 1-5); and to establish a fast and effective regime of international co-operation (Chapter III, Section 1, Titles 1-4 & Section 2, Titles 1-3). It was drawn up by the Council of Europe in Strasbourg with the active participation of the Council of Europe's observer states Canada, Japan and USA. It has been ratified by 22 Council of Europe member states, and is also open to non- member states, of which one, the United States, has ratified. Section 1 of Chapter II (substantive law issues) covers both incrimination provisions and other connected provisions in the area of computer or computer-related crime, and includes sections on computer-related forgery and computer-related fraud:

Article 7 – Computer-related forgery

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.

Article 8 – Computer-related fraud

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:
a) any input, alteration, deletion or suppression of computer data,
b) any interference with the functioning of a computer system,
with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.

Both Article 7 and Article 8 contain broad definitions, and some of the types of offences potentially caught under these headings are, in jurisdictions like the UK, caught under specific computer misuse legislation rather than under the heading of computer or online fraud. However, it is clear that identity fraud techniques, including spyware, packet sniffers, keylogging as well as phishing messages "[which] pretend to be legitimate invitations to submit personal information, for instance as fake PayPal, e-Bay or banking requests, referring to fake websites or using the 'cross-site scripting' that exploits security weaknesses in legitimate sites to unlawfully collect data" (de Hert, González Fuster & Koops 2006) would also fall under provisions within the Convention.

With regard to procedural legal issues, the Convention requires states to establish a minimum set of national procedural tools so that LEAs within a state have sufficient authority to conduct certain types of investigations specific to computer crime offenses. Such procedural powers include: expedited preservation of stored data, expedited preservation and partial disclosure of traffic data, production orders, search and seizure of computer data, real-time collection of traffic data and interception of content data.

The Convention also provides a set of general principles in the areas of international co-operation, extradition, mutual assistance, and spontaneous information, notably that:

- international cooperation will be provided among states "to the widest extent possible;
- the obligation to cooperate extends not only to the crimes established in the treaty, but also to the collection of electronic evidence whenever it relates to a criminal offense
- provisions for international cooperation do not supersede pre-existing provisions of international agreements on these issues.

Rules are also provided on extradition of suspects under specific conditions (again deferring to pre-existing treaties or alternative extradition arrangements), as well as on the establishment of other forms of co-operation in the field of criminal investigation and prosecution, such as a network of contact points with a 24/7availability, to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

6.2.4. The OECD

The OECD has played an important role in stimulating international action against cross-border fraud, with the aim of securing consumer trust in, and the growth of, the global digital economy. In 1999, the *Guidelines for Consumer Protection in the context of Electronic Commerce* suggested that OECD Member countries should combat cross-border fraud through increased "information exchange, coordination, communication and joint action" among "judicial, regulatory, and law enforcement authorities."

The OECD *Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices across Borders* were adopted in June 2003. They establish a common framework to combat cross-border fraud occurring online and offline through closer, faster, and more efficient co-operation between consumer protection enforcement agencies (CPEAs). The key elements of the Guidelines are that:

Domestic frameworks for combating cross-border fraudulent and deceptive commercial practices

- Member countries should have an effective framework of laws, CPEAs, institutions, practices, and joint initiatives to limit fraudulent/deceptive commercial practices against consumers.
- Member countries should ensure their CPEAs have the authority to obtain evidence sufficient to investigate and take action in a timely manner against fraudulent/deceptive commercial practices.
- Member countries should have appropriate judicial or administrative mechanisms to permit CPEAs to preserve evidence, particularly that of a transient nature, until it can be

examined, including where CPEAs are assisting agencies in other countries, subject to appropriate safeguards.

- Member countries should develop mechanisms for co-operation and information sharing between and among their own CPEAs and their other LEAs, for the purpose of combating fraudulent/deceptive commercial practices
- Member countries should identify and remove obstacles to effective cross-border co-operation in the enforcement of laws designed to protect consumers against fraudulent/deceptive commercial practices in their domestic frameworks
- Member countries should educate consumers about fraudulent/deceptive commercial practices, undertaking joint initiatives as appropriate
- Member countries should consider how, in appropriate cases, their own CPEAs might use evidence, judgments, and enforceable orders obtained by a CPEA in another country to improve their ability to prevent the same conduct in their own countries

Principles for international cooperation

- Member countries should improve their ability to co-operate in combating cross-border fraudulent/deceptive commercial practices whilst recognizing that co-operation on particular investigations or cases remains within the discretion of the CPEA being asked to co-operate.
- CPEAs should co-ordinate their investigations and enforcement activity to avoid interference with the investigations and enforcement activity of CPEAs taking place in other Member countries.
- CPEAs should attempt to resolve disagreements as to co-operation that may arise.
- Member countries and their CPEAs should make use of existing international networks and enter into appropriate bilateral or multilateral arrangements or other initiatives.
- Member countries should enable their consumer protection policy agencies (CPPAs) in consultation with CPEAs to take a leading role in developing the framework for combating fraudulent/deceptive commercial practices
- Member countries should designate a CPEA or a CPPA to act as a contact point to facilitate co-operation under the Guidelines.

Notification, information sharing, assistance with investigations, and confidentiality

- Member countries and their CPEAs should promptly, systematically and efficiently notify CPEAs in other Member countries of investigations affecting those countries.
- Member countries should improve the abilities of CPEAs to share information within timeframes that facilitate investigations of matters involving fraudulent and deceptive commercial practices against consumers, notably:
- publicly available and other non-confidential information;
- consumer complaints;
- information allowing quick location/identification of those engaged in fraudulent/deceptive commercial practices (e.g. addresses, Internet domain registrations);
- expert opinions and the underlying information on which those opinions are based; and
- documents, third-party information, etc. obtained via judicial/other compulsory processes.
- Member countries should work together to develop fast, efficient methods for gathering and sharing information, to counter the speed at which those engaged in fraudulent and deceptive commercial practices can victimise large numbers of consumers, e.g. through the Internet.
- Member countries should address the dispersal of evidence across multiple jurisdictions by authorising their CPEAs, directly or via appropriate judicial/administrative mechanisms, to obtain information and provide investigative assistance to foreign CPEA investigations and actions, subject to appropriate safeguards.
- Member countries, their CPEAs, and other competent authorities should work together, and with domain name registrars and other relevant stakeholders, to reduce the incidence of false header and routing information and inaccurate information about holders of domain names
- Member countries should maintain the necessary confidentiality of information exchanged under the Guidelines, especially when sharing confidential business or personal information.

Authority of consumer protection enforcement agencies

- all CPEAs whose territories are affected by fraudulent and deceptive commercial practices against consumers should have appropriate authority to investigate and take action within their own territory.
- Member countries should enable their CPEAs to take action against domestic businesses engaged in fraudulent and deceptive commercial practices against foreign consumers.
- Member countries should enable their CPEAs to take action against foreign businesses engaged in fraudulent and deceptive commercial practices against their own consumers.
- The previous 3 points may be subject to other bilateral arrangements between countries, or other arrangements within a regional economic integration organization.

Consumer redress

- Member countries should jointly study the role of consumer redress in addressing the problem of fraudulent and deceptive commercial practices, devoting special attention to the development of effective cross-border redress systems.

Private-sector co-operation

- Member countries should co-operate with businesses, industry groups, and consumer groups to further the goals of the Guidelines, and should solicit their input and support, in particular on consumer education, and encourage their referral of relevant complaints to CPEAs.

The Guidelines have been recognized at the international level as an effective means to address fraudulent and deceptive commercial practice against consumers, e.g. the Free Trade Agreement ("AUSFTA") signed between Australia and the United States, which entered into force in January 2005, explicitly recognizes the Guidelines, as a valuable existing mechanism for enforcement co-operation in relation to consumer protection. Several consumer protection enforcement agencies in OECD Member countries have implemented informal arrangements to improve such information sharing, e.g. the signing of Information Sharing Protocols between the Competition Bureau Canada, the US FTC, the ACCC, and the United Kingdom Office of Fair Trading ("UK OFT"), between 2003 and 2004. Further details about national OECD Member country implementation actions can be found in the OECD's *Report on the Implementation of the 2003 OECD Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices across Borders* (2006).

6.2.5. The European Union

Generally, EU legislation does not provide an integrated approach to online fraud and cybercrime laws. However, as early as 2001, the Council of Ministers endorsed the G8 24-hour information network for combating high-tech crime, and recommended that Member States join - *Council Recommendation on Contact Points Maintaining a 24-Hour Service for Combating High-Tech Crime* (2001). This proposal has been more recently addressed in Article 11 of the *Council Framework Decision on attacks against information systems* (2005/222/JHA), which states that "Member States should … make use of the existing network of operational contact points referred to in the Council Recommendation of 25 June 2001 on contact points maintaining a 24-hour service for combating high-tech crime for the exchange of information."

The European Commission has also specifically recognized the OECD Guidelines as an important step in addressing the issue of cross-border fraud at the international level. This recognition is also reflected in the adoption of the EU *Co-operation between National Authorities Responsible for the Enforcement of Consumer Protection Laws Regulation* (2006/2004/EC) which aims to institute an integrated EU consumer protection enforcement network, and which contains many similar principles to those found in the Guidelines. As it is a Regulation, it is directly applicable and binding in the EU Member States without the need for any national implementing legislation.

The Regulation establishes a network of authorities responsible for monitoring the application of legislation concerning consumers. The aim is to ensure compliance with the legislation and the smooth functioning of the internal market. The Regulation applies only to intra-Community infringements of consumer protection legislation.

Each Member State designates the Competent Authorities and a Single Liaison Office responsible for the application of the Regulation. These Competent Authorities have the investigation and enforcement powers necessary for the application of the Regulation and exercise them in conformity with national law. The Competent Authorities must act without delay to put a stop to any infringement identified, using the appropriate legal instrument. In most cases this will be an injunction, which allows action to be taken quickly. Injunctions make it possible to stop or prohibit unlawful activities and take rogue traders to court in other Member States.

Under Article 8(3) CPC, Competent Authorities can effectively sub-contract the enforcement of cross-border cases to other enforcement bodies having a legitimate interest in the cessation of consumer law breaches in their jurisdiction (Article 8(3) bodies)

The Regulation establishes a framework for mutual assistance which covers the exchange of information, requests for enforcement measures and coordination of market surveillance and enforcement activities. When a Competent Authority becomes aware of an intra-Community infringement it must notify the Competent Authorities of other Member States, and the Commission. It also supplies, at the request of another Competent Authority, all relevant information required to establish whether an intra-Community infringement has occurred. In addition, it must take all necessary enforcement measures to bring about the cessation or prohibition of the intra-Community infringement.

The Competent Authorities inform the Commission of intra-Community infringements, the measures taken and the effect thereof, and the coordination of their activities. Information communicated may only be used for the purposes of ensuring compliance with the laws that protect consumers' interests. The Commission stores and processes the information it receives in an electronic database. Requests for mutual assistance must contain sufficient information to enable a Competent Authority to fulfill the request. In certain circumstances a Competent Authority may refuse to comply with a request for enforcement measures or information or decide not to fulfill its obligations. In this case it informs the applicant a Competent Authority, and the Commission, of the grounds for refusing to comply with a request for assistance.

Member States inform each other and the Commission of their activities of Community interest in certain areas, such as:

- enforcement coordination: the training of their CPEA officials, the collection and classification of consumer complaints;
- administrative cooperation: provision of consumer information and advice, support of the activities of consumer representatives.

It should also be noted that the EU member states have ratified the EUROPOL Convention, which provides for a framework of police cooperation against organized crimes, including cyber-criminality.

Application of Fraud Laws and other Regulatory Strategies to the Online Environment

As can be seen from the foregoing, when it comes to the application of national fraud laws and other regulatory strategies to the online environment, the international experience suggests there are several key elements that will influence the likely level of success. National governments need to:

- examine their existing fraud and related laws to ensure that these mesh to form an internally consistent system, and that they are capable of application to the online environment/the use of new technologies, i.e. they are not drafted in such a way as to exclude, limit or impede their use by LEAs and CPEAs;
- ensure that legislators, regulators, LEAs, CPEAs and members of the judiciary and legal professions have an adequate understanding of the technologies and techniques that they are being asked to oversee, e.g. when members of the judiciary are faced with instances of 'phishing' and 'pharming', they should be able to understand how the technology is being used, identify when and how the law is being broken, and apply appropriate legal sanctions;
- ensure that in fraud cases appropriate evidence can be obtained and shared by national LEAs and CPEAs, both nationally and, as appropriate, internationally - ideally through international networks of competent authorities which can handle information promptly, systematically and efficiently;
- involve the private sector, including businesses, industry groups, and consumer groups, both in terms of education and consultation (i.e. taking advantage of private sector expertise), and in terms of seeking to engage private sector organizations in regulatory processes, such as involving sectoral groups in self-regulatory practices which deter fraudulent behavior e.g. Internet Service Providers, domain name registrars etc.

6.3. The UK Approach

In the UK, these issues have already been addressed to some degree. In addition to ensuring that it has adopted appropriate measures to comply with its international obligations/requirements, including involvement in the G8 24-hour information network, the UK Office of Fair Trading has signed Information Sharing Protocols between itself and a range of other countries' competition/consumer protection bodies. With regard to the EU *Co*-

operation between National Authorities Responsible for the Enforcement of Consumer Protection Laws Regulation (CPC), the UK has appointed the Office of Fair Trading as its Single Liaison Office, and a number of bodies, including the OFT, the Civil Aviation Authority (CAA), Ministry of Trade and Industry (Gibraltar), Financial Services Authority (FSA) and the Medicines and Health Regulation Authority (MHRA) as Competent Authorities. Additionally a number of Article 8(3) bodies have been authorized, including ICSTIS (premium rate phone regulator). The OFT is also involved with the International Consumer Protection and Enforcement Network (ICPEN)

In 2006, a new Fraud Act was passed, which sought to simplify the existing law, much of which was contained in the Theft Acts of 1968/1978, and which was considered to be unsuitable to the current legal environment, as the nature of fraud has changed considerably over recent years, largely as a consequence of new technology. The Fraud Act is not the only criminal provision which can be used against criminal/fraudulent behavior (e.g. consumer protection laws) but provides a new approach for combating fraud.

The Act creates a general offence of 'fraud', in place of eight specific statutory crimes, such as 'obtaining property by deception,' and a common law offence of 'conspiracy to defraud'. The new offence is punishable by up to 10 years in prison and/or a fine.

There are three ways of committing fraud under the new Act:

- False representation – this replaces the offence of obtaining property by a lie, a trick or a deception but also includes offences such as fraudulent references, qualifications or, fictitious entries on a CV. It appears that this would also catch 'phishing' inasmuch as a person who sends phishing e-mails is falsely representing that the email has been sent by a legitimate financial institution.
- Failing to disclose information – such as the failure to disclose unspent criminal convictions or other matters when there is a legal or other obligation to do so
- Abuse of position –for example, where an employee copies his employer's client database for the purpose for setting up a rival company

Two basic requirements must be met before a party can be charged under any of these three heads:

- the behaviour of the defendant must be dishonest;
- the defendant must intend to make a gain, or cause a loss to another.

However, there is no need to prove that a gain or loss has in fact been made, or that any victim was deceived by the defendant's behaviour.

As well as introducing the offence of fraud, the Act also creates two new offences designed to target technology fraud - 'obtaining services dishonestly' and 'possessing articles for use in frauds'. The former is likely to be used to prosecute internet credit card fraud, whilst the latter would criminalise 'phishing kits' permitting the sending of e-mails in bulk, purporting to represent a well-known brand, in the hope of tricking victims to access a bogus website that, for example, misleads them into disclosing bank account details.

In terms of private sector involvement in reducing online fraud, there are a number of private sector initiatives, many of which aim to educate users about avoidance of online fraud, or to permit users to report potential frauds e.g.

Banksafe Online	Cardwatch
http://www.banksafeonline.org.uk/	http://www.cardwatch.org.uk/
Educational and Reporting	Educational

6.4. G8 Principles and Action Plan to Combat High-Tech Crime

(10 principles and a 10 point action plan)

Statement of Principles

We hereby endorse the following PRINCIPLES, which should be supported by all countries:

- There must be no safe havens for those who abuse information technologies.
- Investigation and prosecution of international high-tech crimes must be coordinated among all concerned States, regardless of where harm has occurred.
- Law enforcement personnel must be trained and equipped to address high-tech crimes.
- Legal systems must protect the confidentiality, integrity, and availability of data and systems from unauthorized impairment and ensure that serious abuse is penalized.
- Legal systems should permit the preservation of and quick access to electronic data, which are often critical to the successful investigation of crime.
- Mutual assistance regimes must ensure the timely gathering and exchange of evidence in cases involving international high-tech crime.
- Trans-border electronic access by law enforcement to publicly available (open source) information does not require authorization from the State where the data resides.
- Forensic standards for retrieving and authenticating electronic data for use in criminal investigations and prosecutions must be developed and employed.
- To the extent practicable, information and telecommunications systems should be designed to help prevent and detect network abuse, and should also facilitate the tracing of criminals and the collection of evidence.
- Work in this area should be coordinated with the work of other relevant international fora to ensure against duplication of efforts.

Action Plan

In support of these PRINCIPLES, we are directing our officials to:

- Use our established network of knowledgeable personnel to ensure a timely, effective response to transnational high-tech cases and designate a point-of-contact who is available on a twenty-four hour basis.

- Take appropriate steps to ensure that a sufficient number of trained and equipped law enforcement personnel are allocated to the task of combating high-tech crime and assisting law enforcement agencies of other States.
- Review our legal systems to ensure that they appropriately criminalize abuses of telecommunications and computer systems and promote the investigation of high-tech crimes.
- Consider issues raised by high-tech crimes, where relevant, when negotiating mutual assistance agreements or arrangements.
- Continue to examine and develop workable solutions regarding: the preservation of evidence prior to the execution of a request for mutual assistance; trans-border searches; and computer searches of data where the location of that data is unknown.
- Develop expedited procedures for obtaining traffic data from all communications carriers in the chain of a communication and to study ways to expedite the passing of this data internationally.
- Work jointly with industry to ensure that new technologies facilitate our effort to combat high-tech crime to preserving and collecting critical evidence.
- Ensure that we can, in urgent and appropriate cases, accept and respond to mutual assistance requests relating to high-tech crime by expedited but reliable means of communications, including voice, fax, or e-mail, with written confirmation to follow where required.
- Encourage internationally recognized standards-making bodies in the fields of telecommunications and information technologies to continue providing the public and private sectors with standards for reliable and secure telecommunications and data processing technologies.
- Develop and employ compatible forensic standards for retrieving and authenticating electronic data for use in criminal investigations and prosecutions.

7. PORNOGRAPHY DISSEMINATION ONLINE

7.1. Introduction

The primary problem with tackling the issue of online pornography is that the issue of what the term 'pornography' should cover is a highly subjective one. The term 'pornography' itself is often avoided in legal drafting because of this subjectivity - one person's 'pornography' may well be another's 'great work of literature or art', ' protected social political or sexual statement', or just holiday photographs.

