EUROPEAN ACADEMIC RESEARCH
Vol. II, Issue 1/ April 2014

Impact Factor: 3.1 (UIF)
DRJI Value: 5.9 (B+)

ISSN 2286-4822
www.euacademic.org

Cybercrime in Albania: A Discourse on Law, Policy and Practice

BLEDAR ABDURRAHMANI
"Aleksandër Moisiu" University, Durrës
Albania

Abstract:

With the emergence of new technologies and innovations the individuals, businesses and governments world-wide are also facing an alarming growth in cybercrime. Albania is no exception to the paradigm of cybercrime. In recent times there has been a rapid growth in various forms of Information Communication Technology (ICT), particularly internet users. What is the definition of cybercrime? "Cybercrime is any criminal activity which involves a computer or network as the source, tool, target or place of a crime" (Grabosky 2001, 38). In recent years there has been a considerate focus by all the government structures to improve the computer-related crime legislation and means of resources and mechanisms to combat it. On the basis of the "desk research", taking into consideration the main legal documents in this field and various authors' doctrinal positions in Albanian and European level, this paper will examine the phenomena of cybercrime in Albania and the current enacted relevant legislation to prevent and combat computer crimes.

To have a full treatment as to the extent of this phenomenon in our country there have been conducted meetings and interviews with focus groups, such as experts of the State Police and the Prosecutor General. This paper based on the official data will try to find out the most common types of cybercrime activities in Albania, reasons and motives behind the development of these crimes, and regulatory measures taken by the Albanian authorities to curb these phenomena. In addition, this paper will focus on the characteristics and defense mechanisms that the computer crime laws have foreseen to protect

against these offences.

Key words: cybercrime, Albania, law, policy, practice.

1. THE PHENOMENON OF CYBERCRIME.

Computer, Internet and electronic communication increasingly occupy an important place in everyday life. Using the Internet at home, work or in other settings indicate that individuals need to be informed and also to communicate in real time. Electronic communication is already an important instrument of free expression, a fundamental right guaranteed in any democratic society. Computer is widely used for storage and processing of confidential data in various aspects of social, political, economic or even in the sphere of personal life. People, businesses and governments, widely use information and communication technology to achieve their goals and objectives. The use of this technology provides them with great advantages, setting new standards in speed, efficiency and security of the communication, as key elements to stimulating innovation, invention, creativity and above all productivity. The use of computer networks and systems for carrying out banking transactions for personal or business purposes, e-government and many other aspects are the most important achievements of a new era, the digital one. On the other hand, large-scale use of mobile devices or other electronic communication devices via the Internet is an important indicator of new technological standards. All these technological changes have enabled replacement of transactions and actions previously committed through acts and paper documents with electronic communication.

The spread of the Internet and the development of information technology have created new opportunities for people who are involved in criminal activity. The rapid technological development and communication system "online"

has led to the display of a range of criminal activities that seriously affect social relationships. These activities have as an object not only equipment and computer systems, affecting the confidentiality, integrity and availability of computer data and systems, but, through computer technology, they violate the constitutional order, life, health, morals, dignity, property of the person or of the state. These illegal activities are known as the cybercrime phenomenon. Cybercrime is the newest form of criminal activity and is seen as a byproduct of technological revolution which has involved the entire society in the last decade. This phenomenon has led the society to facing the challenge of building a better defensive scheme to guarantee the life, health, morals, dignity of the person, his property, public order and security, domestic stability and socio-economic development from a range of illegal actions or behavior (Wall 2007, 64).

Therefore, it has been and remains essential that the phenomenon of cybercrime be addressed in a comprehensive manner, through a special legal framework that clearly defines specific types of cybercrime and regulates in detail the procedural aspects such as jurisdiction and international cooperation.

To respond to this phenomenon with global social consequences, the Council of Europe adopted on 23 November 2001, in Budapest, the Convention on Cyber Crime. This Convention, which entered into force on 1 July 2004, is the first international legal basic document, which addressed the phenomenon of cybercrime. This document has attempted to provide solutions to this phenomenon, providing a range of recorded crime types over time, such as the unauthorized computer access, illegal computer espionage, computer data and systems interference, infringement of copyright and other rights related to computer fraud and forgery, distribution of child pornographic materials etc (CoE 2001, 3-6).

One of the main purposes of this document, expressed in

its preamble as well is the need to follow in order of priority a common penal policy, aimed at the protection of society against cybercrime, inter alia, adopting appropriate legislation and fostering international cooperation (CoE 2001, Preamble).

Therefore, harmonization of national laws, improvement of investigative techniques and increase of the level of cooperation between nations has been another objective of this document.

