The Regulation of Cyber Crime in Albania in the Framework of Harmonization of Internal Legislation with the European Legislation

Aldo Shkembi, PhD

Lecturer of "European University of Tirana"; Email: aldo-sh86@hotmail.com

Indrit Shtupi, PhD

Lecturer of "Windom University"; Email: indritshtupi@yahoo.com

Arjan Qafa, PhD

Inspector of "Supreme Council of Justice"; E-mail, arjan.qafa@hotmail.com

Doi:10.5901/ajis.2016.v5n1p127

Abstract

The big social dangerousness of cybercrime and the increase of computer misuse, demand that his problem has to be addressed on certain law provisions. So, new interventions in penal codes are needed, interventions that will deal with this activity. In order to prohibit computer crime, many states are trying to find more efficient tools, methods and acts in this direction. Firstly, it is the juridical-penal regulation that has to be done, seeing the problem as a juridical protection fro the unauthorized interventions in computer systems. There has been discussion among low-making structures, with the approval of laws that has to do with the incrimination of the act of illegal intervention, concerning the moment when that intervention starts to be considered as a penal act. So, different states, see it as a penal act from the moment of the very first unauthorized intervention and some others from the moment that the smallest damage is caused. The aim of this paper is to make an overview of the regulation of cyber crime in Albania in the framework of harmonization of internal legislation with the european legislation. In recent years, Albania has worked for the establishment and implementation of international standards in the fight against organized crime, money laundry and corruption. Enough laws function in the national legislation such as: the law for electronic assignment, classified state information, protection of personal data, electronic communication, communication interception, for books, mail service etc.

Keywords: Cybercrime, Covention, Harmonization, Computer system, Computer fraud, Computer falsification.

1. Introduction

Related to the Albanian legislation on cyber crime in the range of the harmoization with the legale European Framework on Cyber crime, it is important to mention that there are also politics and documents and strategies confirmed, that help in the fight against cybercrime, from which the mos important are: The Sectorial Strategy of Society of Information; The Document of politics for electronic communication in the Republic of Albania; the Document of politics for development of telecommunication in the Republic of Albania; The decisions of the Council of Ministers for ratification of documents of politics and strategies etc. Some of the laws that help in the security of systems in society of information, are presented as below:

- Nr. 9880 law, date 25.02.2008 "On electronic signature"
- Nr. 9880 law, date 10.03.2008 "On protection of personal data"
- Nr. 9643 law, date 20.11.2006, changed "On public procurements", that makes possible the possibility of electronic procurement
- Nr. 9723 law, date 3.05.2007 "On the National Center of Registration"
- Nr. 9918 law, date 19.05.2008 "On electronic communication in the Republic of Albania"

2. The Albanian Legislation on Cyber Crime: The Ratification of Budapest Convention

Until the penal legislative changes of 2008, there weren't laws on penal acts in the computer field in Albania, although

computer systems were already part of the Albanian society.

Here, we include the harmonization of the national legislation with the international one, for the fight against cybercrime. Another reason that campaigned the inclusion of new juridical-penal norms, was related to the will of the legislator sto approach the Albanian legislation with the legislation of the European Union. Related to that, the Republic of Albania with the nr. 8888 law, date 25.04.2002 (published in the official notebook nr. 18, p. 18)[1] has ratified the convention for cybercrime, while in 2004 it also ratified the additional protocol of this convention. In this direction, we may say that provisions included in the Albanian Penal Code, in the fight against cybercrime are in a full coherence with the Convention of the Council of Europe "On cyber crime"

3. Cyber Crime as a Penal Act in the Internal Legislation of the State

To reflect the commitment of Albania, in the framework of the Convention on Cybercrime, the Ministry of Justice took the initiative to make the adequate provisions and add them in the Penal Code of the Republic of Albania and in the Code of Penal Procedure. These initiatives came to an end with the approval of the nr.10023 law, date 27.11.2008[2], and nr. 10054 law, date 29.12.2008. Cyber penal acts includes penal acts committed against or through systems and computer programs that contain computer data.

Nr. 10023 law/2008[3] adds as penal acts those behaviours (defined as such from the Protocol of the Convention on Cybercrime), that refer to computer deliverance of materials that has to do with genocide, crimes against humanity, racism or xenophobia. The normative solution that the Albanian legislators have given in this direction, was the one of including new provisions in the text of Penal Code, related to penal acts in computer field.

In this law there are provisions that make sanctions for illegal acts performed through computer, electronic devices, electronic networks etc, where the most widespread ones will be illustrated with examples from the court practices.

In the part of the work that follows, is presented an authentic juridical- penal analyze of circumstances of implementation of penal responsibility according to provisions we are talking about.