> "What is viewed as pornographic varies from one person to another, from culture to culture, and over time. The term "pornography" can be used in discussion and debate to refer broadly to material that is sexually explicit, or more specifically to sexually explicit material designed primarily to produce sexual arousal in viewers, or to sexually explicit material that subordinates women or is harmful to women and children, or with some other definition in mind." (*Casavant & Robertson, 2007*)

For example, in the UK, despite the popularity of the use of the word 'pornography' in the media, the term has largely avoided in the relevant national legislation, which has until recently concerned itself rather with whether the material in question is 'obscene' or 'indecent'. However, while this means that the courts have not been caught up in an argument as to what is or is not 'pornographic', as matters stand neither 'obscene' nor 'indecent' lend themselves easily to clear definitions either, and this difficulty of definition is reflected in both the UK legislation and existing caselaw. With the passage of the UK *Criminal Justice and Immigration Act 2008* (see below), UK criminal law does now define an 'extreme pornographic image', as an image that:

- is of such a nature that it must reasonably be assumed to have been produced solely or principally for the purpose of sexual arousal; and is NOT part of a sequence of images which in context are not pornographic;
- AND portrays, in an explicit and realistic way, any of the following;
    - an act which threatens a person's life,
    - an act which results, or is likely to result, in serious injury to a person's anus, breasts or genitals,
    - an act which involves sexual interference with a human corpse, or

- a person performing an act of intercourse or oral sex with an animal (whether dead or alive)
- AND a reasonable person looking at the image would think that any such person or animal was real

- AND is grossly offensive, disgusting or otherwise of an obscene character.

This can perhaps be taken as a demonstration of how difficult it can be to create a comprehensible, and yet appropriately narrowly construed, definition of a sub-category of pornography.

In most, if not all, countries there is a clear understanding that the creation of pornographic material involving children justifies criminalisation. However, even here there are significant disagreements between countries over what 'child pornography' should cover. Some countries consider child pornography to include material involving persons under the age of 18, others have set the level at material involving persons under the age of 16. Some countries criminalize creation, offering, dissemination, procuring and possession of child pornography; others restrict incrimination to creation, offering and dissemination. Some countries require evidence that an actual minor was involved in the creation of the pornography, others also criminalize materials that appear to involve a minor (e.g. where a person over the age of 18 pretends to be under 18, or where innocent images of minors are merged with pornographic images), and/or images that depict minors engaged in sexual activity (e.g. sketches or comic strips).

These significant cultural differences have made developing a coherent international legal response to the regulation of 'pornographic' material online extremely difficult. The availability of 'pornographic' material, other than child pornography, on the internet is widespread, and the applicability of national laws to providers running websites, e-mail lists, and other distribution mechanisms which are based outside the country in question is often limited. Some countries have sought to tackle the issue by placing legal requirements upon Internet Service Providers (ISPs) within their jurisdiction. Such requirements may include: blocking particular websites, or ranges of IP addresses; installation of filtering software to prevent users downloading particular types of material; and passing information about users accessing such material to the authorities. Countries with a single ISP (often state-owned) have tended to find such approaches more feasible than countries with competing private sector ISPs, where the

imposition of such legal obligations upon ISPs may be argued to have a significant anti-competitive effect. Countries with constitutional freedom of speech provisions may also find that imposing filtering or other ISP-based blocking technologies will fall foul of those provisions, where they may also prevent lawful material from being disseminated, or deny access to materials that adults are entitled to view in order to protect children.

7.2. International Responses

7.2.1. United Nations and ILO

Following the International Conference on Combating Child Pornography on the Internet, held in Vienna in 1999, which called for the worldwide incrimination of the production, distribution, exportation, transmission, importation, intentional possession and advertising of child pornography, and stressing the importance of closer cooperation and partnership between Governments and the Internet industry, the United Nations General Assembly adopted the Protocol on the Sale of Children, Child Pornography and Child Prostitution (Sale of Children Protocol)

The Sale of Children Protocol was the first international instrument to define the term "child pornography. It requires states parties to treat acts relating to such conduct as criminal offenses, and provides for cooperative law-enforcement mechanisms to prosecute offenders. It also established broad grounds for jurisdiction over offenses and commitments to extradite offenders, with the aim of ensuring that offenders can be prosecuted regardless of where they are found.

Sale of Children Protocol

Article 2

[...]

(c) Child pornography means 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. Each State Party shall ensure that, as a minimum, the following acts and activities are fully covered under its criminal or penal law, whether such offences are committed domestically or transnationally or on an individual or organized basis:

[...]

(c) Producing, distributing, disseminating, importing, exporting, offering, selling or possessing for the above purposes child pornography as defined in article 2.

The Protocol also complements the International Labour Organisation (ILO) Convention (No. 182) on the Worst Forms of Child Labor, adopted by the International Labour Conference in 1999, which requires that states parties take immediate and effective action to secure the elimination of the use, procuring, or offering of a child for, amongst other things, the production of pornography, or pornographic performances.

ILO Convention (No. 182) on the Worst Forms of Child Labor

Article 2

For the purposes of this Convention, the term "child" shall apply to all persons under the age of 18.

Article 3

For the purposes of this Convention, the term "the worst forms of child labour" comprises:

[...]

(b) the use, procuring or offering of a child for prostitution, for the production of pornography or for pornographic performances;

[...]

(d) work which, by its nature or the circumstances in which it is carried out, is likely to harm the health, safety or morals of children.

In many countries, the age of sexual consent is set between thirteen and sixteen, and if a child of that age has consented to a sexual act, no crime involving child prostitution or child pornography has been committed. The Protocol requires states parties to criminalize activities relating to child prostitution and child pornography, without reference to state law or the ageof consent.

It does not specifically define the term "child," but states parties to the Convention on the Rights of the Child are bound by Article 1, which defines "child" as "every human being below the age of eighteen years unless, under the law applicable to the child, majority is attained earlier."

While these initiatives were not solely aimed at the issue of child pornography available online, it is clear that the apparent increasing availability of such online material was a key driver in their passage.

7.2.2. Council of Europe

The Council of Europe adopted the Convention on Cybercrime (ETS 185) in 2001. The Convention aims to harmonize national criminal substantive law elements of offences and connected provisions in the area of cyber-crime (Chapter II, Section 1, Titles 1-5); to provide for domestic criminal procedural law powers necessary for the investigation and prosecution of such offences (Chapter II, Section 2, Titles 1-5); and to establish a fast and effective regime of international co-operation (Chapter III, Section 1, Titles 1-4 & Section 2, Titles 1-3). It was drawn up by the Council of Europe in Strasbourg with the active participation of the Council of Europe's observer states Canada, Japan and USA. It has been ratified by 22 Council of Europe member states, and is also open to non- member states, of which one, the United States, has ratified. Section 1 of Chapter II (substantive law issues) covers both incrimination provisions and other connected provisions in the area of computer or computer-related crime, and includes a provision dealing with the issue of child pornography, which is the only content-related offence. All offences in the Convention, including those relating to child pornography, must be committed deliberately and 'without right'. The provision was intended to mirror the Optional Protocol to the United Nations Convention on the Rights of the Child in its coverage of child pornography.

Article 9 – Offences related to child pornography

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:

a) producing child pornography for the purpose of its distribution through a computer system;

b) offering or making available child pornography through a computer system;

c) distributing or transmitting child pornography through a computer system;

d) procuring child pornography through a computer system for oneself or for another person;

e) possessing child pornography in a computer system or on a computer-data storage medium.

2. For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts:

a) a minor engaged in sexually explicit conduct;

b) a person appearing to be a minor engaged in sexually explicit conduct;

c) realistic images representing a minor engaged in sexually explicit conduct.

3. For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.

4. Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.

The Explanatory Memorandum to the Convention defines 'sexually explicit conduct' as including: 'a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, between minors, or between an adult and a minor, of the same or the opposite sex; b) bestiality; c) masturbation; d) sadistic or masochistic abuse in a sexual context; or e) lascivious exhibition of the genitals or the pubic area of a minor. It also provides that 'national standards' will determine what constitutes pornography . States can enter reservations concerning procuring and possessing child pornography, and for images of adults which appear as children or of morphed or computer generated images where no child is violated (pseudo-photographs) The Convention does not specify levels of punishment leaving this to State Parties, but Article 13 requires punishments that are 'effective, proportionate and dissuasive'.

The Council of Europe has taken a further step in tackling online child pornography, since the Cybercrime Convention, with the adoption of the *Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse* (CETS 201) which was opened for signature in October 2007. Twenty nine Member States of the Council of Europe have signed it, although at time of writing there have been no ratifications. The Convention will enter into force when there are 5

Ratifications, including at least 3 Member States of the Council of Europe. The Convention is wide ranging, requiring State Parties to amongst other things:

- take preventive measures including the screening, recruitment and training of people working in contact with children, making children aware of the risks and teaching them to protect themselves, as well as monitoring measures for offenders and potential offenders.
- establish programmes to support victims, encourage people to report suspected sexual exploitation and abuse, and set up telephone and internet helplines for children.
- ensure that certain types of conduct are classified as criminal offences, such as engaging in sexual activities with a child below the legal age and child prostitution and pornography.
- criminalise the use of information and communication technologies– the internet in particular – to sexually harm or abuse children, for example by "grooming", (e.g. befriending and establishing an emotional connection with a child, in order to lower the child's inhibitions in preparation for sexual abuse).

Article 20 – Offences concerning child pornography

1 Each Party shall take the necessary legislative or other measures to ensure that the following intentional conduct, when committed without right, is criminalised:

a producing child pornography;

b offering or making available child pornography;

c distributing or transmitting child pornography;

d procuring child pornography for oneself or for another person;

e possessing child pornography;

f knowingly obtaining access, through information and communication technologies, to child pornography.

2 For the purpose of the present article, the term "child pornography" shall mean any material that visually depicts a child engaged in real or simulated sexually explicit conduct or any depiction of a child's sexual organs for primarily sexual purposes.

3 Each Party may reserve the right not to apply, in whole or in part, paragraph 1.a and e to the production and possession of pornographic material:

– consisting exclusively of simulated representations or realistic images of a non-existent child;

– involving children who have reached the age set in application of Article 18, paragraph 2, where these images are produced and possessed by them with their consent and solely for their own private use.

4 Each Party may reserve the right not to apply, in whole or in part, paragraph 1.f.

[…]

Article 23 – Solicitation of children for sexual purposes

Each Party shall take the necessary legislative or other measures to criminalise the intentional proposal, through information and communication technologies, of an adult to meet a child who has not reached the age set in application of Article 18, paragraph 2, for the purpose of committing any of the offences established in accordance with Article 18, paragraph 1.a, or Article 20, paragraph 1.a, against him or her, where this proposal has been followed by material acts leading to such a meeting.

While in large measure the Convention Articles 20-23 appear to replicate other international initiatives such as those of the UN, ILO and EU (see below), it is suggested in the Explanatory Memorandum that it is designed to address a perceived lack of exhaustive national criminal legislation in the State Parties, especially as concerns trafficking of children, "sex tourism" and child pornography, the lack of a clearly defined minimum age for consenting sexual relations and lack of protection for children against abuse on the Internet.

There is also a clear expectation (Article 9) that the private sector, including the information and communication technology sector (e.g. Internet service providers) should participate in the elaboration and implementation of policies to prevent sexual exploitation and sexual abuse of children and to implement internal norms through self-regulation or co-regulation, for example taking responsibility for controlling the material they host, and securing the best monitoring system for activities on the Internet and logging procedures.

7.2.3. The European Union

The EU published a Green Paper on the protection of minors and human dignity (COM (96) 483 final) in 1996. This opened a debate on the protection of minors and human dignity in

audio-visual and information services, including Internet services. An extensive consultation process led to the adoption of the *Recommendation on the development of the competitiveness of the European audiovisual and information services industry by promoting national frameworks aimed at achieving a comparable and effective level of protection of minors and human dignity* by the Council. Amongst its other provisions on-line Internet service providers were asked to develop codes of good conduct so as to better apply and clarify current legislation.

The Recommendation offered guidelines for the development of national self-regulation regarding the protection of minors and human dignity. Self-regulation was to be based on three key elements:

§ the involvement of all the interested parties (Government, industry, service and access providers, user associations) in the production of codes of conduct;

§ the implementation of codes of conduct by the industry;

§ evaluation of measures taken.

The Recommendation was closely linked to the Decision No 276/1999/EC adopting a multiannual Community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks, which in turn referred back to the Commission Communication on Illegal and Harmful Content on the Internet. (COM (96) 487 final).

The EU has very largely avoided the wider debate about pornography online, not least because 'community standards' relating to the acceptability of pornographic material vary considerably across the Member States. Where the EU has played an active role, has been in seeking to bring consistency to Member States policies on combating the sexual exploitation of children and child pornography, and in encouraging wider participation in schemes to provide 'safety' on the Internet via methods such as:

- Hotlines to allow members of the public to report illegal content.
- R & D into performance and effectiveness of filtering software and services
- Technological measures allowing users to limit the amount of unwanted and harmful content (e.g. quality rating of websites, cross-media content rating, rating and filtering techniques)
- Self-regulatory measures including consultation and appropriate representation of the parties concerned; codes of conduct (e.g. handling notice and take down procedures,

cross-border codes of conduct); national bodies facilitating cooperation at Community level; and national evaluation of self regulation frameworks

- distribution of information about Internet safety to large numbers of users, notably by using multiplier organisations and electronic dissemination channels

These initiatives have been contained in series of Council Decisions, including the Decision adopting a multiannual Community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks (276/1999/EC), and the Decision establishing a multiannual Community Programme on promoting safer use of the Internet and new online technologies (854/2005/EC)

While various measures existed to enable the European Union to combat the sexual exploitation of children (e.g. the 1999 joint action plan and the extension of Europol's mandate in 1999) or the dissemination of messages with an illegal and harmful content on the Internet, by 2000, it was felt that it was necessary to introduce a specific instrument to combat child pornography on the Internet, with a view of the perceived scale of the problem. The *Council Decision to combat child pornography on the Internet* (2000/375/JHA) required Member States to take measures to:

- encourage Internet users to inform law enforcement authorities if they suspect that child pornography material is being distributed on the Internet;
- ensure that offences are investigated and punished by setting up specialised units within the law enforcement authorities, for example;
- ensure that the law enforcement authorities react rapidly when they receive information on alleged cases of the production, processing, distribution and possession of child pornography;
- ensure that Europol, within the limits of its mandate, was informed of suspected cases of child pornography
- regularly verify whether, in the light of technological developments, their criminal law procedures should be amended with a view to combating child pornography on the Internet.
- investigate all measures which could help to eliminate child pornography on the Internet and are to exchange information on best practice

- examine the possibility of placing Internet providers under an obligation to advise the competent authorities of child pornography material which is distributed through them, to withdraw such material from circulation, to retain such material in order to make it available to the authorities, and to set up their own control systems.
- encourage the production of filters and other technical means of preventing the distribution and facilitating the detection of such material

In order to facilitate cooperation between Member States, a list of 24-hour national contact points and specialised units was created, Europol was formally involved in collecting information about suspected cases of child pornography, and regular meetings were set up between the national specialised services.

These measures were reinforced in 2004 by the *Framework Decision on combating the sexual exploitation of children and child pornography* (2004/68/JHA). This requires Member States to take all necessary measures to ensure that the particular intentional conduct (including Instigation, aiding, abetting and attempt) is punishable:

- coercing a child into prostitution or profiting from or otherwise exploiting a child for such purposes;
- engaging in sexual activities with a child, where use is made of coercion, force or threats, money or other forms of remuneration or consideration are given as payment in exchange for the child engaging in sexual activities, or abuse is made of a recognised position of trust, authority or influence over the child.
- whether undertaken by means of a computer system, or not:
    - production of child pornography;
    - distribution, dissemination or transmission of child pornography;
    - supplying or making available child pornography;
    - acquisition and possession of child pornography.

Member States must make provision for criminal penalties which entail imprisonment for at least one to three years. For certain offences committed in aggravating circumstances, the penalty must entail imprisonment for at least five to ten years.

The Framework Decision provides a list of aggravating circumstances, which does not preclude the recognition of other circumstances under national law:

- the victim is a child below the age of sexual consent under national law;
- the offender has deliberately or by recklessness endangered the life of the child;
- the offences involve serious violence or caused serious harm to the child;
- the offence has been committed within the framework of a criminal organisation as defined in Joint Action 98/733/JHA making it a criminal offence to participate in a criminal organisation in the Member States of the European Union

Member States may take measures to ensure that individuals convicted of one of listed offences are prevented from exercising professional activities related to the supervision of children.

The Decision also requires Member States to ensure that legal persons can be held liable under criminal and civil law for commission of the listed offences as well as Instigation, aiding, abetting and attempt. This liability is complementary to that which is borne by natural persons. A legal person is deemed to be liable if an offence is committed for its benefit by another person who acts individually or as part of an organ of the legal person, or who has decision-making powers. Sanctions on legal persons must include criminal or non-criminal fines and other sanctions such as temporary or permanent disqualification from the practice of commercial activities, a judicial winding-up order or exclusion from entitlement to public benefits or aid.

To prevent a crime from going unpunished because of a conflict of jurisdiction, the Decision establishes criteria for determining jurisdiction. A State has jurisdiction if:

- the offence is committed within its territory (territoriality principle);
- the offender is a national of that Member State (active personality principle);
- the offence is committed for the benefit of a legal person established in the territory of that Member State.

A State that refuses to extradite its nationals must take the necessary measures to prosecute them for offences committed outside its territory.

A recent report by the Commission, *Report based on Article 12 of the Council Framework Decision of 22 December 2003 on combating the sexual exploitation of children and child pornography* (COM(2007) 716 final) notes that:

> … the requirements set out in the Council Framework Decision have been met by almost all of the Member States, either as a result of pre-existing domestic laws, or through the implementation of new and specific legislation. … Concerning child pornography, the requirement concerning incrimination of production of pornographic materials involving children is generally met, although it is not possible to provide a precise assessment of the range of exemption from criminal liability concerning child pornography involving children between the age of sexual consent and 18 years. … Member States generally now dispose of specific criminal law provisions incriminating the sexual exploitation of children and child pornography, and provide for effective, proportionate and dissuasive penalties … new issues have been raised, for example regarding fraudulent solicitation of children for illicit purposes through the Internet ("grooming"). ... In the light of the outcome of these discussions, the Commission may consider the need to update and further strengthen the present Framework Decision regarding ...in particular offences committed through electronic communication networks and information systems.

The Commission is currently studying a new set of measures to curb child pornography. Among these is the establishment of points of contact for all actors involved, such as financial institutions and Internet providers, to quickly block illegal websites and payments carried out through them. The financial sector set up a steering group in autumn 2007 to implement the preparatory measures. In 2008, they will submit a project for a Commission funding, in order to create this one-stop-shop.

The INHOPE Association of Internet Hotlines, co-ordinated from Ireland, was founded in 1999. INHOPE is one of the few international responses to illegal content and activity on the Internet and is partly funded by the EC Safer Internet Action Programme and Microsoft. INHOPE facilitates and co-ordinates the work of 18 national hotlines against illegal internet content. Hotlines monitor the internet and it is where the general public can report illegal internet content such as child pornography. The hotline confidentially then reviews each report, referring illegal material onto the relevant law enforcement agencies or Internet Service

Providers for further action. Whereas a single hotline can be successful on a national level to tackle the problem, it's influence is limited when content is hosted in a foreign country or the perpetrator is located abroad. The INHOPE network is a important means to co-ordinate the exchange of information and expertise between hotlines worldwide.

7.3. Application of Anti-Pornography Laws and other Regulatory Strategies to the Online Environment

As has been demonstrated thus far, the issue of controlling pornography dissemination online is a complex one. States may find it difficult to construct clear definitions of the types of pornographic context that they wish to criminalize, and may (as the United States has struggled to do for over as decade since the Communications Decency Act of 1996 (Krause 2008)) find it problematic to balance the protection of minors and other vulnerable constituencies with competing constitutional principles, such as freedom of speech and freedom of expression online.