The Cyber Crime Convention, in Article 1, gives the definition of some basic concepts of this field[1]. Given that some crime types have as their target computer system or data, it is necessary to explain their meaning in detail. The computer system includes any device or group interconnected or related devices, one or more of which, follow-up of a program, perform automatic processing of data (CoE 2001, 2). The term computer system means a device used for the automatic processing of data. These devices include both "hardware" and "software" or any other device used for receiving, delivering or storing data. In the above definition, the word "automatic data processing" means that the data in a computer system are processed through a certain software program without physical human intervention. According to the definition given by the Convention, computer data means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable for the performance of a computer system to perform a function (CoE 2001, 2). This definition is similar to the one given by the International Organization for Standardization (ISO) for the term "data".

Meanwhile, computer data means that the data must be electronic or in some other directly processable form. Therefore, computer data may be stored in a computer system, as well as

[1] Legislations of some countries provide definition of concepts such as “computer data” or “computer system” in the Penal Code or in the specific law, see Bulgaria.

outside the system, e.g. a magnetic or optical disk, smart card, chip, etc.

The Convention treats Cybercrime in terms of its material aspect as divided into four main directions. In articles 2-6 it addresses specific types related to computer crime. Cybercrime is focused on computer "hardware" and electronic information or data contained within it, such as "software" and personal data. Therefore, cybercrime has as its effect violating the integrity and reliability of the information technology infrastructure of a computer or computer network and security of operations or transactions carried out through them. Criminal activity is mainly related to the function that the computer performs, especially when included in the global communications network. These illegal activities are directed against the rights and interests related to the proper functioning of the computer or computer system. The Articles 7 and 8 of the Convention deal with the *computer-related forgery and fraud*. Computer related forgery and fraud is a totality of illegal actions carried out through the use of computer, as opposed to computer crime which refers to actions that have the computer as an object. The difference lies in the fact that the computer and computer equipment are presented as means to enable or simplify the performance of traditional crimes. This includes such crime types as: computer fraud and computer forgery. Moreover, the Convention in Article 9 and 10 deals respectively with offenses related to content or child pornography and offenses related to the infringements of copyright and related rights (CoE 2001, 3-8).

In 2003, the Council of Europe member states and other countries having signed the Convention, considering that computer systems can be used to perform illegal actions which seriously violate fundamental rights as the right to life, health, morals and dignity, decided the adoption of an additional protocol. The Additional Protocol to the Convention was signed on 28.01.2003 in Strasbourg and specifically provides for

regulation of some specific crime types, as the commission of acts and actions which constitute a crime against humanity or genocide, or other actions of racist and xenophobic nature committed through computer systems and that target the violation of life, morality and dignity of the individual (Additional Protocol 2003, 2).

On March 1, 2006 the Additional Protocol to the Convention on Cybercrime came into force. Albania is one of the first countries to have signed the Convention and ratified it after a few months by law no.8888, dated 25.04.2002 "On ratification of the Convention on Cybercrime". So far, the Convention has been signed by 46 countries around the world, and it has been ratified and implemented in 30 of them.

2. UNDERSTANDING CYBERCRIME

The term cybercrime is seen as a concept that includes a number of illegal activities that have in common the role played by networks of information and communication technology in its performance. Numerous authors have expressed different views about cybercrime. Thomas and Loader (2003, 3) perceive cybercrime as the totality of those activities performed on devices or computer systems or computer mediated through the use of global electronic networks and which are considered illegal by the criminal law of a state. The uniqueness of cybercrime is that it was born and evolved as a result of technological developments in a broad interactive environment called "virtual space" generated by computer link with extensive international network of exchange of information (Castells 2002, 177). The main problem in the analysis of cybercrime continues to be the lack of a precise and adequate definition in both domestic and international criminal legislation, leaving it in the hands of criminal law doctrine. Not having a legal definition, this institution remains a notion that is broadly treated by the jurisprudence, politics, media and the

public.

What is cybercrime? Cybercrime is a term that is used to refer to a broad range of illegal activities relating with the misuse of computer data, computer systems and computer network and carried out by the entity for the purposes of personal or property interests. More comprehensive definition was given by Wall, who by cybercrime means illegal activities carried out in a deliberate way, through unauthorized access to a computer or computer system in order to change, delete, remove, intercept, copy or destroy the database of a computer or computer system. It also consists in unauthorized access to a database or computer program aiming at the implementation of an action plan for assuming control of illegal data or software and/or using them in order to obtain wealth. (Wall 2004, 43).

