Nov 1st, 5:30 PM - 5:45 PM

Crimes In The Information Technology Sector And Their Investigation

Nikoll Rica
Albania University, nikoll_rica@yahoo.com

Crimes In The Information Technology Sector And Their Investigation

Nikoll Rica
Lecturer at "ALBANIA UNIVERSITY", Tirane
nikoll_rica@yahoo.com

Abstract. Through this thesis I would like to present to the reader information on criminal action in the computer sector, features of prosecution, disclosure, prevention and punishment of the authors of this criminal action. These type of crimes encountered in the last decade, are of international character and they cause serious consequences, threatening personal or public property rights through computer fraud. For first time, the computer crimes were predicted in the Albanian penal legislation in 2008, in a full approach with other European Union and USA countries experience. Of special interest for the reader it will also be the legal analysis of criminal actions of "through computer distribution of pro genocide or antihuman crime" "Intimidation caused by racism and xenophobia through computer system" "computer fraud" "Through computer counterfeiting " "Unauthorized access in a computer" The aspect of legal analysis of material law closely linked with the transformation changes that criminal procedural law, will be presented in the function of a full and comprehensive investigation, by charging new competences and responsibilities to Juridical Police for accelerated storage and maintenance of data, as well as the accelerated storage and partial disclosure of computer data. Moreover, I aim to create a clear concept on digital evidences as well as their sequestration procedure. The accomplishment of computer investigation will be presented closely linked with procedural competences in order to store the accelerated observation of certain computer data, include here the rules of delivery. Although that criminal act of computer fraud is more actual, electronic crime also expands in some other criminal acts, such as: child and female abuse, counterfeit, threat of murder, robbery, terrorist acts, prostitution, financial crime, etc. Last but not least, in this thesis I will present to the reader manageable aspect of investigation and judgment of these acts, mainly in Tirana.

Keywords: criminal , computer , Juridical Police , Albanian, European Union , USA

1 Introduction

The rapid changes in the technologicarea have not only made possible for the information to be available at any place on Earth or space, but also to influence every life aspect of the individuals and the societies in general. On the other hand, the mass use of computers and its advantages enable the coordination of action between criminal groups form different countries which increases the size and the pace of criminal activity. The spread of computer technology in all life aspects, the difficulty of identification and detection and the development of a mutual world wide web have actually enabled the cybercrimes to be more dangerous and to be present in many countries simultaneously. Thus, computer crime is an important issue pertaining to all the countries worldwide. In Albania as well, according to the statistics there are about 1.4 million users of internet i.e. almost 49% of the population with a rate of increase of 60% in the last decade. Only on Facebook there are 1.084.880 registered users from Albania. On the other hand there exist databases where information about the public and private institutions' financial and economic state are administered, some of which may be also classified information. The wide distribution of the web and computers potentially increases the risk of illegal intervention in the system in order to steal or modify classified information which would further lead to grave consequences. For example the leak of information from the State Police or the Prosecutors' Office for a certain case, would not only jeopardize the integrity of the investigation but would also put in danger the life of the individuals involved in the process particularly the witnesses and the collaborators of justice.

2 The development of the legislation against computer crimes

The first law with solid provisions against computer crimes was passed in the US in 1984. This enabled the protection of the classified information in the databases of the computers being used by the public administration and financial institutions. According to these provisions the computer crimes are classified under three main categories: The unauthorized access or obtainment of information from the financial computer networks, credit institutions, businesses and government agencies. The transferring, damaging, destruction or interference of/with the information and the restriction of unauthorized access to computer data bases. The access of governmental information of national importance regarding defense and international relations. Later on, in 1985 in Canada, some articles were implemented in the Penal Code, regarding the computer crimes such as: unauthorized intervention in the computer systems and databases; the use or the attempt to use a computer system to commit one of the following offenses: destruction, reproduction, termination, and the deliberate damage of the data; illegal spying on communication, the theft of telecommunication services; illegal earning of communication facilities; the use, withhold or the smuggling of passwords etc. The penal legislation has undergone sensible changes in the provisions regarding computer crimes also in the European countries. Changes of this nature are the ones in the Polish penal code (1997), which envisions the criminal offenses in acts committed through telecommunication fraud, software theft, computer espionage and the prevention of the risks related with the interference in the databases and data processing entities. Another example is the Macedonian penal code of the 1996 which condemns the interventions in the computer networks. For the first time, computer crimes were envisioned in the Albanian penal legislation in 2001 with the changes in the article 192 of the Penal Code, "Interference in the computer networks". This provision predicts that: "The intrusion of any form in the computer software or networks constitutes a criminal offense and it is condemned by monetary penalty or imprisonment up to three years. The same offense when brings about serious consequences can be condemned with an imprisonment up to seven years." Whereas in 2008, there were other important amendments in the penal code regarding the computer crimes, which were in accord with the experience of the other European Union countries. These changes are based in the legal context below: The Budapest Convention on Cybercrime (Council of Europe) ratified with the law nr.8888 of the date 25.04.2002
The Lanzarote Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Council of Europe) ratified in the law nr. 10071, date 06.03.2009
The Guidelines nr. 2011/92/EU of the European Parliament and Council of Europe on the fight against child abuse and sexual exploitation and child pornography.
The main dispositions that the Albanian penal code envisions nowadays in the field of information technology are:
Article 74/a, "Computer dissemination of materials in favor of genocide or crimes against humanity."