This explanation aims to make clear the risk that every individual, private business, or governmental agency has to take into consideration from the moment that it decides to use the services of an interconnected computer network in continuity.

3.1 Sharing materials in favor of genocide or crimes against humanity through computer

Nr. 10023/2008 law adds in addition as penal acts those behaviors (defined as such from the Protocol of the Convention for Cybercrime) that refer to the computer deliverance of materials that have to do with genocide, crimes against humanity, racism and xenophobia, Concretely, it is written in the proper part of Penal Code, article 74/a "*computer deliverance of material pro-genocide or crimes against humanity*"[4]. This act aim to punish the protectors of people and historic events that has to do with crimes against humanity, ignoring the sacrifice, the suffering and the memory of people that were objects of international crime.

This prevision aims to protect the life and the health of persons who belong to an ethnicity, nation, race or certain religion, this is in accordance with the constitutional provisions and also with the international instruments of basic human right and freedoms.

Because of the object that it aims to protect, this provision is positioned in the Second Chapter of the Penal Code "Penal acts against life. Crimes against life", in the session "Crimes against life committed deliberately".

And more concretely, objects of crimes are juridical relations established to protect life and the health of the person who belongs to an ethnicity, nation, race or certain religion.

---

[1] *Law nr. 8888, date 25.04.2002 (published in the official notebook nr. 18, p. 18).*
[2] *Law nr. 10023, datë 27.11.2008 for some changes in law nr. 7895 date 27.01.1995 " Penal Code of Republice of Albania ".*
[3] *Law nr. 10023 date 27.11.2008 (pg 190, uffícial jurnal nr. 9395, 2008).*
[4] *Article 74/a of Penal Code of Republic of Albania.*

3.2 In addition, nr. 10023/2008 law defines as penal acts "Sharing racist or xenophobic materials through computer system and insulting for racist or xenofobic motives through computers (article 119/b)

The goal of this provisions is the protection of dignity and personality of persons who belong to an ethnicity, nation, race or certain religion. For this reason they are positioned in the Second Chapter of the Special Part of Penal Code "Penal acts against life. Crimes against life", section VIII "Penal acts against moral and dignity"[5].

In this two penal acts three concepts "computer system" or "racist motives or xenophobie" are found, these are circumstances that specify this two penal acts in two directions: A) in the direction of the tool that the penal act is performed with and B) in the direction of the "racist or xenophobic motive", as a subjective part. The two acts, for the low risk that they present, are considered criminal offence, having for the two of them as sanction, fines or imprisonment up to two years.

As for the insult for racist or xenofobic motives through computers, we have to emphasize that with the nr. 10054 law, date 29.12.2008, "For things and changes in the Code of Penal Procedure"[6], it is said in the 59 article of the Code of Penal Procedure, to also among penal acts that are to investigate, if the person demaged asks such a thing, to be also insult for racist motives or xenophobie (article 119/b).

3.3 Computer fraud

Another penal act is the one of 143/b article of Penal Code "computer fraud". This provision aims to protect the wealth of people from computer interventions, that is done to their systems.

The aim of this provision is the criminalization of every manipulation in processing data, aiming an illegal transfer of wealth and causing a reduce of the wealth of the other person.

Computer manipulations are considered penal acts, if as a result of that possessor of the wealth, have now a reduced wealth and if the perpetuator of the criminal act acts in this was with his fre will. The terms "economical benefit" or "reduce of wealth" are too wide and include from money to the rights for credits, treasury bonds etc

3.4 Computer falsification

A computer penal act added with nr. 10023/2008 law is also "computer falsification" (article 186/a)[7]. This provision aims to protect the authenticity of computer data from access, change, erase, or removal in an unfair way, in order to present and use them as authentic.

This kind of falsification is specified from an objective side, because of the special way it is done. Specific for this penal act is that the acts of accessing, changing, removing or erasing computer data, has to be done unfairly. This reflects the idea that such a behavior is not always punishable, but can be legal or justified as a case of exercising a right.

3.5 Unauthorized access on computer

The penal act "Unauthorized access on computer" is written on article 192/b of Penal Code, that is a crime because of the relations that it violates, the forms it is practiced, and consequences that it causes[8]. This provision aims to protect the content of computer data from unauthorized access. Unauthorized access that can be emerged even in the form of overcoming competence to have access in a computer system, is a penal act that is just consumed by doing the action of accessing the system and seeing data that the system contains, without excluding the possibility that the perpetuator of the act can be responsible even for other acts, as the provisions of following articles show...

The unauthorized computer access covers the basic violation of threat against security (confidentiality, integrity, and availability of computer system and data.