The cybercrime notion includes computer crimes, as well as any other form of criminal activity related to the use of a computer, computer system or global communication network for illegal purposes.

Most authors, for study purposes, categorize cybercrime based on treatment that the Convention makes to specific types of cybercrime. Therefore, the criterion used for this type of classification is the fact whether the computer is the target of the crime or is a tool that serves to perform it. *Computer crimes* are new forms of criminal activity. They have as their object a computer device, the data that it contains, or its proper operation, as an instrument that processes or stores data. The lawmaker's aim to specifically regulate computer crimes is protection from illegal actions of entities that own or use computers or computer systems, ensuring their normal functioning in accordance with the purpose for which they were created or used. Therefore, in the case of computer crimes, the target of criminal actions is the computer itself or the computer system. Computer crimes refer to illegal activity that is focused on computer hardware and electronic data it contains, such as software and personal data. Computer crimes are intended to

damage the integrity and credibility of the information technology infrastructure, i.e. the computer and electronic communication systems and security of the operations carried out by them. Given its nature, cybercrime is a new phenomenon generally. It has to do with a totality of illegal actions based on specialized knowledge in the field of information technology.

Computer-related crimes involve a set of criminal actions carried out with the help of the computer. Most authors agree that computer-related crimes are nothing else but an ordinary crime carried out with the help of a new technology. These authors refer to a series of images of crime, such as fraud, forgery, insults, threats, etc. Moreover, they were of the opinion that the substantive law did not need changes to address and punish the phenomenon specifically. In computer-related crimes, "computer and computer systems, specialized equipment information and communication technology are used to commit traditional crimes." (UN Manual, 42). Information Technology in these types of offenses serves as an alternative tool in the implementation of criminal intent. These crime types are presented as a separate category of crime in general, with the only difference that these actions are based on the use of computers, computer systems or networks and the use of electronic technology equipment, as instruments that enable or facilitate the commission of traditional offenses (Furnell 2002, 22).

2.1. Cybercrime: a global phenomenon.

The global communication network enables citizens to enter the electronic systems of the businesses, government bodies of different countries, regardless of their country of origin. This means that criminal activity and potential victims of cybercrime may be located geographically in different countries. It is now clear that cybercrime has an international character and thus interstate coordination in terms of drafting and enforcement of legislation is necessary to guarantee that the

substantive and procedural law is able to cope with the new challenges established by the spread of cybercrime. Cybercrime is not a phenomenon that needs to be addressed only at the national level, but it is a global phenomenon. As in the case of pollution or global warming, a state legislator cannot operate to predict a more suitable arrangement for these phenomena without international cooperation in this field. This would allow a unique international protection against this dangerous phenomenon. While international organizations such as OECD and G-8 have raised the urgent necessity of drafting common schemes of cooperation and coordination in the fight against computer crime, certain states are not involved in these initiatives, arguing that they have more important issues to address. In fact, this problem is a global concern, because the authors of works may be protected by a lack of jurisdiction.

European Parliament and the Council of Europe have undertaken some important initiatives to combat the phenomenon of cybercrime. In this context, we mention the Council Framework Decision 2005/222/JHA of 24 January 2005 "On Attacks Against Information Systems", which highlights the risk of the spread of some specific forms of criminal activity directed against information systems such as electronic piracy , viruses and other attacks against computer systems. In this framework decision there is a need of strengthening international cooperation for the prevention and elimination of these criminal activities through improvement of infrastructure of networks and information systems and technological equipment of law enforcement bodies charged with combating these activities. This document addresses the necessity of the approximation and harmonization of legislation in this field and deepening the cooperation among judicial authorities (CoE 2005/222/JHA).

Another important document is directive no.2011/92/EU, 13 December 2011 "*On combating the Sexual Exploitation of Children Online and Child Pornography*." Through this

directive is proposed the regulation of a number of emerging phenomena related to sexual exploitation and abuse of minors through the use of the Internet, actions consisting of proposals, harassment, shows in front of web cameras of minors with pornography[2] purposes, etc. Along with these new regulations in this directive is proposed stricter sentencing policy, which would serve full harmonization of legislation between Member States. Article 21 of this Directive proposes measures to block the "sites" which display or offer child pornography on the Internet. Now, the next step belongs to the governments of the European Union to implement the proposals of the directive. Another important document of the EU is the Internal Security Strategy[3]. According to this document, in 2013 the European Union will establish the European Cyber Crime Centre, through which member states and EU institutions will build an operational structure, which will possess the necessary capacities for investigation and cooperation with the international partners (Internal Security Strategy 2010, 20).