Many countries are disinclined to tackle the issue of 'adult pornography' by attempting to criminalise its dissemination online. Even in the US, which has taken a relatively hard line in the past, there appears to be relatively little legislative or LEA interest in either creating further laws, or actively enforcing existing laws . Instead action has tended to centre upon preventing access to it, particularly by minors and other vulnerable constituencies. A number of technology-based content-blocking schemes are used across various countries, for purposes including denying access to pornography, including China (a firewall scheme that resets connections - the 'Great Firewall of China'), Saudi Arabia (a web proxy system with a generic list of banned sites from a filtering software provider, augmented by citizen reported URLs submitted via a web form), and Norway. (*Clayton 2005*)

Child pornography is a different matter. Although it is clear that there remain significant definitional differences (e.g. over whether to criminalize images where a real child is not used, such as pseudo photographs, or use of actors who only look like children) and varying policy rationales (e.g. prevention of direct harm to children in the making of child pornography; or prevention of indirect harm to children by on-line access to distressing material, or when child pornography is used to 'seduce or encourage children into participating in sexual activity')

between states, it is equally clear that there is significant national, regional and international consensus that child pornography should be illegal, and that its degree of availability online will require both public and private sector action and significant cross-border co-operation to tackle.

Some states have found it hard to rationalize treating a person below the age of 18 as a 'child' for the purposes of the protection of children from sexual exploitation and child pornography, when their legal age for sexual consent may be considerably lower (in the EU the age of consent varies in Member States' legislation from the age of 13 in Spain to 17 in Ireland). However, from the ILO *Convention on the Worst Forms of Child Labor*, to the UN *Convention on the Rights of the Child*, to the EU *Decision to combat child pornography on the Internet* of 2000, to the CoE *Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse* it appears that an international consensus is emerging that any child below 18 should be strongly protected from exploitation in child pornography, that there should only limited exceptions between the age of sexual consent and the age of 18, and that harmonization of the age of sexual consent is probably necessary.

7.4. The UK Approach

The UK has taken a relatively active approach to the issue of online 'pornography' despite, until recently, not using the word in legislation.

7.4.1. Obscenity Legislation

The UK *Obscene Publications Act 1959* (OPA) states that 'an article shall be deemed to be obscene if its effect . . . is, if taken as a whole, such as to *tend to deprave and corrupt* persons who are likely . . . to read, see or hear the matter contained or embodied in it.' The key issues for a jury to consider when assessing particular material are:

- *The possibility of the relevant material being seen as likely to deprave and corrupt*. Could an observer come to the conclusion that some of those who viewed the material might be depraved and corrupted by it?
- *The likely audience for the material*, as this will form part of the assessment of its tendency to deprave and corrupt. When deciding whether material is obscene, an important

determining factor is the consideration of whom its likely audience is going to be. This is because some potential audiences are regarded as being more susceptible to being depraved and corrupted than others. Children are seen as an audience that is especially vulnerable in this respect. Thus, material made available in a forum or media that is available to children will be always be subject to stricter regulation than material that is not.

If an article is obscene, it is an offence to publish it or to have it for publication for gain. The *Obscene Publications Act 1959*, as amended by the *Criminal Justice and Public Order Act 1994*, defines a publisher as one who in relation to obscene material:

- distributes, circulates, sells, lets on hire, gives or lends it, or who offers for sale or for letting on hire, or.
- in the case of an article containing or embodying matter to be looked at or a record, shows, plays or projects it, or, where the matter is data stored electronically, transmits that data

Thus, the transfer of obscene material either manually, by use of computer disks or other storage media, or electronically from one computer to another, via a network or the Internet (e.g. sent by e-mail, or posted to websites), will be caught by the legislation.

The UK *Obscene Publications Act 1964* makes it an offence to have an obscene article in ownership, possession or control with a view to publishing it for gain. As a result, obscene material placed on a webserver will be caught even when an individual simply makes the data available to be transferred or downloaded electronically by others, so that they can access the materials and copy them. In *R v Arnolds, R v Fellows* (1997) the Court held that while the legislation required some activity on the part of the 'publisher', this was provided by the fact that one of the appellants had taken 'whatever steps were necessary not merely to store the data on his computer but also to make it available worldwide to other computers via the Internet. He corresponded by e-mail with those who sought to have access to it and he imposed certain conditions before they were permitted to do so.' However, following the decision in *R v Perrin* (2002 - defendant published a preview webpage, available free of charge to anyone with access to the internet featuring pictures of people covered in faeces, coprophilia or coprophagia, and men involved in fellatio), the prosecution will need to show that more than a negligible number of persons likely to be depraved and corrupted would be likely to see the material.

Some UK publishers of obscene material have sought to avoid the reach of UK obscenity law by uploading their material on webservers in other countries. In *R v Waddon* (2000) the defendant prepared the obscene material in England, and uploaded it from England to a website in the US, from which it was then downloaded by a police officer in London. Waddon argued that the material was not published in the UK for the purposes of the OPA 1959, and was thus outside the court's jurisdiction. However, the court held that Waddon was involved both in the transmission of material to the website and its transmission back again to this country, when the police officer gained access to the website – and there was, for the purposes of the OPA 1959, publication on the website abroad, when images were uploaded there; and then further publication when those images were downloaded elsewhere.

In short, a UK-based publisher of internet pornographic material featuring adults can be prosecuted for obscenity, if a jury finds the material likely to deprave and corrupt a particular audience. An open access webpage is effectively open to the world, including children, and thus its tendency to deprave and corrupt those likely to have access to it will be high. Publishing the material on a website outside the UK will not bar a prosecution for obscenity, if the material is accessible in the UK. Material open to prosecution need not be image based. Charges have been brought against the author of a blog post detailing the imaginary kidnap, torture and murder of the members of the pop group 'Girls Aloud' (*R v Walker* 2008).

7.4.2. Indecency Legislation

With regard to child pornography, the relevant parts of the amended *Protection of Children Act* 1978 (PCA) deal with photographic representations of children under 18 (or persons who appear to be under 18). The Act makes it an offence to take, make, permit to be taken, distribute, show, and possess intending to distribute or show, or publish indecent photographs or pseudo-photographs of children. The Act defines 'distribution' very broadly. It is not necessary for actual possession of the material to pass from one person to another, the material merely has to be exposed or offered for acquisition. The PCA also criminalises advertisements which suggest that the advertiser distributes or shows indecent photographs of children, or intends to do so.

The *Criminal Justice and Public Order Act 1994* (CJPOA) amended the PCA adding that 'photograph' shall include:

> data stored on a computer disc or by other electronic means which is capable of conversion into a photograph.

This definition of photograph covers digital representations of physical photographs (thus gif and jpeg image files, downloaded from FTP sites, embedded in webpages, or compiled from Usenet messages, will be treated as photographs).

The CJPOA additionally added the concept of the "pseudo photograph"

> "Pseudo-photograph" means an image, whether made by computer-graphics or otherwise howsoever, which appears to be a photograph."

Thus a pseudo-photograph means any image which is capable of being resolved into an image which appears to be a photograph and, if the image appears to show a child, then the image is to be treated as if that of a child. This means that there is no need for a child to have been used in the creation of the image, indeed the Act covers an indecent image which may not be based on any living subject. The pseudo–photograph amendments deal with situations where, for instance, morphing software is used to create images which look as if they are of children from images of adults.

The *Criminal Justice and Immigration Act 2008* (CJIA) further amends the definition of "photograph".

> References to a photograph also include:
>
> (a) a tracing or other image, whether made by electronic or other means (of whatever nature):
>
> (i) which is not itself a photograph or a pseudo photograph, but
>
> (ii) which is derived from the whole or part of a photograph or pseudo photograph (or a combination of either or both); and
>
> (b) data stored on a computer disc or by other electronic means which is capable of conversion into an image within para.(a)

The term 'indecency' is not defined in either the PCA, or any other statute in which it occurs. In essence, the test would seem to be whether the item in question offends current standards of propriety, or to put it in the American phraseology, whether it offends contemporary community standards. Given that community standards of adult behaviour tend to be rather higher where children are involved, an image involving a naked adult which might be perfectly acceptable, could well be treated as indecent if a child or pseudo-child image were to be portrayed in a similar manner.

The provisions discussed above have clear relevance to activities on the Internet. Placing of indecent pictures of children on a webserver will almost inevitably mean that they will be distributed; when such pictures are held on a computer they can be plausibly said to be in someone's possession; a link to a web site may be considered an advertisement; and an e-mail offering such pictures in digital or paper form certainly would.

A person charged under the PCA with distributing, showing, or possessing intending to show or distribute, has two potential defences:

- they did not see the image and that they had no knowledge or suspicion that the image was indecent;
- there was a legitimate reason for possessing or distributing the image e.g. for academic research or in the process of gathering evidence.

It is also an offence to possess an indecent image of a child or indecent child-like image. The defences available include:

- they had a legitimate reason for having the photograph or pseudo-photograph in their possession;
- they had not seen the photograph or pseudo-photograph and did not know, nor had any cause to suspect, it to be indecent;
- the photograph or pseudo-photograph was sent to them without any prior request made by them or on their behalf and they did not keep it for an unreasonable time

With regard to the computerised making or possession of indecent photographs of children, the UK courts held in *R v. Bowden* (2000) that the intentional downloading and/or printing out of computer data of indecent images of children from the Internet constituted the 'making' of an indecent photograph and was thus an offence under s1(1)(a) of the Protection of Children Act 1978. With regard to the unintentional storage of computer data of indecent images of children in a computer cache the court in *Atkins v DPP* (2000) held that this did not automatically constitute 'making', nor did their possession in a computer cache necessarily mean an offence had been committed under s160 Criminal Justice Act 1988, as the defendant, in such circumstances, must be shown to have known he had the photographs in his possession, or to know he once had them.

In *R v Smith and Jayson* (2002) Smith had received an indecent photograph as an email attachment, and Jayson had browsed an indecent pseudo-photograph on the Internet. In both cases, their browser software automatically saved the images to a temporary Internet cache on their computers. With regard to Smith, the court held that no offence of "making" or "being in possession" of an indecent pseudo-photograph was committed simply by opening an email attachment where the recipient was unaware that it contained or was likely to contain an indecent image. However, when Smith's opening of the e-mail attachment was considered in the light of the evidence relating to his other activities, the court did not believe him to be unaware of the nature of the attachment. Jayson argued that his act of viewing the indecent pseudo-photograph did not constitute the necessary intent to 'make' a photograph or pseudo-photograph. The court, however, held that the act of voluntarily downloading an indecent image from the Internet to a computer screen was an act of making a photograph or pseudo-photograph, as the intent required was 'a deliberate and intentional act with the knowledge that the image was or was likely to be an indecent photograph or pseudo-photograph of a child.'

In summary, a UK-based maker, owner, or publisher, of internet pornographic material featuring children can be prosecuted for indecency, if the jury finds the materials in question contain images of children under 18 (or persons who appear to be under 18) which offend current standards of propriety, and those materials are either photographs, or they appear to be photographs. Downloading and/or storing an indecent image constitutes a making an image offence. Mere possession is also an offence (except for narrow defences).

7.4.3. Extreme Pornography Legislation

Under the UK *Criminal Justice and Immigration Act 2008* (CJIA) it is an offence for a person to be in possession of an 'extreme pornographic image'. As noted above an 'extreme pornographic image' is an image that:

- is of such a nature that it must reasonably be assumed to have been produced solely or principally for the purpose of sexual arousal; and is NOT part of a sequence of images which in context are not pornographic;
- AND portrays, in an explicit and realistic way, any of the following;
    - an act which threatens a person's life,
    - an act which results, or is likely to result, in serious injury to a person's anus, breasts or genitals (references to a part of the body include references to a part surgically constructed e.g. through gender reassignment surgery),
    - an act which involves sexual interference with a human corpse, or
    - a person performing an act of intercourse or oral sex with an animal (whether dead or alive)
    - AND a reasonable person looking at the image would think that any such person or animal was real
- AND is grossly offensive, disgusting or otherwise of an obscene character.

A person charged under the CJIA for possession of an extreme pornographic image has three potential defences:

- they had a legitimate reason for being in possession of the image concerned;
- they had not seen the image concerned and did not know, nor had any cause to suspect, it to be an extreme pornographic image;
- they were sent the image concerned without any prior request having been made by or on behalf of them, and did not keep it for an unreasonable time.

There is an additional defence for a person charged under the CJIA for possession of an extreme pornographic image where the offence relates to an image that portrays an act which

threatens a person's life; an act which results, or is likely to result, in serious injury to a person's anus, breasts or genitals; or an act which involves sexual interference with a human corpse and the defendant can prove

- that they directly participated in the act or any of the acts portrayed, AND that the act or acts did not involve the infliction of any non-consensual harm on any person, AND if the image portrays an act which involves sexual interference with a human corpse, that what is portrayed as a human corpse was not in fact a corpse.

To date there do not appear to have been any prosecutions under the Act.

7.4.4. Grooming Legislation

'Grooming' is commonly defined as a process by which a person befriends a child to gain their trust and to create a situation whereby the child will allow the perpetrator to have sexual contact with them and will not tell anyone of it. It is a significant concern online. Research in the USA suggests that between 5 - 20% of children were solicited via the Internet. In the UK, the *Sexual Offences Act 2003* makes it an offence to meet with a child with the intent to have sexual contact with them, where the person (>18 years) has

- either met or communicated with the child (<16 years) on two previous occasions AND
- either meets the child OR travels with the intention of meeting the child (in any part of the world) AND
- at that time, has the intention of committing a relevant sexual offence .

The legislation criminalises the meeting following sexual grooming, not the sexual grooming behaviour itself. It enables police to conduct proactive policing via the Internet - police officers pose as vulnerable children in Internet chat rooms, and wait for offenders to prey on them. Offenders who arrange to meet these undercover police officers can then be arrested subject to the availability of evidence that proves their sexual intent. Pornography is often used in the grooming process.

7.4.5. Other Measures

The Internet Watch Foundation (IWF) is a UK independent self-regulatory body, funded by the EU and the wider online industry, including internet service providers, mobile operators and manufacturers, content service providers, filtering companies, search providers, trade associations and the financial sector (e.g. the Association for Payment Clearing Services). It provides a channel for the UK public and IT professionals to report potentially illegal online content via an online Hotline. Potentially illegal online content includes child sexual abuse content hosted anywhere in the world, and criminally obscene and incitement to racial hatred content hosted in the UK. The IWF also:

- helps ISPs and hosting companies to combat abuse of their networks through a national 'notice and take-down' service which alerts them to potentially illegal content on their systems;
- provides unique data to LEAs in the UK and abroad to assist investigations into the distributers of potentially illegal online content
- facilitates the industry-led initiative to protect users from inadvertent exposure to potentially illegal content hosted abroad by blocking access to it through provision of a dynamic list of child sexual abuse URLs.

According to the IWF, as a result of its activities, less than 1% of child sexual abuse content (the IWF prefers this term to 'child pornography'), known to the IWF, has apparently been hosted in the UK since 2003, down from 18% in 1997. Users of the IWF dynamic list of child sexual abuse URLs include British Telecom's (BT) Cleanfeed, a content blocking system, and WebMInder, used by a range of ISPs. The IWF is a member of INHOPE.

A new UK Council for Child Internet Safety (UKCCIS) was set up in September 2008 to unite over 100 organisations from the public and private sector working with government to deliver recommendations from the Byron Report *Safer Children in a Digital World*. The role of the council is to improve the regulation and education around internet use, tackling problems around online bullying, safer search features, and violent video games. It will report directly to the Prime Minister.

It is involved in the development of a UK Child Internet Safety Strategy, to be delivered in 2009, which will

- establish a comprehensive public information and awareness and child internet safety campaign across Government and industry including a 'one-stop shop' on child internet safety
- provide specific measures to support vulnerable children and young people, such as taking down illegal internet sites that promote harmful behaviour
- promote responsible advertising to children online
- establish voluntary codes of practice for user-generated content sites, making such sites commit to take down inappropriate content within a given time.

7.5. Best Practice

As can be seen from the foregoing discussion, there are a number of often complementary approaches to addressing the issue of controlling, and where necessary criminalizing, various forms of on-line pornography. Best practice in this area for most states is likely to consist of ensuring that suitable legal provision is made to meet international obligations, whilst taking note of such national factors as may affect the effective and efficient development of policy and regulation. Thus, states may, in the short or long term, need to derogate from, or reserve the right not to apply, as permitted, certain aspects of international agreements, until existing national rules and practices (e.g. the age of consent) can be harmonized.

When developing national legal approaches to controlling, and where necessary criminalizing, various forms of on-line pornography, it is important to consider carefully the types of environment in which the material is currently, and may in the future, be available and accessed, with regard to the impact that regulation may have on either the marketplace – heavy regulation may constitute a barrier to entry for new businesses and technologies; or upon other legal principles such as freedom of speech and freedom of expression - social norms change over time, and it can be difficult to ensure that rigid regulatory regimes can move with the times. In the UK, the obscenity/indecency approach has proved flexible as social norms surrounding adult pornography have changed – what might have been considered obscene in the 1950s may now be considered mainstream culture or artistic expression; however, that flexibility has come partly at the expense of certainty – there may be some chilling of speech/expression simply because there is no 'bright line' rule as to what is obscene/indecent. These are issues that national legislatures and courts will have to consider.

Attempting to utilize only national legal approaches to on-line pornography is unlikely to prove satisfactory. As with other areas of cybercrime, such as fraud and money laundering, if enforcement and control are to be effective, there must be an ability to exchange information and as appropriate, evidence between competent authorities and LEAs at an international level, promptly, systematically and efficiently.

Mobilizing both public and private sectors in support of regulatory goals, including businesses, industry groups, and consumer groups, both in terms of education and consultation (i.e. taking advantage of private sector expertise), and in terms of seeking to engage private sector organizations in regulatory processes, such as involving sectoral groups in self-regulatory practices can often achieve significantly more that attempting a top down 'command and control' approach. In many cases, it is advantageous to private sector bodies such as ISPs and other information society service providers to be able to police their own environments, as uncontrolled pornography may be an obstacle to prompting their services as, for example, family friendly, or child safe. The aim of governments can thus be to provide them with the necessary legislative and/or financial support to do so.

8. MONEY LAUNDERING ONLINE

8.1. Introduction

Money laundering" is not a legal term in international law although the act by which illicit funds are made to appear legitimate is defined in several key international instruments, e.g.

> *The conversion or transfer of property, knowing that such property is the proceeds of crime, for the purpose of concealing or disguising the illicit origin of the property or of helping any person who is involved in the commission of the predicate offence to evade the legal consequences of his or her action; or the concealment or disguise of the true nature, source, location, disposition, movement or ownership of or rights with respect to property, knowing that such property is the proceeds of crime.* (Article 6, UN Convention against Transnational Organized Crime, adopted November 2000, entered into force September 2003).

A money laundering 'predicate offence' is defined as the underlying criminal activity that generated proceeds, which when laundered, results in the offence of money laundering. Such offences could include drug dealing, racketeering, robbery or theft, corruption and bribery and fraud. The general trend at the international level in recent times has been to widen the number of predicate offences that can result in charges of money laundering being brought.

Money laundering offences are perceived as particularly serious because they:

- incentivise criminal behavior by making it profitable;
- provide domestic and transnational organised crime with a cash flow to perpetrate further crimes; and
- threaten the financial system and its institutions, both domestic and international.