[5] *Article 119/ of Penal Code of Republic of Albania.*
[6] *Law nr. 10054, date 29.12.2008, "For things and changes in the Code of Penal Procedure"*
[7] *Article 186/a of Penal Code of Republic of Albania.*
[8] *Article 192/b of Penal Code of Republic of Albania.*

3.6 Illegal eaves dropping of computer data

It is added in the Penal Code, article 293/a as penal act the process of "illegal eavesdropping"[9], that aims the protection of computer data from or inside of a computer system from illegal eavesdropping. This act, because of the big social risk, is considered as crime, having a sentence from 3 to 7 years imprisonment. This penal norm takes under protection the right of privacy in transmission / communication of data. It violates the privacy of communication in the same way as traditional eavesdropping and the registration of telephone conversations among people. Eavesdropping may also contain the registration of data. Technic tools may contain technical tools on transmission lines, also tools to gathe and register wireless communications. They may contain software use, passwords and codes.

3.7 Intervention on computer data, intervention on computer systems.

After 293/a article, another article, 293/b is added, it expresses as penal act the unauthorized interventions on computer data[10]. The legal interest that is supposed to be protected by that, is integrity and proper functioning, or the use of saved computer data or computer programs. The ""damages" or "deformations" are acts that cause a negative change of integrity or information of data or programs. The erase of data destroys them, and makes them unknown. While "suprimation" means every action that prevents or ends the availability of the data of the person, who can access the computer. These acts are penally punishable, if they are performed in an unauthorized way, that means that the person who has done the action didn't have the right for such a thing. This means that the testing or protecting a computer system that is authorized from the owner or its user, is the exercise of a right, and is not considered as penal act.

After 293/b article, another article293/c is added, it considers as penal act the intervention on computer systems, through the creation of serious and unauthorized obstacles that violate the normal functioning of the computer system[11]. The term "obstacle" refers to acts that affect in the normal functioning of the computer system. These obstacles can be crated through access, damage, deformation, change, erase or from the process of disestablishing computer data. After 293/c article, it is added another article, 293/ç that considers as penal act the misuse of devices or tools, according to the provision, the production, sale, giving for use, spreading or any other act for making a device available, if the device contains a computer program, a password, a code or some other similar data, that are created or adopted in order to access a computer system or a part of it, aiming to commit penal acts considered in 192/b, 293/a, 293/b, 293/c articles.

4. Conclusions

The companies around the world are attracted from many benefits that come from information and communication technology and governments in developed countries are investing more in this field. It is necessary that these profits which pass to the government and its citizens, be protected from cyber attacks, because those are very important for country's security. Cyberspace as a space without borders seek an international collaboration and coordination in order to guarantee cyber security. Furthermore with the membership in NATO and the progress made toward EU membership, Albania more and more is active part of many initatives and programs for cyber security and it must complete its commitments towards allies countries.

Albania must develop policies,standards, instructions and procedures based on best standards and practices in order to guarantee cyber security, to offer protection from cyber threats and respecting in every moment the principles of fundamental rights e freedom and also other democratic principles. Strategies and programs must be adjusted to the needs and the availability of the country to implement them, without avoiding to reflect the future needs of the country. The best strategy for our country would be the construction of capacities for cyber security, in the period when it is required it is more necessary.

Strategical objectives that must be followed in order to complete the above vision are:

1. The completion of legal framework in the field of cyber security
2. Raising awareness about cyber security
3. Increasing the level of knowledge, skills and capacities for expertise on the field of cyber security

[9] *Article 293/a of Penal Code of Republic of Albania.*
[10] *Article 293/b of Penal Code of Republic of Albania.*
[11] *Article, 293/c of Penal Code of Republic of Albania.*

4. The establishment of specialized units
5. Identification and protection of Critical Information Infrastructure (CIIP)
6. Creation and implementation of basic requirements of cyber security
7. Increasing investments for growing the security in state networks/systems.

References

Article 74/a of Penal Code of Republic of Albania.
Article 119/ of Penal Code of Republic of Albania.
Article 186/a of Penal Code of Republic of Albania.
Article 192/b of Penal Code of Republic of Albania.
Article 293/a of Penal Code of Republic of Albania.
Article 293/b of Penal Code of Republic of Albania.
Article, 293/c of Penal Code of Republic of Albania.
Law nr. 8888, date 25.04.2002 (published in the official notebook nr. 18, p. 18).
Law nr. 10023, datë 27.11.2008 for some changes in law nr. 7895 date 27.01.1995 " *Penal Code of Republice of Albania* ". (uffícial jurnal nr. 9395, 2008).
Law nr. 10054, date 29.12.2008, "*For things and changes in the Code of Penal Procedure*"