Article 84/a, "Threat due to racist and xenophobic motives through the computer system",

Article 117, "Pornography",

Article 119/a, "Dissemination of racist or xenophobic materials through the computer system",

Article 119/b, "Insulting due to racist or xenophobic motives through the computer system",

Article 137/1, "Theft of the network of electronic communication",

Article 143/b, "Computer Fraud",

Article 186/a, "Computer falsification"

Article 192/b, "Unauthorized computer access",

Article 293/a, "Unlawful wiring of computer data",

Article 293/b, "Interference in computer data",

Article 293/c, "Interference in computer systems",

Article 293/ç, "Misuse of equipment",

A computer crime can be considered any type of illegal action which is committed directly against data bases or computer systems and also when these actions committed through this technology.
The target of these criminal offenses are the legal relations established to ensure the confidentiality, integrity and the availability of the computer systems, network and data as well as to protect the legitimate rights in the use and development of information technologies.
These criminal offenses are committed through acts which aim to illegally interfere in computer transmissions and programs. The lawmakers have considered illegal any interference in the computer programs and transmission without determining the kind of interference and the concrete method by which this is achieved. The illegal interference can be partial or whole and can be achieved through illegal interceptions, interferences in the system or data bases as well as through the misuse of the computer devices to commit the above mentioned offenses. Objectively considered, these offenses necessarily demand a flow of consequences. These offenses are deliberately committed while the motives or intents have no relevance for the qualification of the criminal offense, other than the increased social risk.

3 The accelerated storage and data maintenance and preservation of accelerating or partial disclosure of computer data

In the fourth chapter of the section II of the Criminal Procedure Code titled "Ex officio activity of judicial police" the Albanian Parliament in 2008 has added two provisions, which deal with the accelerated storage and data maintenance and preservation of accelerating or partial disclosure of computer data. Regardless their situation in the Criminal Procedure Code, these provisions clearly state that the court police only acts with the consent of the prosecutor. The warrant for the accelerated storage of specific computer data, including those of traffic, is issued in the cases where there is reasonable suspicion based on evidence to believe that this data can be lost, damaged or altered.In this case the person responsible for the accelerated storageof the data traffic is obliged to take the necessary precautionsto ensurethat the stored data are valuable regardless the number of service providers included in the transmission of the information.

This person should guarantee the prosecutors or the authorized court police, the disclosure of an adequate amount of data traffic, in order to make possible the identification of the service provider and the path of transmission of the communication. The authority given to the prosecutor to warrant the accelerated storage, partial disclosure and maintenance of the computer data is an exception from the general rule, when there is reasonable suspicion based on evidence to believe that this data can be lost or damaged. Meanwhile the general rule on handing in of computer data states that this action can be warranted only by the court. This competence was given to the Court, on December 20081, as responsibility to protect the privacy of juridical and physical persons during the phase of investigation in order to prevent the abuses during the gathering and handing in of computer data. According to Article 191/a, in case of proceedings on criminal acts in the field of information technology, at the request of a party, the Court orders the controller or the holder to deliver memorized computer data. This procedure also applies in case of service providers for delivery of any information for subscribers or services offered by providers. Only in the cases where there is a reasonable suspicion based on evidence to believe that the delay can impair the investigation process, the Prosecutor has the right to decide to enforce the holder, controller or the service provider the disclosure of the computer data memorized in a computer system or other mean of data storage. In this case, the Court should asses the Prosecutor's decision within 48 hours after taking notice.