Additionally, after the events of 9/11, there is increased interest in terrorism and its associated financing, as terrorists' access to, and use of, what may be in money laundering terms quite small sums of money, can have a disproportionate effect on the general public.

Money laundering has, like many other forms of online crime, a considerable off-line history – indeed it has been claimed (probably incorrectly) that the term itself originated from Mafia

ownership of self-service laundries or 'Laundromats' in the United States. Whatever the origins of the term, money laundering is generally deemed to have three main stages:

- Placement/Hiding. The illegally obtained money to be laundered is introduced to the economy, often via commercial concerns which may knowingly or unknowingly be part of the laundering scheme, and which provide the interface between the money launderer and the financial sector. A basic money laundering scheme might simply add cash payments to an existing revenue stream, i.e. placing cash from illegal gambling into the cash take of a self-service garage from which payments are made under some apparently legitimate pretext to the launderer; however, large and/or frequent sums of illegal finance laundered in this fashion may still attract attention.
- Layering/Moving. In order to avoid attention, in more sophisticated money laundering schemes, the money launderer will usually engage in complex networks of transactions, which may use transfers, sales and purchase of assets to break up the original sum of money, and to disguise the initial entry point of the funds into the economy.
- Investment/Integration. Once the money has been successfully laundered, i.e. has become associated with a legitimate revenue source, it can be reclaimed by the money launderer for investment in assets or lifestyle.

Example:

Mr. A, a money launderer, obtains money via a predicate offence – drug trafficking. He sets up multiple anonymous accounts in a large Virtual World which maintains its own internal currency, the VWdollar, at a set rate against the US$. He credits the accounts with VWdollars using a credit card or digital money payment. The VWdollar balances are stored online by the Virtual World owners and the virtual funds may be used within the virtual world to buy 'land', or to trade in virtual goods and services – Placement.

Mr. A, and other users acting on his behalf, use the accounts to engage in trading activities between themselves and other innocent users in the Virtual World, and this activity is co-ordinated by coded messages sent by Mr A. using the Instant Messaging system built into the Virtual World. Mr. A is willing to take up to a 15% loss of the value of the 'dirty' money entered into the system in order to produce 'clean' money - Layering

Balances or profits made by members of the Virtual World in VW dollars can be transferred back into the real world, as US$ via PayPal or other digital money payment, or

by striking deals with other players through external online auction sites, and then to various bank accounts owned by Mr. A - Integration

National legal strategies may be aimed at all 3 of these stages, usually by means of placing legal obligations upon banks or other financial service providers (e.g. money transfer agencies, e-money institutions); businesses (e.g. law firms, estate agencies); and even individuals, to report suspicious financial activities.

From its early days as a recognized crime, money laundering has had a significant international component, not least because (as with online fraud) cross-border money laundering complicates the jurisdictional issues and involves multiple national law enforcement agencies (LEAs). The arrival of Internet technologies, and particularly e-commerce/e-banking services, has added further difficulties due to factors such as:

> "…non face-to-face registration, possible anonymity of the users, speed of transactions, limited human intervention, high number of transactions, international presence, limited jurisdictional competences, difficulties for traditional financial institutions to monitor and detect suspicious financial transactions … when an Internet payment service provider is used…" (FATF 2008)

These difficulties may be made worse where national legal systems have concentrated their reporting obligations on off-line financial services and businesses, or have yet to place such obligations on new types of organization engaged in on-line/digital 'value transfers' e.g. 'virtual precious metals' exchanges.

It is worth noting that significant international financial transfers have long taken take place through informal money transfer systems (IMTS, also known as alternative or parallel remittance systems) e.g. *hawala* or *hundi* (South Asia); *fei ch'ien*, *chiti*, *chop shop* or *flying money* (China). These traditional systems usually operate within a close-knit community, often using lines of communication built up all over the world over a period of decades. ITMS attract customers because of their simplicity, efficiency, reliability and low cost, relative to other available options. They are often unregulated, or operate illegally where such activities are notionally regulated, and have been significantly facilitated by online communications. (Jost &

Sandhu 2000) While *hawala* and *fei ch'ien* are long established, more recently similar ITMS appear to have developed as a mechanism for expatriate workers from Africa and Eastern Europe to export value to their home countries from countries such as the UK, thus avoiding bank transaction charges, foreign exchange commission, currency controls and taxes. While many of these transfers may be innocent, merely reflecting a desire for a cheap and simple method of transferring value to overseas dependants, it is clear that ITMS can offer a highly effective, and difficult to regulate, mechanism for international money laundering.

A modern version of these ITMS is the digital money/currency provider. An example of such a provider is the WebMoney service <http://www.wmtransfer.com/>, headquartered in Russia, which allows account holders in a number of countries to transfer funds globally without using the formal banking sector. While digital money services have proven popular, as they provide a rapid, cost-effective and potentially anonymous service for their customers, increasing evidence that their services have been used international money laundering, means that they have come under increasing pressure to bring their services into line with international anti-money laundering practices. (*NDIC 2008*)

Table 1: – Examples of Online Money Laundering

Type	Nature of money laundering	Goal	Example
Masking the origin of funds.	The money launderer uses 3rd parties to purchase luxury goods with cash from offline shops. The 3rd parties then offer the goods for sale at a loss on commercial websites. Payment for the online sales is made to bank accounts connected to the money launderer.	The money launderer is seeking to bring money (often obtained from illegal activities, e.g. prostitution, gambling, drug dealing) into the financial system from apparently innocent activities.	Mr. A. has $5000 obtained from drug dealing. He pays Mrs. B, Mrs. C and Mrs. D to go to boutique shops and buy jewelry and designer goods for cash. The goods are offered for sale on an auction website, using different identities, with payment collected via an IPSP, also using different identities. Payment for the online sales is made to Mr. A's overseas bank accounts.
Masking evidence of dealing in stolen or fake goods	The money launderer sells stolen or counterfeit goods on an auction website under a variety of identities. Money from those sales is used to purchase 'clean' goods or services online, which can in turn be sold.	The money launderer is seeking to distance both his identity and the source of the money from connection with the stolen or counterfeit goods.	Mr. A sells counterfeit software on an auction website, using different identities, with payment collected via an IPSP, also using different identities. Mr. A. then uses the money stored at the IPSP to purchase legitimate goods/services via the auction house, which can be sold online or offline.
Masking evidence of trade in illegal goods/services.	The money launderer seeks to use an Internet payment service provider (IPSP) to collect the proceeds of an illegal activity undertaken in one jurisdiction, and transfer it to another jurisdiction.	The money launderer is seeking to obscure the identity of the recipient of the money, and to complicate any investigation by national agencies by adding a cross-border element. Further difficulties may be caused where the activity generating the money is illegal in one jurisdiction, but not in the other.	Mr. A, a citizen of Country X, sells materials or services which are illegal in Country X (e.g. drugs, weapons, prostitution) to customers, both national and international, via a website. Payment for the materials or services is collected via an IPSP, and credited to a bank account held by A in Country Y.
Masking evidence of fraudulent transactions	The money launderer places advertisements for non-existent goods on commercial websites. Buyers are instructed to send	The money launderer is seeking to obscure the identity of the recipient of the money, and to complicate any investigation by	Mr. A, a citizen of Country X, offers to sell expensive jewelry via a commercial website. Buyers from other countries are told to send money orders to a Miss B,

	payment by money order to a fictitious individual in another jurisdiction. The payment is intercepted by a 3rd party, who forwards it using a fake identity, either to the money launderer, or the next in a chain of 3rd parties working for the money launderer.	national agencies by adding a cross-border element. Further difficulties may be caused where the activity generating the money is illegal in one jurisdiction, but not in the other.	in country Y. Money sent to Miss B is in fact picked up by Mr. C. Mr. C (who receives 10% of the money order) is instructed by text message (either by Mr. A, or by another 'money flow manager' working for Mr. A.) to send the money to Mr. D (who may in fact be Mr. A, or yet another 3rd party working for Mr. A)
Masking the purpose of payment	The money launderer offers non-existent goods for sale on a commercial website and accepts 'purchases' only from specific 3rd parties.	The money launderer is seeking to transfer money to a 3rd party or 3rd parties without arousing suspicions about the reason for the transfer.	Mr. A seeks to transfer $5000 payment for a criminal activity to Mr. B. Mr. B places an advertisement selling a car valued at $5000 on a commercial website. Mr. A purports to purchase the car, and sends $5000 to Mr. B's overseas bank account. No car is delivered. Mr. A. will not flag the transaction as fraudulent, and the digital trail for the 'sale' via the commercial website provides Mr. B with a justification for the money transfer.
	The money launderer offers real goods for sale, but for an inflated/ markedly low price. Inflating prices can easily be done on auction websites where a fair market price for items can be hard to gauge, and where bidder interaction (including 'shill bidding') may drive prices beyond usual expectations	This has a similar effect of transferring money from the money launderer to a 3rd party or 3rd parties, but has the added advantage of a genuine delivery trail. Law enforcement agencies must then demonstrate that the price paid is significantly out of proportion to the market value of the goods.	Mr. A offers a china figurine, purchased for $500, for sale on an auction website. International interest in such pieces is high and collectors often pay significantly more than market price for such items. Mr. B. bids $2500 for the figurine. Mr. A, either via collector interest, or through fake bids made through additional accounts he has created, raises the cost of the figurine to a price, prearranged with Mr. B, of $2000.
Tax and VAT avoidance	A company purchases goods, which the company claims will be exported, and but it	The company aims to present its business activities as lawful operations, and thereby	Company B, in Country X, purchases duty free goods to sell outside the domestic market. The

	then sells them within the domestic market, avoiding VAT, excise duty payments or other national taxes. Internet sales, via credit card or IPSP payments, are used to create the impression that the company is running a legitimate export business to international customers.	defraud national tax authorities, and to complicate any investigation by national agencies by adding a cross-border element.	company purports to export the goods to legitimate international customers via a website through which it receives credit card payments. However, the 'customer' orders and payments are in fact made by officers of Company B using foreign credit cards and bank accounts. These are supplied with funds by wire transfer from Country X, or other countries, under assumed names and through front companies. No goods are exported.
Unlicensed/ unlawful money transfers The modern equivalent of parallel banking systems such as *hawala.*	The money launderer purchases 'digital value' in the form of 'digital currency' or 'virtual precious metals'. Once the money launderer has acquired 'digital currency' or 'digital precious metals' some or all of their holding can be transferred online to a 3rd party for goods and services. In many jurisdictions, dealings in 'virtual precious metals', which are essentially options to purchase an amount of precious metals at a specific price (derivatives) fall outside the scope of existing national restrictions on/regulation of money transmission. Additionally the dealer of the 'virtual precious metals' and/or the exchanges often used to facilitate transfers are often outside the jurisdiction in which the money launderer is located	The money launderer is seeking to be able to transfer a sum of fixed 'value' via a digital money service, or virtual precious metal exchange, essentially unsupervised and unauthorized by national anti-money laundering and law enforcement agencies.	Mr. A, in Country X opens a account with Platinum E-change Ltd, a 'virtual precious metals' dealer, which maintains user accounts containing virtual holdings of precious metals. Mr A uses Platinum E-change Ltd to transfer funds to a 'virtual precious metals' exchange service, which acts as a broker for the virtual precious metals that the dealers buy or sell for their account holders. Mr. A then transfers his ownership of $1.5 million in 'virtual precious metals' held at Platinum E-change Ltd, via the 'virtual precious metals' exchange service, to Mr. B in Country Y, who sells the options and uses the funds to purchase property for Mr. A in Country Y. Despite its size, the transfer is not reported to the relevant money laundering prevention authorities in either Country X or Country Y as neither Platinum E-change Ltd nor the 'virtual precious metals'

			exchange service fall under their respective national restrictions on/regulation of money transmission, and both companies are based in Country Z, which has limited banking regulation.

This table is derived from the following reports of the Financial Action Task Force (FATF/GAFI) an inter-governmental body whose purpose is the development and promotion of national and international policies to combat money laundering and terrorist financing.

FATF (2006) *Report on New Payment Methods*, 13 October 2006.
<http://www.fatf-gafi.org/dataoecd/30/47/37627240.pdf>

FATF (2008) *Money Laundering & Terrorist Financing Vulnerabilities of Commercial Websites & Internet Payment Systems*, 18 June 2008.
<http://www.fatf-gafi.org/dataoecd/57/21/40997818.pdf>

8.2. International Responses

Although money laundering has a long history, concerted international efforts to combat it have developed relatively recently, with international agreements such as the United Nations *Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances* (1988) (Vienna Convention) and the United Nations *Convention Against Transnational Organized Crime* (2000) (Palermo Convention) both seeking to encourage signatories to incorporate anti-money laundering (AML) provisions as part of their efforts to defeat crimes such as drug and people trafficking. Other international organizations, including the Bank of International Settlements (BIS), the Council of Europe, Interpol, the Organisation of Economic Cooperation and Development (OECD) and the Wolfsberg Group of international banks, have also been involved in developing measures including good practice guidance, expert committees, national AML evaluations, and fostering international co-operation.

Currently the key element of the international approach to money laundering is the Financial Action Task Force (FATF), which was founded in 1989 by the G7 states. The main tasks of FATF are to examine money laundering techniques and trends and set out recommendations for AML measures. The FATF currently comprises thirty-four members: 32 member jurisdictions and two regional organisations (the European Commission and the Gulf Co-operation Council), representing most major financial centres worldwide. The FATF also works through 8 FATF-style regional bodies (FSRBs), which bring together, on a regional basis, other jurisdictions that have committed to implementing the 40+9 Recommendations and have agreed to undergo mutual evaluations of their AML/CFT systems. Five of these FSRBs are associate members of the FATF:

- the Asia/Pacific Group on Money Laundering (APG),
- the Caribbean Financial Action Task Force (CFATF),
- the Council of Europe Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL),
- the Grupo de Acción Financiera de Sudamérica (GAFISUD), and
- the Middle East and North Africa Financial Action Task Force (MENAFATF).

The 3 remaining FSRBs are working towards associate membership status:

- Eurasian Group on combating money laundering and financing of terrorism (EAG),
- Eastern and South African Anti Money Laundering Group (ESAAMLG), and
- Groupe Inter-gouvernemental d'Action Contre le Blanchiment en Afrique (GIABA).

In 1990 FATF issued its 'Forty Recommendations', (see below) which were designed to provide a complete set of counter-measures against money laundering. The recommendations covered:

- National criminal justice systems and law enforcement, with the aim of ensuring that appropriate measures were in place to criminalise money laundering
- National financial systems and their regulation, with the aim of requiring financial institutions and other organizations (e.g. banks and accountancy firms) to take appropriate measures (e.g. customer due diligence and reporting requirements)
- International co-operation, with the aim of creating effective domestic regulatory bodies and a commitment to international cooperation.

These recommendations essentially form the basis for all domestic and regional anti-money laundering (AML) regimes. They set out the principles for action and allow countries a measure of flexibility in implementing these principles according to their particular circumstances and constitutional frameworks. Between 2001 and 2004 the FATF also issued nine Special Recommendations which, when combined with the Forty Recommendations on money laundering, set out the basic framework to detect, prevent and suppress the financing of terrorism and terrorist acts. (See below)

As well as its "40 + 9" Recommendations FATF has issued a list of "Non-Cooperative Countries or Territories" (NCCTs), usually called the "FATF Blacklist". Initially, in 2000, this was a list of 15 counties that were regarded by FATF members as uncooperative in international efforts against money laundering. Such lack of co-operation usually takes the form of failure to provide foreign law enforcement officials with information such as bank account and brokerage records, as well as

information about shell companies, and other financial vehicles frequently used in money laundering. The Blacklist is compiled by FATF staff on the basis of a 25 point check-list. If a country is found not to conform in more than one point it is automatically labeled "non-cooperative", or "partially non-cooperative" depending on the number of shortcomings.

The FATF blacklisting process has had significant effect in achieving co-operation from NCCTs, because although being placed on the FATF Blacklist carries no formal sanctions, transactions coming from or transferring to a country on the FATF Blacklist are more likely to be considered a suspicious activity, which in most FATF member states will automatically trigger closer regulatory scrutiny (and considerably more paperwork). The result of this is that many financial institutions will not conduct business with counterparts based in NCCTs. A further 8 countries were added to the Blacklist in 2001, but since then, increased attempts at compliance have meant no further listings and a decline in the use of the Blacklist. At the time of writing, it appears that no countries are currently listed on the Blacklist, with the removal of Myanmar in 2006.

The mutual evaluation process is a key part of both FATF and its FSRBs' work. Through this process FATF monitors the implementation of the *40+9 Recommendations* in its member jurisdictions, and assesses the overall effectiveness of AML/CFT systems. Each FATF member jurisdiction is examined in turn by FATF, or in some cases by the IMF, with the final report adopted by FATF. The aim of these evaluations is to assess whether the necessary laws, regulations or other measures required under the new standards are in force and effect, that there has been a full and proper implementation of all necessary measures, and that the system in place is effective. FATF mutual evaluation reports are shared with all members and observers, are discussed in open session in the FATF plenary, and are made available on the FATF website once adopted. The *AML/CFT Handbook for Countries and Assessors 2007* provides instructions and guidance for all countries and bodies that are undertaking assessments.

8.2.1. The Council of Europe

The Council of Europe adopted the *Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime (Strasbourg Convention)* (ETS 141) in 1990. The Convention aims to facilitate

international co-operation and mutual assistance in investigating crime and tracking down, seizing and confiscating the proceeds of crime, by providing a degree of efficiency and co-operation between Council of Europe member states even in the absence of full legislative harmony. It has been ratified by all 48 Council of Europe member states, and is also open to non- member states, of which one, Australia, has ratified.

The convention was updated and widened in 2005 with the adoption of the *Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism* (CETS 198). This covers both the prevention and the control of money laundering and the financing of terrorism, and includes a mechanism to ensure the proper implementation by parties of its provisions.

MONEYVAL was established in 1997. It reviews the anti-money laundering measures and measures to counter the financing of terrorism in Council of Europe member States (and Council of Europe applicants which apply to join the terms of reference) which are not members of the Financial Action Task Force (FATF). Council of Europe member states which are members of MONEYVAL but subsequently become members of the FATF can retain full membership of MONEYVAL (e.g. Russian Federation). It assesses its members' compliance with all relevant international standards in the legal, financial and law enforcement sectors through a peer review process of mutual evaluations. Its reports provide detailed recommendations on ways to improve the effectiveness of domestic regimes to combat money laundering and terrorist financing and states' capacities to co-operate internationally in these areas.

Current members include, Albania, Georgia, Romania, Andorra, Hungary, Russian Federation (also FATF member), Armenia, Latvia, San Marino, Azerbaijan, Liechtenstein, Serbia, Bosnia and Herzegovina, Lithuania, Slovak Republic, Bulgaria, Moldova, Slovenia, Croatia, Malta, "The former Yugoslav Republic of Macedonia", Cyprus, Monaco, Ukraine, Czech Republic, Montenegro, Estonia, and Poland. Israel was granted active observer status with MONEYVAL in January 2006,

which enables it to take part in the evaluation process. The current chairman is Mr Vasil Kirov of Bulgaria. Bulgaria's latest evaluation, in the Third Evaluation Round, was carried out in April 2007 and the Report was submitted in April 2008, Romania's latest evaluation, in the Third Evaluation Round, was carried out in May 2007 and the Report was submitted in July 2008. (see below)

8.2.2. The European Union

There have also been three EU directives on money laundering, the last of which was issued in October 2005. The EU has tended to adopt the FATF 40 recommendations, thus the latest EU Directive states that 'Community action should continue to take particular account of the Recommendations of the Financial Action Task Force' and that the EU guidelines should be in line with these standards.