3. CYBERCRIME IN ALBANIA

3.1 Background

Albania is one of the signatories to the Convention on Cybercrime. It has ratified this Convention by Law no.8888, dated 25.04.2002 "On ratification of the Convention on Cybercrime". Meanwhile, the implementation of the Convention in the domestic law by the Albanian state dates back to January 2008. Thus, law no. 9859, dated 21.01.2008, under Article 117 of the Criminal Code, entitled "pornography" has been added a special paragraph which provides for the punishment of actions that consist in the use of a child for the production of pornographic materials, as well as their distribution or publication on the internet or in other forms.

[2] Article 6 of the Directive, "Solicitation of children for sexual purposes"
[3] The EU Internal Security Strategy COM(2010) 673 final, 22 November 2010

Key steps in the implementation of the Convention in domestic legislation are made with the approval of Law no.10023, dated 27.11.2008. Criminal lawmakers, given the special characteristics of cybercrime, as regards the aspect of jurisdiction, made the necessary changes to Article 7 / of the Penal Code. Furthermore, by this law a series of types of criminal offenses in the computer field were included in the Criminal Code. These changes in substantive law should be supported with measures of procedural nature. With the approval of Law no.10054, dated 29.12.2008 some changes were made in the procedure code by providing some procedural moments, as the obligation to submit the computer data, sequestration of computer data, expedited preservation of stored computer data, expedited preservation and partial disclosure of computer data.

The existence of a comprehensive legislation, which provides a detailed breakdown of specific types of cybercrime, is not the only adequate solution to this problem. Implementing the above legal changes aimed at preventing and investigating criminal activities in the field of information technology requires the development of specific structures in the body of scientific police, the court and the prosecutor, capable to respond with expertise to all the problems. It is very important that crime prevention and investigation bodies understand and know well the way how each crime type might be performed or carried out, and also get equipped with the necessary technological tools to investigate and fight it. In 2009, for the first time, the Computer Crime Special Section was established in the General Directorate of the State Police, the Department against Organized Crime and Serious Crime, Directorate of Financial Crime. The number of employees at this facility has been increased from 3 employees in 2009 to 5 employees currently. One such sector since 2011 would also be extended to

9 (nine) of the Regional Police Directorates[4]. Increased level of expertise to investigate and detect cybercrime is associated with changes in the structures of the scientific police.

3.2 Categorization of cybercrime under Albanian law.

For a more complete treatment it is necessary to analyze the phenomenon of cybercrime and classification made to it by European or international doctrine associated with the Albanian criminal law, which has issued the provisions of the Convention rigorously and without any change. In the Albanian criminal law cybercrime is divided into two groups. *The first group* includes all those new illegal actions provided for by the penal legislators carried out through the use of communication technology and computer system or computer object to a particular subject. In this regard, computer crime includes any illegal activities conducted through electronic equipment and systems operations, and which has as its object the violation of the integrity and security of the computer or computer system and the data that it stores or processes. This category includes all those crime types aimed at protecting computer systems from: *unauthorized interference (Article 192 / b), illegal interception (293 / a), unlawful and unauthorized interference in computer data (Article 293 / b); illegal and unauthorized access to computer systems (Article 293 / c).* These crime types have got broader dimension mainly to the spread of the Internet. They can be consumed even without access to the global Internet network, usually in companies or institutions that use the intranet, or through separate specialized devices with electromagnetic waves. In categorizing these crime types, it is does not matter to the criminal lawmakers whether the subject of the offense committed these acts in order to obtain property or not. Legislators in these provisions intend to protect the integrity of the system and the security, accuracy and

[4] There is not yet such a structure in the Police Directorates of the regions of Kukësi, Dibra and Berati.

privacy of the data contained in the equipment or computer systems. The main element that distinguishes this category of actions is the fact that the object of the criminal activity is a device or computer system (which has stored data), an activity which is carried out through the use of computer networks and specialized computer knowledge by the subject of the criminal offense.

The second group includes all those cybercrime types which do not refer to equipment or computer systems, but use these technological tools to perform common crimes. In this case, the computer equipments serve as tools or instruments that help in committing the crime. In this regard, cybercrime, rather than a new phenomenon, is presented simply as the use or exploitation of information technologies to commit old crimes with new ways. Accordingly, this criminal activity occurs in different forms. From this perspective, cybercrime includes any illegal action committed through the use of a computer system, or in connection with it (computer network), which aims at unauthorized access, provision or distribution of information, possession, transfer of rights or money from the rightful owner to the subject of the offense or to a third party through a devices of another computer system or network based on personal or property purposes. This group includes a number of old crime types, but they are already committed using new tools or communication technology, such as: computer fraud (Article 143/b), computer forgery (Article 186/a), misuse of computer equipment (Article 293 / d), infringement of copyright and other rights related to it, use of a minor for the production of pornographic materials and distribution and publication of such material on the Internet (article 117/2), computer distribution of materials pro genocide or crimes against humanity (Article 74/a),distribution of racist or xenophobic materials through computer systems, racist and xenophobic motivated intimidation and insult through computer systems, respectively (Articles 84/a and 119/a and 119/b of the Criminal Code). In all