The storage of computer data traffic or communication is related not only with the criminal offense of "Computer Fraud" but also with other offenses which include a computer system. The provisions on the accelerated storage of computer data are new methods of collecting electronic evidence related to a criminal offense. These provisions enable the traditional methods of control, examination and sequestration to remain effective also in the new technological environment. Meanwhile the offense of "Computer Fraud" envisions provisions for the new forms of criminal activity such as fraud including

the one with bank cards. The new technological advances have made possible the administration of money through computer systems such as money accounts, deposits etc. These can easily become a target of manipulation like any other traditional form of property. These manipulations can be achieved through the insertion of fraudulent data on computers or software during the processing of data, through two main ways:
Through entering, altering, deleting or removing computer data;
Through the interference in the functions of a computer system etc.
There are computer systems involved also in other criminal offenses like the abuse or exploitation of children and women, falsification, threaten of murder, theft, terrorist acts, prostitution, financial crime, corruption etc.

4 Some other forms of computer crimes in Albania

Fraud through the internet:

Fraudulent electronic mail for the organization of fictive lotteries (Nigerian Scam)
The creation and use of the fraudulent webpages with the intent of obtaining financial and personal information of the Web users, for illegal profit, for example the phishing method.
Monetary profit through deceit using false computer data obtained through the use of fraudulent websites which come across as commercial entity in foreign countries.

Bank Card Fraud:

The usage of magnetic stripe cards, which contain stolen bank information mainly from foreign citizens, in the ATM's of the second level banks.
The use of the cards mentioned above to buy goods or services in commercial entities or shopping centers.
The use of data from stolen bank cards for the booking of travel tickets, hotel accommodation, booking for the organization of ceremonies.
The theft of bank cards data through different devices plugged into different parts of ATM's or through modified POS terminals.

Computer Falsification:

The falsification of digital data of legal importance
The falsification of software programs with the intent of selling them as authentic.
Unauthorized computer access
The illegal access of public or private entities' webpages with the intent to cause a malfunctioning or to destroy the reputation.
The unauthorized access of the email addresses of Internet users.
Breaking into systems or programs to steal personal or financial data
Child pornography on the net
The exchange of pornographic materials featuring minors from internet users in Albania.

5 Statistical data on criminal offenses in the computer crime's field

According to the statistics from the State Police during the year 2012 have been detected about 83 criminal offenses of which 54 have been solved, with 71 perpetrators, 5 arrested on the spot and 66 free defendants.

Classified according to the categories:

Table 1. Divided according to the criminal offense:

Nr	Computer crimes	Detect.	Solved cases	Offenders in total	Arrested and detained	Free	Run away
1	Information and technology field related	34	23	28	-	28	-
2	Through computer systems	49	32	43	5	38	-
3	Total Sum	83	55	71	5	66	-

Computer fraud, article 143/3, 35 detected cases with 35 offenders of which 15 arrested and 30 free.
Computer falsification, article 186/a, only 11 detected cases with 6 offenders.
Interference in computer data, article 293/b, 14 detected cases with 11 offenders.
Interference in computer systems , article 293/c, 8 detected cases with 8 offenders.
Unauthorized computer access, article 192/b, 12 detected cases with 8 offenders.
Threat due to racist and xenophobic motives, article 84/a, 1 case, 1 free defendant.
Dissemination of racist or xenophobic materials, article 119/a, 1 case, no identified offender.
Child pornography, article 117/2, 1 case, no identified offender.

During 2011, there have been detected 82 criminal offenses, with 111 perpetrators of which, 26 have been arrested and 85 have been investigated in freedom.
According to their courses the offenses are divided:

Table 2 During 2010 there have been detected about 65 cases, with 60 perpetrators, 10 arrested and 50 free defendants.

1	IT crimes	61	52	94	26	68
2	Computer syst. crimes	21	19	17		17
IV	Total	82	71	111	26	85

According to the offense they are divided:

1 case for the offense of "Threat due to racist and xenophobic motives through the computer system", article 84/4, Penal Code, 1 free defendant.

1 case for the offense of "Insulting due to racist or xenophobic motives through the computer system "article 119/b of the Penal Code, 1 free defendant

31 cases for the offense of "Computer fraud", article 143/b of the Penal Code, with 30 defendants, 10 arrested and 20 free.

16 cases for the offense of "Computer Falsification", article 186/a of the Penal Code, with 15 free defendants.

6 cases for the offense of "Unauthorized computer access", article 192/b, with 6 free defendants

1 case for the offense of "Unlawful wiring of computer data", article 293/a of the Penal Code, with 1 free defendant.

5 cases for the offense of "Interference in computer data", article 293/b of the Penal Code with 4 free defendants.

4 cases for the offense of "Interference in computer systems",article 293/c of the Penal Code with 2 free defendants.