The initial EU *Council Directive on prevention of the use of the financial system for the purpose of money laundering* (91/308/EEC) provided a basis for Member States' efforts to prevent criminal money entering the financial system. It defined the concepts of credit institution, financial institution and money laundering, and required Member States to ensure that money laundering was prohibited, and that credit and financial institutions (including '*bureaux de change*') required identification of their customers by means of supporting evidence, unless the customer was also a credit or financial institution. The identification requirement applied when a single transaction or linked transactions exceeded ECU 15,000 or when credit and financial institutions suspected laundering (even where the transaction was below the threshold).

Credit and financial institutions were also required to:

- keep a copy or the references of the evidence required, for at least five years after the relationship with their customer ended, as well as supporting evidence and records of transactions for at least five years following execution of transactions.
- not disclose to anyone that information had been transmitted to the authorities or that an investigation was being carried out. Credit or financial institutions were given immunity from liability where their disclosure to the authorities was in good.

- inform the authorities responsible for combating money laundering if they discovered facts that could constitute evidence of money laundering.
- establish procedures of internal control and communication in order to forestall and prevent operations related to money laundering and take appropriate measures so that their employees were aware of the provisions contained in the directive.

The second EU *Directive of the European Parliament and of the Council amending Council Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering* (2001/97/EC) extended the number of crimes to which the provisions applied and widened the range of professions who had to observe it to include lawyers, auditors, accountants, notaries, casinos and estate agents. It also provided for the establishment of financial intelligence units in each member state to which suspicious transactions reports (SRTs) were to be made.

The third EU *Directive of the European Parliament and of the Council on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing* (2005/60/EC) effectively repealed the first and second Directives.

It describes money laundering as the following conduct, when committed intentionally:

- the conversion or transfer of property derived from criminal activity or from an act of participation in such activity, for the purpose of concealing or disguising the illicit origin of the property;
- assisting any person who is involved in the commission of such activity to evade the legal consequences of his action;
- the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of property;
- the acquisition, possession or use of property, knowing, at the time of receipt, that such property was derived from criminal activity.

Intent requires knowledge that the property is derived from criminal activity. Knowledge, intent or purpose may be inferred from objective factual circumstances. The Directive also covers participation in, association to commit, attempts to commit and aiding, abetting, counselling and facilitating the commission of any of the above-mentioned acts. Money laundering must be regarded as such even where the criminal activities which generated the property to be laundered were carried out in the territory of another Member State or of a Non-EU Member Country.

By "terrorist financing" the Directive means the provision or collection of funds by any means, directly or indirectly, with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out terrorist offences, including, hostage taking, the drawing-up of false administrative documents, the leadership of a terrorist group, etc.

The Directive (Art.2) applies to:

- credit institutions;
- financial institutions;
- legal or natural persons acting in the exercise of their professional activities, including auditors, external accountants and tax advisors; notaries and other independent legal professionals acting for, or helping plan and execute transactions for, clients, e.g.
    - buying and selling real property or business entities;
    - managing client money, securities or other assets;
    - opening or management of bank, savings or securities accounts;
    - organisation of contributions necessary for the creation, operation or management of companies;
    - creation, operation or management of trusts, companies or similar structures;
- trust or company service providers not already covered under the first two heads
- real estate agents;

- natural or legal persons trading in goods, where payments are made in cash in an amount of EUR 15000 or more, whether the transaction is executed in a single operation or in several operations which appear to be linked;
- casinos.

Art 2. entities are required to apply customer due diligence measures

- when establishing a business relationship;
- when carrying out occasional transactions amounting to EUR 15 000 or more;
- when there is a suspicion of money laundering or terrorist financing, regardless of any exemption or threshold;
- when there are doubts about the veracity or adequacy of previously obtained customer identification data.

These due diligence measures involve

- identifying the customer and verifying his identity,
- obtaining information on the purpose and intended nature of the business relationship and,
- where appropriate, identifying and verifying the identity of the recipient, etc.

The degree of due diligence required is determined by the entity involved on a risk-sensitive basis depending on the type of customer, business relationship, etc. and they may call on third parties to meet these requirements. In certain circumstances the Directive permits lesser or simplified customer due diligence.

Where there is a high risk of money laundering or terrorist financing, the Art. 2 entities are required to apply enhanced due diligence. Enhanced due diligence involves supplementary measures to verify or certify the documents supplied, for example:

- if the customer has not been physically present for identification purposes,
- in respect of cross-frontier relationships with respondent institutions from Non-EU Member States,
- to permit the assessment of a third-party institution's anti-money laundering and anti-terrorist financing controls, etc.

In addition to the above, there is a stipulation that credit and other financial institutions may not keep anonymous accounts or anonymous passbooks.

Each Member State is required to establish, and provide adequate resources for, a national financial intelligence unit (FIU); which must have the necessary powers to access the financial, administrative and law enforcement information that it requires. A national FIU is responsible for receiving, requesting, analyzing, and disseminating to the competent authorities, disclosures of information which concern potential money laundering, or potential terrorist financing. Art.2 entities must inform their national FIU as quickly as possible when they know, suspect, or have reasonable grounds to suspect, that money laundering or terrorist financing is being, or has been committed, or attempted. At the FIU's request, they must furnish all necessary information required by legislation. Where money laundering or terrorist financing is suspected, Art.2 entities are required to refrain from carrying out transactions until they have informed the FIU of them. Member States have a discretion whether to require independent legal professions, notaries, auditors, external accountants and tax advisers to inform the national FIU, if they receive information that they believe indicates money laundering or terrorist financing is being or has been committed or attempted, whilst providing legal advice, or in the course of legal action.

The fact that information has been transmitted to an FIU may not be revealed to the customer or to other third persons except for law enforcement purposes. The Art.2 entities must keep documents and supporting or other evidence for at least five years from the end of the business relationship or the carrying-out of the transaction. They are also expected to establish appropriate measures and

procedures for customer due diligence, reporting of information and record keeping, etc. and to ensure that relevant employees know of the provisions in force.

Member States are required to monitor compliance with the Directive. Where there is a failure to comply with the national provisions adopted, it must be possible for the Art.2 entities in question to be held liable for those infringements. The penalties must be effective, proportionate and dissuasive. Member States were required to bring into force the national legislation necessary in order to comply with the Directive by 15 December 2007.

8.3. Application of AML/CFT to the Online Environment

It is clear that the increasing emphasis on customer due diligence (CDD or KYC - Know Your Customer) measures is one of the main components of an effective anti-money laundering (AML) and combating the financing of terrorism (CFT) system. Such due diligence does not just mean an organization initially identifying a customer, and where a risk assessment suggests it is necessary, verifying that identity, but also scrutinising transactions undertaken throughout the course of the relationship, to ensure that the transactions conducted are consistent with the customer's known profile, and to permit monitoring for and acting on deviations from the customer's transaction profile. Some of the early e-money and e-commerce businesses were either unable, or unwilling, to adopt such due diligence measures; and some new e-commerce businesses, such as virtual worlds, have not yet fully addressed the implications of permitting their customers to engage in virtual environment transactions, such as sale of virtual property, which have the potential to result in real world financial transactions.

Given the relatively new nature of e-money and e-commerce businesses, there has been relatively little international co-ordination of responses to the risks of money laundering online. This has led to a variety of national approaches, including enforcement action for money laundering against hawala operators (UK) and against virtual precious metals dealers for 'operation of an unlicensed money transmitting business' (US). There are currently few, if any, national AML/CFT measures specifically dealing with electronic commerce. It is arguable that, in fact, such specific measures are unnecessary, given the potential breadth of existing AML/CFT measures, particularly within the EU following the Third AML/CFT Directive. A key concern has been that e-money and e-commerce businesses would seek to locate all or components of their businesses in international and offshore jurisdictions with weak AML/CFT regulation; thus enabling them to avoid regulatory oversight and to complicate prosecutions. In practice, as can be seen from the effect of the FATF Blacklist, direct and indirect pressure against both potentially weak jurisdictions, and against e-money and e-commerce businesses themselves, has tended to reduce this concern, with many such businesses

(e.g. WebMoney, noted above) actively seeking to demonstrate their compliance efforts with international AML/CFT standards.

While there has been some resistance amongst e-money and e-commerce businesses to the adoption of AML/CFT measures, particularly to the extent that these may limit the scope for anonymous transactions, which are potentially a useful market driver for e-money businesses, it should be noted that resistance to increased customer due diligence is not a phenomenon restricted to on-line businesses. The Third EU AML/CFT Directive has been widely criticized for imposing too heavy a regulatory burden on small financial and non-financial entities than the risk of significant money laundering through them actually justifies. Such resistance should not necessarily therefore be seen as signifying that e-money and e-commerce businesses are intrinsically opposed to AML/CFT measures, but rather as signifying that there are concerns that a blanket international approach to AML/CFT regulation, that does not take effective account of the cost/benefits of e-money transactions, even small-scale anonymous transactions, may be inappropriate for certain jurisdictions and market niches. An example of this might be WebMoney, an e-money service which was developed for the market in and around Russia, where access to conventional banking services may sometimes be limited and credit and debit cards are not always a viable payment option. As WebMoney has become a wider international phenomenon, it appears that some aspects of the service are more risky in money laundering terms, which is why it has attracted the attention of AML agencies, notably in the US. WebMoney's response has been to move to eliminate the most risky aspects of its service, but to retain some risky elements on a combined risk assessment and cost/benefit analysis.

8.4. Best Practice

Ideally, online and offline retail merchants and payment services should have comparable AML/CFT obligations. The goal of AML/CFT measures in online services cannot be the total eradication of money laundering, as this is not a realistic goal in either online or offline environments, but rather to make online services a less hospitable environment for money launderers to operate in.

Particular areas of weakness noted in national assessments of offline AML/CFT measures include:

- Inadequate attention given to transactions with higher risk countries;
- Inadequate detection and analysis of unusual large or otherwise suspicious transactions;
- Inadequate systems to report suspicious transactions;
- Inadequate guidelines for detecting suspicious transactions;
- Inadequate AML/CFT programmes in financial institutions and commercial entities, and inadequate authority to cooperate with law enforcement;
- Failure to place obligations on financial institutions and commercial entities to take reasonable measures to obtain information about customer identity;
- Lack of procedures for mutual assistance (e.g. production of records, and obtaining of evidence for money laundering investigations and prosecution) in criminal matters;
- Inadequate internal policies, procedures, controls, audit, and training programmes;
- Failure to report promptly to national Financial Intelligence Units if institutions suspect that funds stem from a criminal activity;
- Poor international exchange of information relating to suspicious transactions, as well as to persons or corporations involved.

It is likely that similar types of weakness will be found in the internet environment, where online retail merchants and payment services have considerably less experience in dealing with money laundering than banks and other financial institutions, and have often had little incentive by way of sectoral awareness raising, industry best practices or national regulation, to improve their AML/CFT measures.

In its 2008 Report *Money Laundering & Terrorist Financing Vulnerabilities of Commercial Websites & Internet Payment Systems*, FATF noted four key issues that it felt Likely to improve international capacity to cope with money laundering risks associated with commercial websites and Internet payment systems:

- Better awareness of money laundering risks: All parties involved, including private sector companies, traditional financial institutions and governmental bodies, need to be aware of both the general and the sector/technology-specific money laundering risks raised by online commercial and payment services. Without that understanding:
    - online commercial and payment services may fail to recognise and act upon key risks and money laundering patterns, that have been identified and catalogued in offline scenarios;
    - traditional financial institutions may fail to play their role in the detection and the monitoring of suspicious financial transactions in their dealings with online commercial and payment services;
    - any regulatory strategies proposed by government may risk failing to set, and meet, AML/CFT goals appropriate to the online environment, and might also damage the development of the sector.

  Development by regulators and trade associations of indicators of suspicious financial transactions (red flags) and reference materials on techniques used to launder money or finance terrorism (typologies), would help to raise awareness of the risks, as would training programmes and outreach sessions to the private sector.
- Similar national regulatory strategies and goals: Given the international character and presence of Internet, it is important that governments impose similar regulations, requiring customer identification, customer due diligence, record keeping and transaction reporting, to Internet payment service providers all around the world, to avoid a move to countries with the poor or no regulation.
- Leveraging industry best practices: There is scope for identifying and encouraging industry best practice and this could be:
    - used to ratchet up the international standard by providing a clear target for low risk practices, thereby allowing banks, financial institutions and other online service providers to identify and marginalise online commercial and payment services that fail to strive to emulate those practices

- an important part of the training programmes and outreach sessions to the private sector.

- Continuing to develop international cooperation: Because of the international character of the Internet and commercial websites' activities, international co-operation will be a key factor in the fight against money laundering. Countries need to work cooperatively to identify appropriate AML/CFT strategies/regulation for commercial websites and Internet payment systems, and to fashion effective responses if there is a failure to comply. International cooperation is also needed to ensure that entities which operate across jurisdictions do not, by default, fall outside any regulatory control. Where money laundering is suspected, countries need to be able to ensure rapid and efficient exchange of information, and to have created appropriate processes for mutual assistance.

This area is still evolving, and new e-commerce/e-money products will give rise to new risks. New mitigation strategies will therefore be constantly needed.

Table:2 AML/CFT Risks in Online transactions

ML Action	Online Transaction Issue	Description	Possible Solutions
Placement	Anonymity on services	Some online commercial/payment services (OC/PS) permit registration and or transactions to take place anonymously, e.g. by e-mail.	- Require OC/PS not to keep anonymous accounts. - Require financial institutions dealing with OC/PS that permit anonymous accounts to treat those transactions as high or higher risk. - Place limits on the amount of money that can be transferred into, or out of, an anonymous account either in total and/or in one transaction. Use activity limits.
	No face-to-face customer/provider relationship	Traditional verification mechanisms used by off-line commercial/payment services are not available to OC/PS.	- Online identity verification (e.g. electronic identity cards) to help OC/PS reduce ML risks. - Require OC/PS to monitor financial transactions, monitoring for and acting on deviations from customer transaction profile. - Require financial institutions dealing with OC/PS to treat those transactions as higher risk. - Remind financial institutions dealing with OC/PS transactions to watch for abnormal or disproportionate transactions with regards to their own customer profiles. - Where payment to OC/PS is via financial institution, use random charge process to verify

			identities of customers (e.g. PayPal)
	Multiple registrations/identities	Use of multiple (and possibly anonymous) registrations to purchase and sell items can create problems for screening, monitoring and reconstructing transactions and flow of funds.	- Require OC/PS not to keep anonymous accounts. - Online identity verification to reduce the ability to create multiple accounts - Require OC/PS to have processes in place to deal with identity theft
	Remote access	Internet services can be obtained from anywhere in the world, e.g. cybercafés. Individuals can connect from web terminals not affiliated or registered to their identity.	- Require OC/PS not to keep anonymous accounts. - Online identity verification to link accesses to identity - Require OC/PS to have processes in place to deal with identity theft
	Anonymous paying in methods	If pre-paid cards, gift cards/gift cheques or cash are used to credit online accounts, the origin of the funds is harder to trace.	- OC/PS not to permit anonymous paying in methods - Place limits on the amount of money that can be transferred into an account by anonymous means either in total and/or in one transaction.
Layering	Speed of transactions	Electronic transactions between sellers and buyers are performed very rapidly – there may be little time for OC/PS to react to suspicious behavior	- Delays could be artificially introduced to permit manual checking of abnormal transactions and of higher use accounts. - Real time screening of customers, their activities and transactions. - Full audit trails of commercial transactions and payments. - Use activity limits e.g. only a certain number of transactions per account per day

	Cross-border/Multiple jurisdiction	The international character of transactions may mean the jurisdiction where the OC/PS is located may not be competent to investigate and prosecute ML. Additionally situations may arise where no single jurisdiction has clear responsibility for regulating and monitoring activity.	- Require financial institutions dealing with OC/PS with operations in riskier jurisdictions to treat those transactions as high or higher risk. - Put pressure on non-conformant jurisdictions through FATF and its regional groups, and work to harmonize AML/CFT rules on the 40+9 Recommendations to reduce cross-jurisdictional issues.
	Volume and size of payments	High numbers of transactions and differing amounts per transaction make it more difficult for OC/PS to define criteria to monitor and screen transactions	- Monitor automatically using risk models built to detect illegal activities, abnormal transactions or high volume activity based on existing information e.g. from customers (identity, address, e-mail, IP addresses used), obtained internally (previous transactions, item country location, customer location), obtained from external sources (countries at risk for certain forms of ML/TF)
	Limited human intervention	The personal interaction often associated with off-line transactions which is a key part of front line 'know your customer' money laundering detection are not available and have to be replaced by second level detection mechanisms.	- Monitor automatically using risk models built to detect illegal activities built to detect illegal activities, abnormal transactions or high volume activity based on existing information
	Inadequacy or lack of technical solutions for audit trails, record keeping or suspicious transactions	Providing sophisticated second level detection mechanisms is often not a priority for OC/PS, particularly smaller services. Even where automated systems are available, they may be of limited use in	- Bar financial institutions from dealing with OC/PS that do not meet minimum requirements for automated AML/CFT monitoring - Require any financial institution dealing with

	reporting	detected sophisticated ML schemes.	OC/PS to assess the AML/CFT risk of doing so - Place limits on the amount of money that can be transferred into, or out of, an account at OC/PS with limited monitoring capacity.
Integration	Ability to buy high value goods	It is possible to buy high value items, precious metals, real estate or securities on commercial websites using an Internet payment system	- Require all high value transactions by Internet payment system to be flagged high risk. - Require high value transactions by Internet payment system to be flagged high risk if the customer is a first time buyer - Require high value transactions by Internet payment system to be flagged high risk, if the transaction is abnormal, or in conjunction with other evidence fits a pattern for ML/TF.
	Anonymous paying out methods	If pre-paid cards, gift cards/gift cheques can be purchased, or cash (e.g. via redemptions at ATMs) obtained via online accounts, the destination of the funds is harder to trace.	- OC/PS not to permit anonymous paying out methods - Place limits on the amount of money that can be transferred out of an account by anonymous means either in total and/or in one transaction.

8.5. Brief Guide to the FATF Forty Recommendations

Legal Systems (in line with UN conventions)

1. Legal systems should specify a broad scope of money-laundering offenses by criminalizing money laundering related to all serious offenses and capturing, at a minimum, the designated range of offenses.
2. Legal systems should establish standards to prove the offense of money laundering and to clarify that criminal, civil, and administrative liability will apply to legal persons (corporations).
3. A country should have authority to confiscate illegal funds and to apply provisional measures, such as freezing or seizing to deal with money-laundering offenses.

Preventive Measures (to be taken by financial institutions and nonfinancial businesses)

4. Secrecy laws should not prevent implementation of the recommendations.
5. Financial institutions and nonfinancial businesses should have an obligation to carry out customer due diligence, including identifying and verifying customer identity.
6. Financial institutions and nonfinancial businesses should have special measures in place for politically exposed persons.
7. Financial institutions and nonfinancial businesses should have special measures in place for correspondent banking.
8. Financial institutions and nonfinancial businesses should have measures in place to address money-laundering threats from new technologies and from business that is not conducted face to face.
9. Financial institutions and nonfinancial businesses should rely on third parties for customer identification and for introduced business.
10. Financial institutions and nonfinancial businesses should adhere to a five-year record-keeping requirement.
11. Financial institutions and nonfinancial businesses should pay special attention to complex, unusual large transactions and to all unusual patterns of transactions.
12. Customer identification should be applied to designated nonfinancial businesses and professions (DNFBPs).