these crime types, computer or computer devices serve as auxiliary instruments in the commission of a crime, therefore the action does not have as main object the computer device or computer system, but it runs counter to the constitutional order and security, the property of the person, his dignity, coexistence in harmony between ethnic, racial, religious groups, etc.. In this case, computer equipments serve as an instrument for committing a criminal offense and not as a separate object.

3.3 Current situation of cybercrime in Albania.

The number of Internet users in our country is growing. As a result, there is an increase in the number of those who fall victim to these crimes and also to those who commit these offenses. Referring to the annual statistics provided by the Ministry of Interior (MoI Annual Report 2010, 37), it results that for 2010 have been referred to and identified about 65 criminal offenses in the area of cybercrime, which has proved involvement of 60 authors. 10 of them were arrested and detained by the police, while the rest were followed at large. In 2011, there have been 82 criminal acts, which were proved to have involved 111 authors, of whom 26 arrested and detained and 85 of them were followed at large (MoI Annual Report 2011, 42). During 8 months of 2012 there have been 48 criminal offenses, 32 of which have been discovered. Discovered works have proved involvement of 40 authors, 3 of which were stopped and arrested and 37 of them were released (MoI Semi-Annual Report 2012, 30).

The analysis concluded that the main forms of cybercrime recorded during this period are computer fraud, computer forgery, computer unauthorized intervention, and child pornography on the Internet. In Albania, the data of State Police Department since 2008 and following show that computer fraud is the most prevalent type. Main forms of computer fraud are computer fraud via the internet and bank card fraud. Specifically, computer fraud via the Internet has

emerged in the form of electronic fraudulent messages for fictitious lottery organization in order to obtain a sum of money from the victim, the creation and use of fraudulent websites in order to obtain personal and financial data of Internet users for illegal benefit, "phishing" method, fraudulently obtaining money amounts, using false computer data through the use of fraudulent websites being introduced as a commercial entity in a foreign country. Bank card frauds are another form of widespread criminal activity in Albania. Criminal activities shown in the form of fraud through bank cards are displayed through actions such as: use in ATMs of second level banks of plastic cards with magnetic stripe containing stolen bank information, mainly carried out by foreign citizens, use of the above cards to purchase goods, products or services in shopping center, use of stolen bank card data for booking travel tickets, accommodation in hotels, etc., providing information and selling through Internet stolen bank cards data and bank card data theft through various devices located in ATM, or using modified POS terminals (MoI Annual Report 2011, 40-53).

The data show that 2011 has been the most successful year in the fight against cybercrime. During this year, several police operations were successfully finalized, among which the one called "false ATM." In this operation, 5 Bulgarian citizens, thanks to some manufactured electronic devices, modified as part of the ATM, copied credit and debit cards data in some ATMs in Tirana, Durres, Vlora and Saranda, and then these data were used to produce cloned cards in order to withdraw money illegally (Interview with Mr.E.Kerluku Chief of the Sector against Cybercrime, General Police Directorate). This case represents the first precedent relating to computer fraud crime type, about which the District Court of Tirana has also given its verdict (The Judicial District Court of Tirana, 2012, Verdict 981).

For a more complete analysis of the phenomenon of cybercrime, given the fact that the legal regulations of specific

types of offenses in this area belong mainly to the end of 2008, we have judged that it is worth doing a detailed treatment of the elements of criminal act types, such as computer fraud, computer forgery, unauthorized access and interference with computer data and computer systems.