13. Financial institutions and nonfinancial businesses should have an obligation to report suspicious transactions to financial intelligence units.
14. Legal protection should be granted for persons reporting their suspicions in good faith, and prohibitions against tipping off should be established.
15. Financial institutions and nonfinancial businesses should have measures in place for internal controls, compliance, and audit.
16. Requirements for reporting and monitoring suspicious activity should be applied to DNFBPs.
17. A country should have effective, proportionate, and dissuasive sanctions for money-laundering offenses.
18. A country should not allow the establishment of shell banks.
19. Financial institutions and nonfinancial businesses should consider monitoring of cross-border cash transportation and should develop a system for reporting currency transactions above a fixed amount.
20. Financial institutions and nonfinancial businesses should consider applying FATF requirements to other businesses beyond DNFBPs.
21. Special attention should be given to higher-risk countries.
22. AML requirements should be applied to foreign branches and subsidiaries.
23. Financial institutions should be subject to adequate regulation, supervision, and monitoring.
24. DNFBPs need to be subject to regulation, supervision, and monitoring.
25. Competent authority should provide guidelines on reporting, along with feedback on effectiveness.

Institutional and Other Measures

26. A country should have established a financial intelligence unit.
27. A country should have a designated law enforcement authority for money-laundering and financing-terrorism offenses.
28. Law enforcement authority should have adequate legal powers for investigation.
29. Regulators should have adequate legal powers to monitor and ensure compliance with AML–CFT requirements.

30. Competent authorities should have adequate resources, integrity, and training for AML–CFT efforts.
31. Effective mechanisms need to be developed domestically for cooperation.
32. Institutions should maintain statistics on reporting, investigations, prosecutions, and mutual legal assistance.
33. Institutions should establish measures to deter unlawful use of corporations and timely information on beneficial ownership and control.
34. Institutions should establish measures to prevent unlawful use of legal arrangements (e.g., trusts), and ensure timely information on settlor, trustee, and beneficiaries.

International Cooperation

35. Each country should adopt Vienna, Palermo, suppression of financing of terrorism, and other international conventions.
36. Each country should rapidly provide mutual legal assistance.
37. Each country should render assistance notwithstanding the absence of dual criminality.
38. Each country should have expeditious powers to identify, freeze, seize, and confiscate property laundered from money laundering and financing terrorism.
39. Each country should recognize money laundering as an extraditable offence.
40. Each country should provide a wide range of other possible international cooperation.

8.6. Special Recommendations for Combating the Financing of Terrorism

1. Ratify and implement relevant UN conventions and resolutions.
2. Criminalize terrorist financing.
3. Implement measures to freeze and confiscate terrorist assets.
4. Have a suspicious transaction reporting requirement that applies to suspicion of terrorist financing.
5. Provide cooperation on proceedings related to financing of terrorism.
6. Implement measures to deter improper use of money- and value-transfer services.
7. Call for countries to require adequate originator information in fund transfers and related messages.

8. Call for countries to review adequacy of laws and regulations related to non-profit organizations to prevent misuse for terrorism purposes.
9. Have measures to detect physical cross-border transportation of currency and bearer negotiable instruments.

From:

Financial Sector Assessment: A Handbook

<http://www.financelearning.org/fsapbook/ch08.pdf>

Table 3: FATF members

Argentina	France	Japan	Russian Federation
Australia	Germany	Luxembourg	Singapore
Austria	Greece	Mexico	South Africa
Belgium	Gulf Co-operation Council	Kingdom of the Netherlands	Spain
Brazil	Hong Kong, China	New Zealand	Sweden
Canada	Iceland	Norway	Switzerland
Denmark	Ireland	People's Republic of China	Turkey
European Commission	France	Japan	United Kingdom
Finland	Italy	Portugal	United States

The Republic of Korea and India became observers on 27 July 2006 and 27 November 2006 respectively, and both are currently working towards becoming FATF members.

9. State of the Art of Cyber Terrorism: Attacks and Countermeasures

9.1. Introduction

The recent news related to the (supposed) reliability incident at the FAA System, which caused more than 24 hours of flights delay and deletion, pointed out to the importance of the critical infrastructure protection. With the term "Cyber Terrorism", Denning (2000) defines "convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyber terrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyber terrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not.

9.2. An Evolving Threat

Susan W. (*Brenner, 2006*) offers her own semantic and operational definitions of Cyber Terrorism. Semantically, Brenner defined 'Cyber Terrorism' as "the use of computer technology to advance terrorist goals. It is the pursuit of terrorist agenda by other means, i.e., computers versus guns and Improved Explosive Devices (IEDs)." Brenner articulate some distinctions between "Cyber Terrorism," with its ideological goals, "Cyber Crime," with its individual goals (e.g. money, sex, revenge, etc.) and "Cyber Warfare," with its nation-state goals (e.g. political, economic and tactical). Of course, as Brenner remarked, these distinctions erode quickly. For example, there are acts of state-sponsored sponsored terrorism and state-sponsored crime. Furthermore, the distinction between "personal" goals and nation-state activity erodes because it is based on territorial sovereignty. Crime is typically viewed as an internal threat and war as an external threat, with terrorism as either or both. But computers undermine this distinction by making territory irrelevant for many purposes. Brenner cited the October 2006 cyber attacks from the People's

Republic of China targeting the US Department of Commerce. The nature of the attack is still unknown. Many expert talks about cyber crime, cyber terror and cyber warfare, offering both primary and secondary operational definitions. The primary operational definition played on the term, "Weapons of Mass Destruction" (WMD), posting that term "Cyber Terrorism" relates to three different types of WMD:

- Weapons of Mass Destruction
- Weapons of Mass Distraction
- Weapons of Mass Disruption

Concerning "Weapons of Mass Destruction", some Security vendor has been rightly condemned because of the use of such hyperbolic terms as "Digital Pearl Harbor" and "Digital 911," noting that it is unlikely computers could inflict the demoralizing kind of carnage experienced on 911 and that such terms foster a misunderstanding of how computers can be used to further terrorists' goals. While some effect of 9/11 has clearly been digital, it shall also be remarked that the widely held belief that "Cyber Terror" is an exaggerated concept meant to spread "F.U.D." (i.e. "Fear, Uncertainty and Doubt") is based on such bombast.

"Weapon of Mass Distraction," on the other hand, refers to the use false information to demoralize civilians. As an example, Power *(2006*) shared an anecdote about the fake report of an impending catastrophe (i.e., that there was a suitcase nuke on mass transit system serving San Francisco bay area). According to Power's source, an anonymous government official, an emergency evacuation order was almost issued for millions of people.

"Cyber Terrorism" as a "Weapon of Mass Distraction" could be used, Power remarked, to exaggerate or enhance a real attack, e.g., by magnifying the impact of the attack or misidentifying targets.

The goals of "Cyber Terrorism" as a "Weapon of Mass Disruption" would be to demoralize civilian populace and create chaos by attacking infrastructure components,

such as the electrical grid, the financial systems, the air traffic control system and/or the transit systems.

As a real world case example, it could be useful to reference the impact of a Botnet attack on a Seattle Hospital. The attack shut down Internal Care Unit (ICU) computers, operating room doors and doctors' pagers.

The secondary operational definition related to "Cyber Terrorism" is as a "Tool," e.g., the use of the Internet for organizational, propagandizing or fund-raising, revenue-generating and money-laundering activities. But problems arise with this secondary operational definition, Many of the activities -- propaganda, other communications, funds transfers, research -- may be legal.

9.3. The Importance of Awareness & Education in Fighting Cyber Terrorism: Getting Beyond the Hype and Hoax

As previously remarked, the purveyors of F.U.D. have done a lot of harm to our cause, and so we stress that cyber security awareness and education must be designed to engage, enlighten and empower the workforce or the citizenry, rather than to sow fear among them or impose control over them.

It is also imperative to use four vital elements in developing awareness and education content: use intriguing themes, reference credible sources, present plausible scenarios, and most important, make it relevant to both current events and people's personal lives.

Underscoring the themes of credibility and plausibility, we ask "Where is Cyber Terrorism on the Scale of Risks and Threats?" Because perspective and proportionality are key issues in developing awareness and education related to Cyber Terrorism. Perspective and proportionality communicate credibility.

In the view of the author of this chapter, there is a "Dissonant Convergence," a 21st Century Security Crisis, in which Cyber Terrorism is no more than a sub-set of both

Terrorism and Cyber Crime, and therefore ranks at the middle and toward the bottom, respectively, in a long list of serious risks and threats:

- Global Warming
- Nuclear Weapons Proliferation
- Pandemics and Other Health Emergencies
- Natural Disasters
- Terrorism (with "Cyber Terrorism" as a sub-set)
- Failed States
- Sustainability Issues (e.g. energy, water, over-population)
- Organized Crime (e.g. human trafficking, drug trade, counterfeiting)
- Cyber Crime (with "Cyber Terrorism" as a sub-set)

Continuing to stress the themes of credibility and plausibility, consider the useful parallels between "Bird Flu" and "Cyber Terrorism."

Although Bird Flu has been found in almost 50 countries since 2003, it has infected less than 300 people and killed less than 200.

Yet billions of dollars are being spent to prepare for a serious Bird Flu pandemic. Why? Because two out of the three factors that create pandemic are already in play, and if the third factor (human to human transmission) is activated, millions of people could die and many hundreds of billions of dollars could be lost to regional and global economies.

But even if Bird Flu does not become a pandemic, the planning, training and preparations will help in coping with whatever health emergencies inevitably befall us. The risk of Cyber Terrorism should be viewed and dealt with similarly. We cannot afford to assume it won't happen because it hasn't (or perhaps merely because it hasn't been acknowledged to already have happened).

In regard to the Who and Why of Cyber Terrorism, our intelligence analysis offers a rather different perspective on the list of usual (and unusual suspects):

- Jihadists bent on delivering crushing economic and psychological blows
- Nation States, i.e., hegemons and rogues, bent on distracting and debilitating the adversary
- Cults and loners bent on hastening the apocalypse, or tear down the social order
- Criminal elements bent on extortion or reprisal
- Corporate enemies bent on foiling competitors
- Political enemies bent on subverting democratic institutions

Although most conventional wisdom focuses on cyber terrorism related to Jihadists or Nation States, in the view of the author of this paper, it is quite likely that the world will experience acts of Cyber Terrorism perpetrated by cults and loners in furtherance of their bizarre world-views.

9.4. Parallelizing Cyber and "Tangible" Terrorism: an "Excursus" on the Major Events of the Last 30 Years

The Aum Shinrikyo (Supreme Truth) cult, which was responsible for the 1995 Sarin gas attack on the Tokyo subway system, and Theodore Kaczynski (aka the Unibomber), who was responsible for sixteen letter bomb attacks over a span of years from 1978 until 1995, exemplify these threats.

In his brilliant study, *Cult At The End of the World*, David E. Kaplin captures the amazing scope and disturbing implications of the Aum Shinrikyo story:

"In 1984, guru Shoko Asahara had a one-room yoga school, a handful of devotees, and a dream: world domination. A decade later, Aum Supreme Truth boasted 40,000 followers in six countries and a worldwide network that brought it state-of-the-art lasers, lab equipment, and weaponry. Aum's story moves from the dense cities of postindustrial Japan to mountain retreats where samurai once fought, and then overseas - to Manhattan and Silicon Valley, Bonn and the Australian outback, and finally to Russia. It is there, in

the volatile remains of the Soviet empire, that the cult found ready suppliers of military hardware, training, and, quite possibly, a nuclear bomb."

But, perhaps the most extraordinary twist in the plot is that the story didn't end with the capture of Shoko Asahara and other cult leaders.

In 2000, the BBC reported: "Japan's Defense Agency delayed deployment of a new computer system after discovering that it used software developed by members of the Aum Shinri Kyo cult. The Defense Agency was only one of 90 government organizations and private companies that unknowingly ordered software produced by the cult." (*BBC, 3-1-00*)

As recently as September 2006, the cult was still a source of concern: "Japanese security officers today raided 25 offices of the doomsday cult behind the 1995 Tokyo subway nerve gas attacks, after its founder lost a last appeal against his death sentence. Since his death sentence was finalised, we are afraid that his followers may possibly plan something illegal, said a Public Security Intelligence Agency spokesman." (*The Australian, 9-16-06*)

Just as the story of Aum Shinrikyo provides a stunning example of what a cult bent on wreaking havoc and mayhem could do, using Cyber Terrorism as a tool, the remarkable tale of Ted Kaczynski, the Unibomber, illustrates what one profoundly disturbed individual can carry out on his own. Working without accomplices, living in seclusion in a shack in the mountains of Montana, without a telephone or a car or electricity or running water, Kaczynski eluded a nation-wide FBI manhunt for many years. All the while, he never betrayed himself, even as he crafted meticulous letter bombs and delivered them, undetected, to commit numerous acts of murder and attempted murder. Until he sent his "Unibomber Manifesto" to the newspapers for publication, and David Kaczynski thought the ideas and writing style bore a striking resemblance to that of his brother Ted.

The most recurring question that hundreds of analysts asked themselves was: "Why did he do it?"

"The Industrial Revolution and its consequences have been a disaster for the human race…. We therefore advocate a revolution against the industrial system. This revolution may or may not make use of violence; it may be sudden or it may be a relatively gradual process spanning a few decades…." (*UNABOMBER Manifesto*)

Imagine what a Cyber Unibomber could do using Cyber Terrorism to target critical infrastructure. Imagine how long he could elude identification and capture.

Just as plausibly, the author of this paper also suggested we could see acts of Cyber Terrorism come from elements of organized crime -- either in pursuit of profit or in an effort to intimidate governments and societies.

Considering this excerpt from a recent news story could help further:

"Cyberscams are increasingly being committed by organized crime syndicates out to profit from sophisticated ruses rather than hackers keen to make an online name for themselves, according to a top U.S. official Christopher Painter, deputy chief of the computer crimes and intellectual property section at the Department of Justice."

"The FBI estimates all types of computer crime in the U.S. costs industry about $400 billion while in Britain the Department of Trade and Industry said computer crime had risen by 50 percent over the last two years."

"A growing worry is that cybercrooks could target emergency services for extortion purposes or that terrorists may be tempted to attack critical utility networks like water and electricity. Painter said there was a recent case in the U.S. where two young hackers inadvertently switched off all the lights at the local airport." (*Reuters 9-15-06*)

Other aspects of the presentation reflected analysis and recommendations from two recent *War and Peace* in *Elsevier Science's Cyberspace* columns, "Ten Years In The Wilderness, A Retrospective, Part 2: Cyber Security = National Security" and "Case Study: A Bold New Approach to Awareness and Education, And How It Met An Ignoble Fate".

9.5. Current and Future Technical Trends

One of the basic rules of information security applied to the critical infrastructure protection and cyber crime enforcement is: Security holes must be responsably disclosed. This will help system owners to fix eventual problems. One of the most important practical security conference of the world (BlackHat.com) is the demonstration of how the security disclosure is important and how much an exploit can be used by "conventional" hackers and cyber terrorism.

At the latest BlackHat conference in LasVegas, two security researchers have demonstrated a new technique to stealthily intercept internet traffic on a scale previously presumed to be unavailable to anyone outside of intelligence agencies like the National Security Agency.

The tactic exploits the internet routing protocol BGP (Border Gateway Protocol) to let an attacker surreptitiously monitor unencrypted internet traffic anywhere in the world, and even modify it before it reaches its destination.

The demonstration is only the latest attack to highlight fundamental security weaknesses in some of the internet's core protocols. Those protocols were largely developed in the 1970s with the assumption that every node on the then-nascent network would be trustworthy. The world was reminded of the quaintness of that assumption in July, when researcher Dan Kaminsky disclosed a serious vulnerability in the DNS system. Experts say the new demonstration targets a potentially larger weakness. This is one of the most dangerous and large internet security holes ever. Nations must be aware of such problems and fix them before is too late.

9.6. The Role of Cyber Investigations in Combating Cyber Crime and Cyber Terrorism

We will discuss Digital Forensics in another chapter of this document. However, it is important to remember that Cyber Investigations are a fundamental part of the game. At

the same time, cyberterrorists know the potentials of the cyber investigations and try to circumvent them.

Today's digital investigators face several major problems, including:

- Anti-Forensics
- Lack of organization and information exchange
- Different Investigative and legal standards
- Lack of skills

"Anti-Forensics" refers to various methods to negatively impact the existence, amount and/or quality of evidence from a crime scene, or to make the examination and analysis of such evidence either more difficult or even impossible to conduct.

Real-world examples include documented attacks against both media analysis tools (e.g., FTK, EnCase, iLook, WinHex, TCT, Sleuthkit, etc.) and traffic analysis tools.

Transmogrify is an example of a tool that foils media analysis; it defeat EnCase's file signaturing capabilities by allowing you to mask and unmask your files as any file type.

The Onion Router (TOR) is an example of a tool that allows you to avoid traffic analysis. The objective of Onion Routing is to make it completely impossible for third parties to perform traffic analysis.

This goal is achieved by applying cryptographic techniques to networking. The packets transiting the chain of onion routers thus appear anonymous.

Practically speaking, there is a group of onion routers distributed around the public network, each of which has the task of encrypting the socket connections and to act in turn as a proxy.

Terrorists and criminals use TOR in several ways:

- File Exchange: TOR makes it possible for users to hide their locations while offering various kinds of services, such as web publishing or an instant messaging server, and also a secure peer-to-peer network. (This method is used to exchange child pornography.)
- Terrorism Operation Management: Using TOR "rendezvous points," other TOR users can connect to hidden services without knowing each other's network identity.
- Blind Crews: In this way, a group of hackers, for example, could break into a system and leave it open for another group, a terrorist cell, who don't know them.

On September 11, 2006, the German police raided seven ISPs and individuals. Although six computers (Tor nodes) were confirmed to have been seized, German civil liberties advocates assert that dozens (if not hundreds) of other computers also seized. The systems taken in this raid were not seized for operating as anonymity proxy servers using the Tor network protocol. The premise for the seizures was that the servers showed up in a server log on a child pornography site. (*Source: Wikinews*)

But as we mentioned there are some other challenges that confront today's digital investigators.

Lack of organization and information exchange can be overcome with international agreements, investigative groups and professional associations.

Differences in investigative and legal procedures can be overcome with RFCs, DFRWs and standards.

Lack of skills can be overcome with training and virtual communities.

Skype and other "Secure VOIP" present some challenges that lawful interceptors are still struggling to overcome. Likewise, steganography, virtual machines and cover channels present some challenges for which technology providers have yet to produce effective defectors.

9.7. The Importance of a Proactive Solution

What should the governments of the emerging Eastern European countries due in regard to cyber forensics? Establish their own incident response teams and national cyber forensics labs by receiving training and consultation with forensics experts from the other NATO and EU countries. Start working on methodologies, and then start working on tools and techniques. Having a national incident response team should be mandatory. This national incident response team should have a forensic lab within it. The Netherlands offers an excellent model.

What should the telecoms and other infrastructure entities in the new nations do? Their number one priority should be starting immediately to set up a logging infrastructure. It should be related but not limited to net logging, connection logging, database applications and share logging (against internal misuse). They should also be working to establish an incident response architecture composed by processes, procedures and technologies. It is also vital that the security function should be separated from internal audit.

What judges and magistrates should do? The author of this paper believes that two different (but synergic) routes should be taken. The first one is Law Harmonization, the second should be an articulate security awareness and technical/intelligence Exchange programme.

The Harmonization of laws is clearly based upon the effective recognition and application of the Convention of Budapest.

The Convention is the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security. It also contains a series of powers and procedures such as the search of computer networks and interception.

Its main objective, set out in the preamble, is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation.

The Convention aims principally at (1) harmonising the domestic criminal substantive law elements of offences and connected provisions in the area of cyber-crime (2) providing for domestic criminal procedural law powers necessary for the investigation and prosecution of such offences as well as other offences committed by means of a computer system or evidence in relation to which is in electronic form (3) setting up a fast and effective regime of international co-operation.

The following offences are defined by the Convention: illegal access, illegal interception, data interference, system interference, misuse of devices, computer-related forgery, computer-related fraud, offences related to child pornography and offences related to copyright and neighbouring rights. It also sets out such procedural law issues as expedited preservation of stored data, expedited preservation and partial disclosure of traffic data, production order, search and seizure of computer data, real-time collection of traffic data, and interception of content data. In addition, the Convention contains a provision on a specific type of cross-border access to stored computer data which does not require mutual assistance (with consent or where publicly available) and provides for the setting up of a 24/7 network for ensuring speedy assistance among the Signatory Parties.

The Convention is the product of four years of work by European and international experts. It has been supplemented by an Additional Protocol making any publication of racist and xenophobic propaganda via computer networks a criminal offence. Currently, cyber terrorism is also studied in the framework of the Convention.

It is clear that the Eastern European Countries are required to apply what they subscribed and, if they did not subscribed the Convention yet they should do it as soon as possible. Magistrates are required to implement the principles introduced by the Convention, with the use of the Specialized Police Forces (if present) and/or supporting such initiatives.

As a former Police Officer who actively worked on cyber crime and cyber terrorism enforcement, the author of this paper also think that a major method used in preventing cyber terrorism is the sharing of intelligence information. The most advanced police and judiciary offices routinely passes intelligence received in active investigations or developed through research to the intelligence community.

Cyber programmes are unique in nature. However, taking proactive investigative measures with tools such as Honey Pots/Nets and Undercover Operations enhances our ability to prevent a cyberterrorist attack. The U.S. Government, for example, has undertaken the following initiatives to combat cyber terrorism: Cyber Task Forces, Public/Private alliances, International Cyber Investigative Support, Mobile Cyber Assistance Teams, Cyber Action Teams, Cyber Investigators Training, a Cyber Intelligence Center, and Cyber Tactical Analytical Case Support. These programmes provide a strategic framework and programme management tool for all the computer intrusion investigations units in a particular country.

A Cyber Specialized Training Programme coordinates with the Engineering Research Facilities Laboratory Divisions, Training Divisions, National White Collar Crime Centers, private industry, academia and others to deliver training to Government cyber squads, Task Forces, International Law Enforcement Officers, and others.

In the event of a cyberterrorist attack, the Police (and the related judiciary unit) will conduct an intense post-incident investigation to determine the source including the motive and purpose of the attack. In the digital age, data collection in that investigation can be extremely difficult. The computer industry is also conducting research and development involving basic security, such as developing cryptographic hardware which will serve to filter attempts to introduce malicious code or to stop unauthorized activity. Continued research in these areas will only serve to assist the nations in its work against cyberterrorism.

Last but not least, Incident and Cyberterrorism Simulations. Researchers at the University of Texas at San Antonio for example performed an exercise testing the city's ability to prevent cyberterrorists from hacking into city computer systems.

The Center for Infrastructure Assurance and Security at UTSA worked with local and state governments and the private sector on the exercise, called "Dark Screen." Dark Screen involved the National Guard of Texas, the San Antonio and Bexar County governments, the San Antonio Water System and city public utilities. Private-sector companies included banks, energy companies and communications companies. One potential threat the exercise examined is an electronic attack on the sewage system. Cyberterrorists could hack into the computer system and reverse the flow of wastewater into fresh water for example. Such examples could be also applied in other parts of the world.

9.8. Conclusions

The technological age we are living has forced the nations to engage a new set of national security challenges. Several potential adversaries have cyberspace capabilities comparable between each others and are constantly conducting surveillance, gathering technical information, and mapping critical nodes that could be exploited in future conflicts. The the cyber terrorism threat is something that cannot be deleted nor wiped. However, there are several steps that can be taken, internationally, to mitigate the threat itself. The most important step is separating the Cyber Prevention from Cyber Recovery. Both Security people intelligence, police and magistrates are part of both factors.

10. COMPUTER FORENSICS

10.1. Introduction

There are several ways to combat cyber crime. One of them is related to the law and judiciary system, while the second concerns the technical aspects to be taken during an investigation. In this chapter we will examine both aspects, with an overview on the state of the art.

The legislative part of the topic has been internationally covered since 2001 with the EU Convention of Cybercrime, also known as "the Convention of Budapest". This convention, which has been "received and signed" by almost all the EU/SEE countries, requires a series of procedural and technical steps to take. For the purpose of this chapter, a description of the inherent steps follows.

Title 4 – Search and seizure of stored computer data

Article 19 – Search and seizure of stored computer data

1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:
a) a computer system or part of it and computer data stored therein; and
b) a computer-data storage medium in which computer data may be stored in its territory.
2. Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system.
3. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to:

a) seize or similarly secure a computer system or part of it or a computer-data storage medium;
b) make and retain a copy of those computer data;
c) maintain the integrity of the relevant stored computer data;
d) render inaccessible or remove those computer data in the accessed computer system.

4. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2 (of the Convention, Nda) .
5. The powers and procedures referred to in this article shall be subject to Articles 14 and 15 (of the Convention, Nda).

Title 5 – Real-time collection of computer data

Article 20 – Real-time collection of traffic data

1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to:

a) collect or record through the application of technical means on the territory of that Party, and
b) compel a service provider, within its existing technical capability:

i. to collect or record through the application of technical means on the territory of that Party; or

ii. to co-operate and assist the competent authorities in the collection or recording of, traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system.

2. Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic

data associated with specified communications transmitted in its territory, through the application of technical means on that territory.

3. Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Article 21 – Interception of content data

1. Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to:

a) collect or record through the application of technical means on the territory of that Party, and

b) compel a service provider, within its existing technical capability:

i. to collect or record through the application of technical means on the territory of that Party, or

ii. to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system.

2. Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory.

3. Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15 (of the Convention, Nda).

10.2. Considerations on the Relationship between Computer Forensics and Legal Procedures

To better understand the requirements established by the convention mentioned above, it is important to define an introduction to computer forensics. Computer forensics is a newly emerged and developing field which can be described as the study of digital evidence resulting from an incident or a crime.

Computer forensics, also called cyberforensics, is the application of computer investigation and analysis techniques to gather evidence suitable for presentation in a court of law. The goal of computer forensics is to perform a structured investigation while maintaining a documented chain of evidence to find out exactly what happened on a computer and who was responsible for it. Thus, it is fundamental, for police operators, consultants, and magistrates, to metabolize the following concepts:

1. Acquire the evidence without altering or damaging the original.
2. Authenticate that the recovered evidence is the same as the originally seized data.
3. Analyze the data without modifying it.

The factors mentioned above are fundamental. Many court proceedings, where such factors were not respected, finished with an invalidation of the digital evidence collection.

10.2.1. Standard Methodology

"A standard methodology will provide for the protection of evidence and some common steps that should be followed in the investigation process" (*McMillan, 2000*). The standard methodology should encompass the following "activities/procedures for securing a suspected computer incident scene [and include] shutting the down the computer, labeling the evidence, providing chain of custody documentation, documenting the evidence and transporting the evidence" (*Grace, 2001*). The methodology should also apply to evidence handling, authentication and storage.

A lack of application of the principles above could generate, again, a non recognition in court. This is not a silly problem. In a world (and an historical period) where many criminal and civil proceedings are managed on international scale, observing a standard methodology is mandatory.

An important thing to remind is also that, at this stage, no local law does regulate the technical procedures. This is important to clarify, because it is better to demand the practical procedures of the principles above to the scientific community, like everywhere in the world.

An important base of this paradigm is clarified by one of the most respected scientific document in the field, the RFC 3227 edited by the Internet Engineering Task Force (IETF). It is one of the most produced (and recognized in court) master documents, and basically relates to several factors, including but not limited to:

10.2.2. Privacy Considerations

A computer forensic procedure must respect the privacy rules and guidelines of companies and individuals, established legal jurisdiction. In particular, the operator must make sure no information collected along with the evidence he/she is searching for is available to anyone who would not normally have access to this information. This includes access to log files (which may reveal patterns of user behaviour) as well as personal data files. This does not mean that investigations and forensics cannot be done because of privacy, but that the operator should not intrude on people's privacy without strong justification. In particular, the operator:

1) should not collect information from areas he/she do not normally have reason to access (such personal file stores) unless you have sufficient indication that there is a real incident or a security violation.

2) Make sure have the backing of the agency established procedures in taking the steps do to collect evidence of an incident/violation.

10.2.3. Legal Considerations

According to Mercuri (*2005*), if access to digital evidence is not forthcoming from an impounding agency, court orders may be necessary to obtain the data as well as use of the extraction tools, in order to determine whether protocols had been appropriately applied. Conversely, a prosecution or defense team may wish to suppress evidence from discovery, if they believe it could be damaging to the case. Here is where the time-consuming aspects of the forensic examination may come into play. Typically it is not possible to perform a comprehensive decomposition and logging of all materials (such as the contents of every sector of a terabyte hard drive, or thousands of hours of digital video from a surveillance camera), so a "scratch-and-sniff" approach might be used to yield promising information. Even though cost-effective, tactical decisions to proceed with only a partial investigation may be regretted in hindsight if a post-mortem comprehensive analysis shows that an alternative outcome might have prevailed.

In any case, Computer evidence needs to be:

- *Admissible:* It must conform to certain legal rules before it can be put before a court.
- *Authentic:* It must be possible to positively tie evidentiary material to the incident.
- *Complete:* It must tell the whole story and not just a particular perspective.
- *Reliable:* There must be nothing about how the evidence was collected and subsequently handled that casts doubt about its authenticity and veracity.
- *Believable:* It must be readily believable and understandable by a court.

10.2.4. The Collection Procedure

The collection procedures should be as detailed as possible. They should be unambiguous, and should minimize the amount of decision-making needed during the collection process. The methods used to collect evidence should be transparent and reproducible. The operator should be prepared to reproduce precisely the methods used, and have those methods tested by independent experts.

There are several Collection Steps that shall be covered. Following there are several points of care.

- Where is the evidence? List what systems were involved in the incident and from which evidence will be collected.
- Establish what is likely to be relevant and admissible. When in doubt err on the side of collecting too much rather than not enough.
- For each system, obtain the relevant order of volatility.
- Remove external avenues for change.
- Following the order of volatility, collect the evidence with tools that are reliable and verified by the community.
- Record the extent of the system's clock drift.
- Question what else may be evidence as you work through the collection steps.
- Document each step.
- Don't forget the people involved. Make notes of who was there and what were they doing, what they observed and how they reacted.
- Where feasible you should consider generating checksums and cryptographically signing the collected evidence, as this may make it easier to preserve a strong chain of evidence. In doing so you must not alter the evidence.

10.2.5. The Archiving and Management Procedure

Evidence must be strictly secured. In addition, the Chain of Custody needs to be clearly documented. In particular, the operator should be able to clearly describe how the evidence was found, how it was handled and everything that happened to it. The following need to be documented:

- Where, when, and by whom was the evidence discovered and collected.
- Where, when and by whom was the evidence handled or examined.
- Who had custody of the evidence, during what period. How was it stored.
- When the evidence changed custody, when and how did the transfer occur (include shipping numbers, etc.).

It is also important to know where and how to archive digital evidence. If possible, commonly used media (rather than some obscure storage media) should be used for archiving. Access to evidence should be extremely restricted, and should be clearly documented. It should be possible to detect unauthorized access.

10.3. Qualification of the Computer Forensic Operators

The literature is plenty of references and maps related to how much an individual should be technically skilled to perform digital investigations and computer forensics in particular.

The first thing that government and judiciary offices should do is splitting the public and the private sector. While the second has wide discretion about how to choose their consultants, the public sector (including the police and the judiciary offices) should follow exact criteria to avoid too many challenges in court.

One of the most successful case studies in this field is given by the English project called *skills for justice.* According to their literature, to meet the standard, an operator needs to

know and understand the following:

Legal and organizational requirements

1. relevant legislation, policies, procedures, codes of practice and guidelines for investigating electronic evidence;
2. relevant legislation and organizational requirements in relation to race, diversity and human rights;
3. relevant legislation and organizational requirements in relation to health and safety;
4. situations and circumstances for which authority is required and how to obtain the authority;
5. how to carry out risk assessments and why these are required;
6. the limits of your responsibility and level of competence;

Investigating electronic evidence

7. how to investigate electronic evidence;
8. the scientific principles underpinning the investigation of electronic evidence;
9. the need to establish the scope of the investigation;
10. the parameters and objectives for these types of investigations;
11. the constraints for these types of investigations;
12. the types of equipment available for investigating electronic evidence;
13. how to use equipment for investigating electronic evidence;
14. the meaning of evidentially sound forensic tools and techniques and how these are applied;
15. how to conduct a cross tool validation of results and the reasons why this is necessary;
16. the strengths and weaknesses of different tools for investigating electronic evidence;
17. the third parties with whom you may need to consult;
18. how to consult with third parties to obtain additional information;
19. how to carry out research activities to obtain additional information;
20. how to create a working product including subsets of the data, and interim reports;
21. how to document the electronic evidence investigation;

22. the reasons why it is important to document the investigation;
23. the types of problems which may occur and how they can be resolved;
24. how to conduct an oral presentation of findings.

While this project is good to interpret the need for skills, it is less indicative about what kind of education a computer forensic operator should have. The common practice suggests the following:

1) At least an academic diploma (the equivalent of an associate degree) in computer science or similar. This should give the operator a minimum skill on computers and systems/networks that he/she is going to investigate.
2) A consequential certification in the field of operation. The so called "certification dilemma" is really important to know. The best practices suggest training people to be certified in the field, regardless the vendor of the technology used to investigate. Common practices suggest also following up with a second certification related to the technology itself.
3) Having a certification which is worldwide recognized is absolutely a must. Of course, local training can be taken, on an annual basis.

It is also suggested to have a computer forensic lab, structured in a scientific way. Every lab should be equipped with the latest technologies and have several experts working. Each one of them should be specialized in some vertical field (e.g. Mobile Phone, Log analysis, etc).

10.4. Budgeting and Technicalities

The computer forensic field is growing and includes several different sub fields. In terms of investment, the investments are not low and must be done with gradual commitment. In particular, while there are several magistrates who prefer to rent the equipment, the best practices suggest buying them. The criteria that are usually followed are:

1) field of operation. If a lab is an entry level one (for example for child pornography investigation and small/mid size cases) we suggest starting with a commitment in

forensic hardware and an exploration of the open source forensic field. The Open Source Digital Forensics field is a reference for the use of open source software in digital investigations (a.k.a. digital forensics, computer forensics, incident response). Open source tools are free and may have a legal benefit over closed source tools (proprietary and commercial) because they have a documented procedure and allow the investigator to verify that a tool does what it claims. While is important to say that both closed and open source tools are widely recognized in court, the open source forensics is an important emerging field. The number of people involved in this field is growing, both for budget and court recognition reasons. The PTK is a new project born at IRItaly (http://ptk.dflabs.com) and it has been released at the end of March 2008. The number of download of this software, which allows effective and concurrent digital investigations a very low cost, is reaching the 10 000 units worldwide. PTK is in English but can be localized in several languages.

2) Number and complexity of managed cases. If the number of cases managed annually overcome the 200, it is better to organize the investment in a more complete way. To do that, a preliminary study shall be conducted, in order to quality the type of laboratories and technology that can be employed. As a general rule, it is better to avoid technology that has not been used before by the rest of the community. This will avoid negative challenges in court.

10.5. The Future

We do agree with the ISACA that recently published a position paper about the future of this discipline. The science of computer forensics has a seemingly limitless future, and as technology advances, the field will continue to expand. Such evidence has to be handled in the appropriate manner and must be documented for use in a court of law. Any methodology, process or procedural breakdown in the application of forensics can jeopardize the cases.

Organizations – both governments and private sector - are beginning to rely on the findings that computer forensics specialists gather when a cybercrime is committed. Computer forensics quickly is becoming standard protocol in corporate and judiciary investigations by expanding beyond the realm of specialized, computer incident response teams and police investigative squads. As the overwhelming majority of documents are now stored electronically, it is difficult to imagine any type of investigation that does not warrant a computer forensic investigation. Thus, computer forensics It is becoming a standard for electronic crime investigations. However, while the corporate world will use it "only" for managing security incidents, the judiciary offices will need it for a wide range of crimes, from the child pornography, to fraud, to terrorism and organized crime.

Computer forensics is not only used for cybercrime cases, but the techniques and methods are also adopted for non-investigative purposes. Examples include data mapping for security and privacy risk assessment, and the search for intellectual property for data protection.

Computer forensics is transitioning from an investigation and response mechanism to one of prevention, compliance and assurance. By utilizing computer forensics techniques, companies can better protect themselves against potential threats from hackers and angry employees. Additionally, computer forensics schemes can be used when critical files have been deleted accidentally or through hardware failure. Thus, there are several additional applications pertaining to the science of computer forensics in addition to utilizing the methods to investigate computer-related crimes.

III. CONCLUSIONS AND RECOMMENDATIONS

1. General Directions of the Reform

1.1. Methodology

The Internet's rate of development is so fast that it is impossible all arising challenges related to it to be resolved by creating one specific legislative act. It is of great importance for the origination of the national legislative framework to be provided enough technologically-neutral flexibility, in order for an optimum balance between the interests of the copyright owners (in the intellectual property legislation), the interests of the society in general (in the intellectual property legislation and in that on cybercrime), and the interests of the Internet users.

1.2. Technologically-Neutral Language

The fast changes in the technology area will soon make each technologically-specialized language old in a specific moment. Although the new technologies are the reason for the creation of the Internet Agreements by the World Intellectual Property Organization (WIPO) in 1996, in the Preambles of the Agreements, when generalizing the statements discussed in the Agreements, the technological aspect is stated barely at fourth place after the 'economic, social and cultural' aspects. According the explanations of Michael Ficsor, one of the Agreement's creators, the choice is not accidental. The purpose is to put an emphasis on the fact that the focus of the reform should not be of technological nature. The clauses 'should not be technologically specified, but more abstract in order to cover the economical, social and cultural issues raised by the technologies'.[203]

1.3. Classification of the Aspects

The legislative problems that appeared in relation with Internet are numerous but their analysis and their placement in different classifications may facilitate the establishment of

[203] Mihaly Ficsor, The Law of Copyright and the Internet, Oxford University Press, 2002, p. 413.

adequate legislative answer. The following modified classification done by Professor Trothar Hardy in 1998 in his research can be useful:

a) new issues on the subject;

b) new usage; and

c) decentralized legislative offences.[204]

1.4. The Price of the Transition

Each legislative reform requires resources of time, money and experts. Knowledgeable and well-educated people are needed to render the legislative standards. Integrity and efficiency among the legislators is indispensable, as well as will by the institutions for a change in their daily way of work. Before making a decision for taking the way of the change, it is important to assess the consequences of its implementation or not implementation. Frederic Shower refers that 'some of the transitions in the legislation, which under other circumstances might be optimal, have to be excluded or to be to delayed to the most in favour of the sustainability, stability and peace.[205] In the case of such decentralized and self-regulated media as Internet, the legislative transitions are most useful when other more economical methods cannot solve the arising issues and there is general consensus among the concerned parties on how to develop it further. Otherwise, it is safer the legislation to be left unchanged, and the lapses to be corrected by means of agreements and interpretation of the legislation norms.