3.4 Computer fraud.

The major factor that characterizes the performance of this crime in the virtual space is the use of transmission computer or electronic devices and manipulation of data as it happens in the real world. Analyzing the computer fraud, we can say that the computer or computer equipment serve as a tool to violate the property of a third person. The first paragraph of Article 143/b of the Criminal Code provides all the elements that constitute the objective side of the offense that consists of input, alteration, deletion or removal of computer data or interference with the operation of a computer system. The main element of this offense in contrast to ordinary fraud is interference in the functioning of a computer system and manipulation of data electronically through actions such as: the input, alteration, deletion or removal of computer data or their transmission electronically, as it often occurs with acts or documents common with fraud crime. Through these actions the subject of the offense aims to transfer the rights or objects from the legitimate owner to himself. These actions provide a crime subject with unjust economic benefit, while reducing the wealth of the victim. The object of this crime are legal relationships established to ensure the normal exercise of private, public or state property rights, as well as to guarantee the integrity and security of computer data from criminal actions. In the case of computer fraud the criminal result is displayed on the changes that occurred in the data or computer system and the damage caused to the defrauded person or other persons. The subject of this crime can be any person who has reached the age of criminal responsibility. On the subjective side, the crime is

committed with direct intent, because the person knows s/he is carrying out an illegal action, but aims through fraud to attain for her/himself or third parties economic benefit or to reduce the wealth of a third party. Our penal code provides as specified circumstances commitment of this criminal act in cooperation, to the detriment of some persons, more than once, or if it has caused serious material consequences.

3.5 Computer forgery.

The main element of the ordinary forgery is the act of interference in the content of a document, changing, deleting, removing or adding data in order to use it for personal interests. Computer forgery is displayed in the form of use of computer equipment or technology to change the contents of an existing electronic document or to create a new document forged. The objects of this crime are legal relationships established to store computer data from any illegal action. On the objective side, the crime is committed with the following actions: access, alteration, deletion or removal of computer data unfairly to create false data in order to present and use them as authentic, regardless of whether the data generated are directly readable or understandable. The subject of this crime can be any person who has reached the age of criminal responsibility. This crime type can be carried out, mainly by changing the data held in electronic documents of the police, banks, insurance companies, etc. The most common forms of computer forgery *are e-mail spoofing, web spoofing, and phishing* (Octopus Interface 2007, 3), where the subject of such offenses, claiming that represents banks or well-known companies, forfeiting their name and logo, seeks to obtain information such as passwords or credit card data. It is worth mentioning that the main victims of these criminal acts are not organizations or financial institutions, but only individuals who fall prey to such tricks, giving personal or financial data. Computer forgery is performed only with fault that appears in the form of direct

intent.

3.6 Unauthorized computer access

Direct objects of this offense are legal relationships that are established to protect the inviolability of the computer system. In the objective side, two actions are predicted to commit this offense: *unauthorized access* or *excess of authorization*. According to the explanatory report of the Convention on Cybercrime, unauthorized access means *access into a computer system or part of it, through the use of another computer system connected to a shared network or global communications networks.* According to Article 192/b, by objective side, the only condition to consume this crime type is that access to the computer system be unauthorized or in excess of authorization, regardless of the outcome that has been achieved. This is in accordance with article 2 of the Convention, which provides for signatory states to call an offense just the act of unauthorized access to computer, regardless of the criminal outcome achieved. In the case when it is access to open systems, designed to use freely, without any restrictions, it cannot be spoken of as offense. Such may be the case of computer systems which can be used by all persons, without any limitations. Also, we are not dealing with a criminal offense if the person intervenes in a computer system according to eligibility. The subject of a criminal offense may be any person responsible. On the subjective side, offense is committed with guilt, in the form of direct intent, because the subject knows s/he has to be authorized to access a computer system, or is in excess of his authorization and again commits such an act. It also provides the commission of this offense in specified circumstances when performed in military computer systems, national security, public order, civil protection, health or any other computer system of public importance.

3.7 Interference in data and computer systems.

Direct objects of such offenses are legal relationships that are established to protect computer data and computer systems from illegal interference. On the objective side, crimes are directed against a particular object, computer data and computer systems. On the objective side, the crime is committed by illegal actions such as unauthorized input, damage, alteration, cancellation or termination of computer data. In all forms offense is committed only by action. From the objective point of view, it is necessary that interference with computer data or computer system is performed without the authorization of the person who manages the computer system. Subject of crime can be any responsible person, with the exception of persons who have a duty of maintaining those computer systems. On the subjective side, the crime is committed with direct intent, because the person knows that s/he does not have the authorization, but still performs all the above actions.

4. CONCLUSIONS AND RECOMMENDATIONS.

Strengthening the legal framework remains one side of the medal. For a more efficient protection it is necessary to build a more adequate penal policy in the fight against computer crime at the local or community level. New technological developments and the wide dimension that the world's cybercrime has taken ask for enrichment of legal regulatory framework with new types of cybercrime. Clear and standardized legal terminology should be used in the definition of each crime type, especially in terms of the objective side of the crime.