If we take into consideration the fact that the legislative processes correspond to the assigned tasks, the 'interpretation' method can turn out to be more economical than an overall legislative reform. This has to be taken into consideration before starting the elaboration of a radically new legislative act.

2. EXECUTION

[204] Project striving for description of copiright in the online world, May 1998, Final Report by I. Trother Hardy, http://www.copyright.gov/reports/thardy.pdf.

[205] Frederick Schauer, Legal Transitions: Is There an Ideal Way to Deal with the Non-Ideal World of Legal Change?: Legal Development and the Problem of Systemic Transition, 13 J. Contemp. Legal Issues 261, 265 (2003).

No matter how good the substantive law standards are, they are useless if their application in practice is not secured. Not only well prepared legislative standards on Intellectual Property and Criminal Law are needed, but also an adequate and coordinated procedural framework allowing the users to successfully defend their rights and interests, as well as independent legislative institutions and organizations dealing with the popularization, explanation and observation of the regulations.

2.1. Execution through Legislative Measures

Article 14 (Securing the execution of legal rights) of the Copyright Agreement of WIPO of 1996 explicitly requires the parties under the Agreement to 'ensure free implementation of the procedures in compliance with their internal legislation, so that successful actions could be undertaken against all violations of rights protected by the Agreement, including fast compensation of losses which can stop further violations'. This obligation also reflects the requirements of the TRIPS Agreement (Art.14).

In April 2004, EU adopts a separate Directive on the application of intellectual property rights. In Art.1 of the Directive, it is emphasized that the measures, the procedures and the necessary resources, required to secure the execution of those rights have to be fair and proportionate, without any unduly complications and rises of costs, also proportional and justified.[206] The Directive demands that the access to the exact measures have to be secured for all interested persons, including:

a) copyright holder;

b) all authorized persons and more specifically the licence holders;

c) organizations for collective copyright management; and

d) professional protective organizations, that can represent the holders of intellectual property rights.[207]

---

[206] Directive of the European Parliament and of the Council in connection with the Intellectual Property Enforcement (IP Enforcement Directive) 2004/48/EO of 29th of April 2004: http://europa.eu.int/eur-lex/pri/en/oj/dat/2004/l_195/l_19520040602en00160025.pdf.

[207] See again in Art.4

For the purposes of simplifying the access to similar protective measures, copyright presumption[208] is provided in the Directive. With a view of the possible substantive law measures of protection, the following instruments for their application are provided:

- Judicial prescripts;[209]
- Judicial compensations;[210] and
- Allocation of judicial expenses.[211]

2.2. Execution through Procedural Measures

The record companies in the United States are carrying out a vigilant procedural campaign. It has proved the benefits of the execution of these measures. After the Record Industry American Association (RIAA) initiated in 2003 a few hundred procedures against file swappers, their number in KaZaa decreased to 4.3 million in August compared to 6.2 million in May, according a web flow survey conducted by Nielsen/NetRatings.[212]

According another market research company, NPD Group, by the end of August, 30% less songs have been downloaded from the Internet, compared their number in the spring. Forrester Research studied the opinion of people between 10 and 22 years, by asking them if they will stop downloading illegal copies of works protected by copyright, if there is serious risk of imprisonment or a fine, and 68% of the interviewed people answered 'yes'.

2.3. Execution through Cultural Changes

In order to lead effective struggle against the offences of the law online, as well as anywhere else, it becomes necessary to stipulate both penalties and stimulations. The European Directive on copyright emphasizes on preventive methods, such as codes of

[208] See again in Art.5

[209] See again in Art.11.
[210] See again in Art.12 and 13.
[211] See again in Art.14.
[212] See Jefferson Graham et al., Hammering Away at Privacy, USA Today (Sept. 11, 2003), at D1.

conducts, developed by professional associations[213] and providing great publicity of judicial court's decisions concerning copyright cases.[214]

It is of great importance to initiate efficient campaigns in order to clarify to the common Internet users why copyright protection is important for them as well. It could be useful some researches to be done that estimate the economical and social impact on similar encroachments on persons outside the concerned industry. The growing relation between the piracy in copyright and the organized crime should be also clarified.

This relation is natural if we take into consideration the fact that the risks for piracy in this field are vastly lower than the ones related to drug dealing and the profits are proportionally higher. While with the amount of $47 000 we can buy one kilogram of cocaine, which can be sold with 100% profit, with the same amount we can buy 1500 pirate copies of Microsoft Office and the generated profit will be 900%.[215]

As a whole, many measures can be applied starting from commercials to essay competitions on this topic, which can convince the community to demand an adequate system for intellectual property protection, instead of neglecting it. Last but not least, the producers in this field have to propose alternatives: easily accessed and legal resources for downloading materials at a reasonable price.

IV. BIBLIOGRAPHY

Cybercrime in Romania

[213] See IP Enforcement Directive, Art. 17.

[214] See again in Art. 15.

[215] *See* Jennifer L. Schenker, Busting Software Pirates, Time (Nov. 18, 2002), at 54.

- Crimes stipulated by special laws (includes cybercrimes)/ Mihai Adrian Hotca, Maxim Dobrinoiu, 2008
- Legal Informatics and IT Law, Ioana Vasiu, 2007
- 10 legal pieces of advice on electronic commerce /Bogdan Manolea 2007
- A few aspects on the acceess without right to a computer system infringement /Bogdan Manolea, 2007
- Crimes related to IT / Maxim Dobrinoiu, 2006
- Legal issues related to child abuse on the Internet - *dr.Horatiu Dumitru* - August - October 2006 – published in "Pandectele Romane" magazine no. 2/2006 si 4/2006
- Cybercrime prevention / Ioana Vasiu, Lucian Vasiu, 2006
- Criminal regulation and investigation of the crimes in IT domain - dr. Gheorghe Alecu , dr. Alexei Barbaneagra, 2006
- Introduction guide for the application of the legal provisions on cybercrime, RITI dot-Gov, 2004
- Use of the computer and electronic services: guide for public officers , RITI dot-Gov , 2004
- Cybercriminality / Tudor Amza, Cosmin Petronel Amza, 2003
- Legal issues on negative content on the Internet - *Dr. Horatiu Dan Dumitru* - (Article issued in "Pandectele Romane" No.3/2003, 4/2003, 5/2003, 6 /2003 and 1/2004)

Fraud Online

Council of Europe, (2001) *Convention on Cybercrime* (ETS 185)
http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm

De Hert, P. González Fuster, G. & Koops, B-J. (2006) Fighting Cybercrime in the Two Europes: The added value of the EU Framework Decision and the Council of Europe Convention, *Revue Internationale de droit pénal* 77(3-4): 503-524.
http://www.vub.ac.be/LSTS/pub/Dehert/260.pdf

European Union, Safer Internet *plus* programmeme
http://ec.europa.eu/information_society/activities/sip/index_en.htm

European Union, (2001) *Council Recommendation on Contact Points Maintaining a 24-Hour Service for Combating High-Tech Crime* (OJ 2001/C 187/02: 5–6.)
<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2001:187:0005:0006:EN:PDF>

--, (2004) *Regulation 2006/2004/EC on cooperation between national authorities responsible for the enforcement of consumer protection law* (OJ 2004 L 364/1-11).
<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:364:0001:0011:EN:PDF>
--, (2005) *Council Framework Decision 2005/222/JHA on attacks against information systems* (OJ 2005 L 69/67-71)
http://eur-lex.europa.eu/LexUriServ/site/en/oj/2005/l_069/l_06920050316en00670071.pdf

International Consumer Protection and Enforcement Network (ICPEN)
http://www.icpen.org/operation.htm

OECD – Consumer Policy Committee
http://www.oecd.org/department/0,2688,en_2649_34267_1_1_1_1_1,00.html

OECD, (1999) *Guidelines for Consumer Protection in the context of Electronic Commerce*
<http://www.oecd.org/dataoecd/18/13/34023235.pdf>
--, (2003) *Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices across Borders*
<http://www.oecd.org/dataoecd/24/33/2956464.pdf>
--, (2006) *Report on the Implementation of the 2003 OECD Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices across Borders*
<http://www.oecd.org/dataoecd/45/53/37125909.pdf>

Savirimuthu, J. (2008) Identity Theft and the Gullible Computer User: What Sun Tzu in The Art of War Might Teach, *Journal of International Commercial Law and Technology* 3(2): 120-128.
http://www.jiclt.com/index.php/JICLT/article/view/65/51

Smith, R. G. & Urbas G. (2001) Controlling Fraud on the Internet: A CAPA Perspective, Australian Institute of Criminology Research and Public Policy Series No. 39.
http://www.aic.gov.au/publications/rpp/39/RPP39.pdf

Smith, R.G. (2008) Coordinating individual and organizational responses to fraud, *Crime, Law and Social Change* (2008) 49(5): 379–396.

Tally G. Thomas, R. & Van Vleck, T. (2004) *Anti-Phishing: Best Practices for Institutions and Consumers*, McAfee Research, Technical Report # 04-004
http://www.antiphishing.org/sponsors_technical_papers/Anti-Phishing_Best_Practices_for_Institutions_Consumer0904.pdf

United Nations, (1994) *Manual on the Prevention and Control of Computer-Related Crime*
http://www.uncjin.org/Documents/irpc4344.pdf
--, (2001) General Assembly Resolution: *Combating the criminal misuse of information technologies* (A/55/593)
http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf

Wilson, G. & Wilson S. (2007) Can the General Fraud Offence 'Get the Law Right'? Some Perspectives on the 'Problem' of Financial Crime, *Journal of Criminal Law* 71(1): 36-52.

Pornography Online

Casavant, L. & Robertson, J.R. (2007) *The Evolution of Pornography Law in Canada*, Parliamentary Information and Research Service, Canada.
http://www.parl.gc.ca/information/library/PRBpubs/843-e.htm

Clayton, R (2005) *Anonymity and traceability in cyberspace*, Technical Report No. 653, University of Cambridge Computer Laboratory
http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-653.pdf

Council of Europe, (2001) *Convention on Cybercrime* (CETS 185)
<http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm>
--, (2007) *Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse* (CETS 201)
http://conventions.coe.int/Treaty/EN/treaties/Html/201.htm

Department for Children, Schools and Families (UK) (2008) *Byron Review – Children and New Technology - Executive Summary*
<http://www.dcsf.gov.uk/byronreview/pdfs/Executive%20summary.pdf>
--, (2008) *Report of the Byron Review– Safer Children in a Digital World*
<http://www.dcsf.gov.uk/byronreview/pdfs/Final%20Report%20Bookmarked.pdf>
European Union, Safer Internet *plus* programmeme
<http://ec.europa.eu/information_society/activities/sip/index_en.htm>
---, (1996) Commission Communication on Illegal and Harmful Content on the Internet. (COM (96) 487 final)
<http://aei.pitt.edu/5895/01/001527_1.pdf>
--, (1998) *Council Recommendation on the development of the competitiveness of the European audiovisual and information services industry by promoting national frameworks aimed at achieving a comparable and effective level of protection of minors and human dignity* (98/560/EC)
<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1998:270:0048:0055:EN:PDF>
--, (1999)*Council Decision adopting a multiannual Community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks* (276/1999/EC)
<https://www.inhope.org/system/files/siap-extension.pdf>
--, (2000) *Council Decision to combat child pornography on the Internet* (2000/375/JHA)
<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:138:0001:0004:EN:PDF>
--, (2004) *Council Framework Decision on combating the sexual exploitation of children and child pornography*. (2004/68/JHA)
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:013:0044:0048:EN:PDF

--, (2005) *Decision of the Parliament and of the Council establishing a multiannual Community Programmeme on promoting safer use of the Internet and new online technologies* (854/2005/EC) http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:149:0001:0013:EN:PDF
--, (2007) *Commission Report based on Article 12 of the Council Framework Decision of 22 December 2003 on combating the sexual exploitation of children and child pornography* (COM(2007) 716 final) http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0716:FIN:EN:PDF
ILO, (1999) *Convention Concerning the Prohibition and Immediate Action for the Elimination of the Worst Forms of Child Labour*
http://www.ilo.int/public/english/standards/relm/ilc/ilc87/com-chic.htm

International Association of Internet Hotlines (INHOPE)
https://www.inhope.org/

Internet Watch Foundation (IWF)
http://www.iwf.org.uk/

Johnson, M. (2008) Camera Obscura - The Criminal Justice and Immigration Act 2008 and Virtual Pornography, *Justice of the Peace* 172 (29): 460-462.

Joyce, R.A. (2008) Pornography and the Internet, *IEEE Internet Computing* 12(4): 74-77.
Krause, J. (2008) The End of the Net Porn Wars, *American Bar Association Journal* 94(Feb): 52-57.
http://abajournal.com/magazine/the_end_of_the_net_porn_wars/

Krone, T. (2004) A Typology of Online Child Pornography Offending, *Trends & Issues in Crime and Criminal Justice*, No. 279
http://www.aic.gov.au/publications/tandi2/tandi279.pdf

Livingstone, S. & Bober, M. (2004) *UK Children Go Online: Surveying the experiences of young people and their parents*, Research Report, London School of Economics and Political Science
http://www.york.ac.uk/res/e-society/projects/1/UKCGOsurveyreport.pdf

McCabe, K.A. (2008) The Role of Internet Service Providers in Cases of Child Pornography and Child Prostitution, *Social Science Computer Review* 26(2): 247-251.

McGlynn, C. & Rackley, E. (2007) Striking a Balance: Arguments for the Criminal Regulation of Extreme Pornography, *Criminal Law Review*: 677-690

UN, (2000) Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography
http://www.iin.oea.org/iin/English/observatorio/documentos/Optional%20Protocol%20to%20the%20Convention.pdf

Wolak, J. Finkelhor, D. & Mitchell, K. J. (2005) *Child-Pornography Possessors Arrested in Internet-Related Crimes: Findings from the National Juvenile Online Victimization Study*, National Center for Missing & Exploited Children
<http://www.missingkids.com/en_US/publications/NC144.pdf>

Money Laundering Online

Carroll, L. (2004) *Alternative Remittance Systems: Distinguishing Sub-Systems of Ethnic Money Laundering in Interpol Member Countries on the Asian Continent,* Lyon: Interpol General Secretariat.
http://www.interpol.int/Public/FinancialCrime/MoneyLaundering/EthnicMoney/default.asp

Council of Europe, (1990) *Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime* (ETS 141).
<http://conventions.coe.int/Treaty/en/Treaties/Html/141.htm>
--, (2005) *Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism*
http://conventions.coe.int/Treaty/EN/Treaties/Html/198.htm

European Union, (2005) Directive 2005/60/EC on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing.
<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:309:0015:0036:EN:PDF>
FATF, (2004) *The Forty Recommendations*, October 2004.
<http://www.fatf-gafi.org/dataoecd/7/40/34849567.PDF>
--, (2004) *Special Recommendations on Terrorist Financing*, October 2004
http://www.fatf-gafi.org/dataoecd/8/17/34849466.pdf
--, (2006) *Report on New Payment Methods*, October 2006.
<http://www.fatf-gafi.org/dataoecd/30/47/37627240.pdf>
--, (2007) *AML/CFT Evaluations and Assessments Handbook for Countries and Assessors*, June2007
<http://www.fatf-gafi.org/dataoecd/7/42/38896285.pdf>
--, (2008) *Money Laundering & Terrorist Financing Vulnerabilities of Commercial Websites & Internet Payment Systems*, June 2008.
http://www.fatf-gafi.org/dataoecd/57/21/40997818.pdf

Jost, P.M. & Sandhu, H. S. (2000) *The hawala alternative remittance system and its role in money laundering*, Lyon: Interpol General Secretariat.
http://www.treas.gov/offices/enforcement/key-issues/hawala/FinCEN-Hawala-rpt.pdf

MONEYVAL, (2008) *Third Round Detailed Assessment Report on Bulgaria - Summary*, 3 April 2008
<http://www.coe.int/t/dghl/monitoring/moneyval/Evaluations/round3/MONEYVAL(2008)02Summ-BUL3_en.pdf>
--, (2008) *Third Round Detailed Assessment Report on Romania - Summary*, 11 July 2008

http://www.coe.int/t/dghl/monitoring/moneyval/Evaluations/round3/MONEYVAL(2008)06Summ-ROM3_en.pdf

National Drug Intelligence Center, (2008) *Money Laundering in Digital Currencies*, Product No. 2008-R0709-003, U.S. Department of Justice June 2008
http://www.usdoj.gov/ndic/pubs28/28675/28675p.pdf

Reuter, P. & Truman, E. M. (2004) *Chasing Dirty Money: The Fight against Money Laundering*. Washington, DC: Institute for International Economics.
http://bookstore.petersoninstitute.org/book-store/381.html

Cyber Terrorism

Forte, Dario: Assembling an Incident Response team in a Small to Medium Organization - Computer Fraud and Security - Feb 2004 Issue

Forte, Dario : Principles of Digital Evidence Collection, Publication: Network Security December 2003 issue

Cyberterrorism: Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives by Dorothy E. Denning, Georgetown University May 23, 2000
Gabriel Weimann: Cyberterrorism: How Real Is the Threat? December 2004 | Special Report No. 119. The United States Institute of Peace, available on line:
http://www.usip.org/pubs/specialreports/sr119.html

Richard Power and Dario Forte: War & Peace in Cyberspace Stalking "cyber terrorists" in Sofia – event report, Computer Fraud & Security .Volume 2006, Issue 11, November 2006, Pages 4-8

Computer Forensics

Armstrong, Illena. "Windows vs. Linux: Taking Security Seriously." 2001.
http://www.securityfocus.com/library/3446 (2 November 2001).

Computer Forensics: An Overview By Frederick Gallegos, CISA, CDE, CGFM Volume 6, 2005, the ISACA control journal.

Farmer, Dan and Venema, Wietse. "Forensic Computer Analysis: An Introduction." Dr. Dobb's
Journal. September, 2000.
http://www.ddj.com/documents/s=881/ddj0009f/0009f.htm (1 November 2001).

Grace, Scott. "Computer Incident Response and Computer Forensics Overview." March 2001.

http://www.sans.org/infosecFAQ/incident/IRCF.htm

Kruse, Warren G. and Jay G. Heiser. Computer Forensics: incident response essentials. Indianapolis: Addison-Wesley, 2002.

Mandia, Kevin and Chris Prosise. Incident Response: Investigating Computer Crime. Berkeley:
McGraw-Hill, 2001.

McMillian, Jim. "Importance of a Standard Methodology in Computer Forensics." May 2000.
http://www.sans.org/infosecFAQ/incident/methodology.htm

Romig, Steve. "Forensic Computer Investigations." October 2001.
http://www.net.ohio-state.edu/security/talks/2001-10_forensic-computer-investigations/6up-pdf/
(2 November 2001)

Challenges in Forensic Computing Rebecca T. Mercuri Communications of the ACM, Volume 48, Number 12 (2005), Pages 17-21
Scambray, Joel, Stuart McClure, and George Kurtz. Hacking Exposed: Network Security Secrets and Solutions. Berkeley: Osborne/McGraw-Hill, 2001.