Law no.9859, dated 21.08.2008, under Article 117 of the Penal Code was added a particular paragraph, within the type of the criminal offense of pornography, which provides for the punishment of actions that consist in the use of a child for the

production of pornographic materials and their distribution or publication on the internet or in other forms. In fact, the provision gives the solution to the problem of distribution through a computer system of child related pornographic materials, not foreseeing actions such as maintenance, storage or possession of child pornographic materials, as defined in Article 9, point "e" of the Convention on Cybercrime: *possessing child pornography in a computer system or on a computer-data storage medium".* "Specialized bodies for the investigation and detection of cybercrime necessitate the inclusion of this provision in the material law. Specifically, in 2011 as part of an operation for investigating the crime of distribution and publication of child related pornographic materials by an Albanian entity, the conclusions of the scientific expertise was that, due to the formatting that the computer has undergone it could not be verified that the online publication of the child pornographic materials was done through that computer. However, the expertise pointed out that other materials related to child pornography were found in the computer. As a result, the criminal case against the alleged subject was dismissed because the fact was not provided for by law as a criminal offense[5].

The other side of the medal relates to the awareness of individuals and businesses to understand and recognize the risks of this phenomenon and to eliminate as much the possibility of exposure to cybercrime. Mainly, the categories most affected are individuals who do not have technical experience in this field and perform actions such as: online shopping, internet banking and those who use social network communication. Increased sensitivity to the public to the risks carried by this phenomenon is a necessity of every society. Therefore, it is necessary to take measures to raise public awareness of the risks posed by cybercrime, the ways of

[5] Interview with Mr. Elton Kurluku, Head of Sector, General Directorate of State Police

protection from this dangerous phenomenon and reporting criminal actions. On the other hand, a closer collaboration with the police is needed so that people become aware to report such crimes. It suggested that a "website" is created, where the public have information about the risks posed by computer and the use of the global network. It is necessary to improve school curricula, especially involving child education to teach them to be more careful in order not to fall victim to cybercrime.

Law enforcement structures and agencies have the duty not only to increase capacity but to interact with counterpart authorities in other countries in the framework of joint operations, to give a blow to these illegal actions. Cooperation at European and international level should be strengthened for a more complete and effective investigation. This collaboration would enable an appropriate solution to the problem of jurisdiction, exchange or increase of specialized capacities capable of investigating computer crime, training members of the scientific police, raising the level of technology or providing technological tools that enable investigation and tracking down offenders and strong collaboration with all computer security stakeholders. In the investigation of computer crime specialized equipment and knowledge are required, which should be updated on an ongoing basis. The investigation of this crime with international scope in accordance with the procedure rule encounters a number of difficulties and delays in the collection of evidence and facts. Liability imposed by criminal legislation for law enforcement authorities to investigate and identify the illegal actions resulting in the loss of property by Albanian buyer in misleading "websites" originating in other countries, not only requires closer bilateral commitments, but also involves a high cost for a small country like Albania. Practice has shown that the investigation and evidence collection techniques often result not efficient, because the crime subjects realize the criminal plan not participating physically, but using automated agents. These elements constitute a challenge to the

lawmakers, the body of scientific police, the court and the prosecution.

Lack of technical capacity of entrepreneurs of internet service provision to identify users who have a contract with the entrepreneur network is another challenge for our authorities. This fact makes it difficult or often makes it impossible to provide information regarding the identification of network users (and corresponding IP) in the case of illegal phenomena. In fact, the law no.9918, dated 19.05.2008 "On electronic communications in the Republic of Albania" has set obligatory standards and rules to be followed by private operators in the electronic communications market. Lack of meeting these standards by these operators, lack of modern technical equipment is an element that should be considered with much priority from respective structures of law enforcement, as AKEP (Telecommunication Authority in Albania).

Internet service providers should take measures to prevent the misuse of their networks for criminal purposes through establishment of a special national service, which shall warn them about possible illegal actions on their systems. Also, these internet service companies should cooperate with and assist the various initiatives of the sector of consumer protection from provision with illegal materials possible from persons or ghost companies, mainly abroad. It is necessary to make changes in the legislation, which would allow the blocking of access to their website. These changes should also include an obligation for service companies to submit and periodically update a list of relevant URLs, especially those with sexual content to minors. Special attention should be paid to copyright protection, organizing effective social campaigns to inform simple internet users about the importance of protecting these rights.

Therefore, adequate measures for maintaining a healthy society from cybercrime are a comprehensive and updated legislation, specialized structures capable to respond to this

phenomenon, as well as a more informed society.

BIBLIOGRAPHY:

_____. 2003. "Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems", Strasbourg, http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm, retrieved 10 Sep.2012.

Aldesco, A. I. 2002. "The demise of anonymity: a constitutional challenge to the convention on cybercrime." *Entertainment Law Review* 23(1): 81–123.

Castells, M. 2002. *The internet galaxy: Reflections on the internet, business, and society*. Oxford: Oxford University Press.

Council of Europe. 2001. Convention on Cybercrime. URL: http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm.

Council Framework Decision 2005/222/JHA of 24 Feb 2005 on attacks against information systems, http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32005F0222:EN:NOT, retrieved 15 Aug.2012.

Carter, David L. "Computer Crime Categories: How Computer Criminals Operate." http://www.lectlaw.com/files/cri14.htm.

EU 2011/92 Directive. http://ec.europa.eu/antitrafficking/entity.action;jsessionid=tlLqP3RBd76hc1wxhLTJZmZpvp396fY2dT1sT1GrBDxZpGHwv9Vy!-471497004?id=8fb6cb4e-d376-47c1-9926-30cf4d7a8abd, ret. 29 July 2012.

Ehuan, A. 2010. "Cybercrime and law enforcement co-operation." In *CyberForensics: Understanding Information Security Investigations*, edited by J. Bayuk,

129–140. London: Springer.

EECTF. 2011. 2011 EECTF European Cybercrime Survey. As of 17 February 2012: http://www.poste.it/salastampa/CYBER_CRIME.pdf, retrieved 3 sep. 2012.

Furnell, S. 2002. *Cybercrime: Vandalizing the information society*. London: Addison Wesley.

Grabosky, P. 2001. *Computer Crime: A Criminological Overview*. V: Forum on Crime and Society, vol. 1, no. 1. New York: United Nations Publications, 35–53.

Judicial Court of Tirana District, Verd 981, 2012, http://www.gjykatatirana.gov.al/ retrieved 24 June 2012.

Kushtetuta e Republikës së Shqipërisë.

Kodi Penal i Republikës së Shqipërisë.

Kodi i Procedurës Penale të Republikës së Shqipërisë.

Ligji nr.9918, datë 19.05.2008 "Për komunikimet elektronike në Republikën e Shqipërisë".

Ligji nr.8888, datë 25.04.2002 "Për ratifikimin e Konventës për Krimin në Fushën e Kibernetikës".

McConnell International, Cyber Crime and Punishment, note 4, http://www.mcconnellinternational.com/services/cybercrime.htm, retrieved 6 Sept.2012.

Ministry of Interior Affairs, *Annual Report 2010,* p. 37.

Ministry of Interior Affairs, *Annual Report 2011,* p. 42.

Ministry of Interior Affairs, Semi-*Annual Report 2012,* p. 30

Octopus Interface 2007 "Cooperation against Cybercrime", 11-12 June 2007, Palais de l'Europe, Strasbourg, France.URL:3_technical_cooperation/CYBER/Octopus_if_2007.asp#TopOfPage, 14.12.2007.

OECD. 2008. "Malicious software (malware): a security threat to the Internet economy." As of 17 February 2012: http://www.oecd.org/dataoecd/53/34/40724457.pdf, ret. 4 Sept.2012

Parker, D.B. 1998. *Fighting Computer Crime: A New Framework for Protecting Information*. Chichester,

England: Wiley Computer Publishing.

Philippsohn, S. 2001. "Trends in cybercrime, an overview of current financial crimes on the internet." *Computers & Security* 53-69.

Power, R. 2002. "CSI/FBI, Computer Crime and Security Survey." *Computer Security Issues and Trends* 1-22.

Robinson et al. 2012. *Feasibility Study for a European Cybercrime Centre*. Santa Monica, CA: RAND Corporation, 2012. http://www.rand.org/pubs/technical_reports/TR1218, retrieved 8 Sept.2012.

The EU Internal Security Strategy in action: five steps towards a more secure Europe. COM (2010) 673 final, 22 November 2010.

Thomas, D. and Loader, B. 2000. *Cybercrime: Law enforcement, security and surveillance in the information age*. London: Routledge.

United Nations Manual on the Prevention and Control of Computer-Related Crime, 4 U. N. Doc. ST/ESA/SER.M/43-44, U. N. Sales No. E.94.IV.5

Wall, D. S. 2001. *Crime and the Internet*. London: Routledge.

Wall, D. S. 2004. "The Internet as a Conduit for Criminal Activity." In *Information Technology and the Criminal Justice System*, edited by A. Pattavina, 77- 98. London, New Delhi: Thousand Oaks.

Wall, D. S. 2007. *Cybercrime: The Trasformation of Crime in the Information Age*. Cambridge, Malden: Polity Press, 49-67.