Considering that these types of criminal offenses have emerged in our country only in the recent year as the result of the development of the information technology and the computer systems, the police court is mainly responsible to execute the first investigations for the detections and accumulation of data regarding computer crimes.

The statistical data are represented in the graph below:

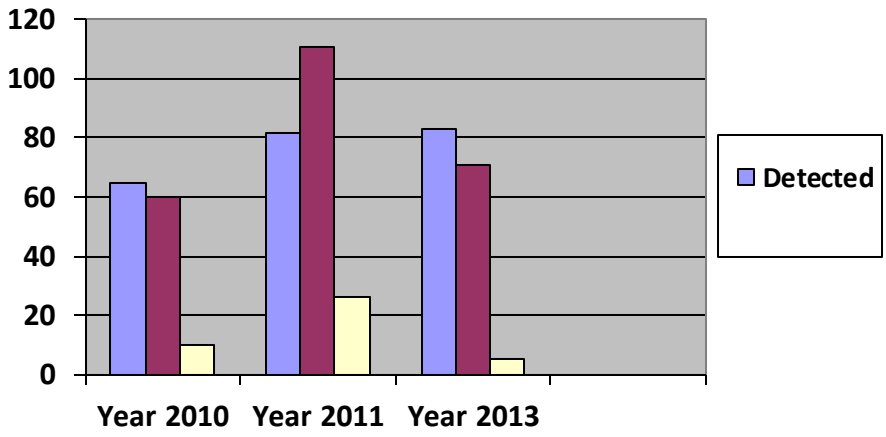

Fig.1. Statistical data

For these reasons, the employees of this procedural entity should be well-prepared to anticipate the criminal activity emerging in the computer crimes field. Particularly in the cases where the documentation of the scene of the crime with computer evidencedisplays some peculiar features and hardships as a result of state of the internet cables or wireless, mobile phones, PDA's, electric current, conductibility to the electric appliances and the lack of appropriate experience regarding these crimes, the obligation of the police court to attend the training regarding computer crimes, is doubled.

Some of the courses to achieve this purpose are:

Firstly: The creation of a clear concept about the digital evidence and the computer crimes in general.

A digital evidence4is considered all the information or data valuable for an investigation, which is stored, transported or transmitted through an electronic device. This evidence is acquired when the data or the electronic devices are levied for examination. The police inspectors should take into consideration the fact that data storing devices can provide crucial evidence regarding the given investigation. For example, from a mobile phone, deleted numbers can be drawn out to indicate the call logs; schedules recorded on a computer are preserved according to a chronologic order and so on. Even the television programs recorded in a VCR can sustain or overthrow an alibi by confirming the time of registration. The digital evidence has some features:

A hidden evidence is one, the value of which is not visible with the naked eye therefore special processes involving criminology investigation are needed to detect it (fingerprints, DNA) :

It can easily overcome the jurisdictional boundaries in a short time;

It can be altered, damaged or destroyed easily;

It may not be durable for long periods therefore it should be handled swiftly;

Secondly:Familiarization with the computer systems and related hardware.

Computer systems contain hardware and software which contain data. A computer system may include:

A metal case which contains circuits, microprocessors, hard drives and connecting units

A monitor or other device for video display;

A keyboard;

A mouse;

Peripheral units or storing and other removable devices.

Computer systems can be of different formats: laptops, desktops, towers, rack mounted, minicomputers and mainframe computers. Other peripheral devices include: modems, routers, and printers, scanners, charging devices and connecting devices.

In o computer system there can be found valuable evidence for the investigation of criminal offenses related to the computer crimes or information technology in general. For example : the storing devices, software, attached documents, pictures, memory cards, electronic emails with attached documents, databases containing financial information, browsing history, lists of friends, electronic agenda and schedules, data saved on removable devices and any other information obtained from a computer system and its components it can be a valuable source of evidence.

Thirdly:The assessment of the sources of digital evidence, the procedure of obtaining and levying them.

The digital evidence on computers or other electronic devices can be altered, hidden or destroyed easily. Therefore it's vital to be familiar with the procedures of crime scene investigation; the sequestration and the acquisition of the material evidence comprises one of the main requirements of an inquiry for the successful finalization of the investigation of computer crimes. The procedure for attainment and sequestration of computer information it is determined in the article 208/a, of the Penal Procedure Code, a provision added with law nr. 10051, of 19 December 20086. These evidences can be picked up by individuals specifically trained for acquiring electronic evidence.

A police officer who comes in contact with a crime scene containing such evidence should keep in mind: To be aware of the fact that on several computer devices like: keyboard, mouse or other removable devices (flash drive), there might be left hidden evidence (finger prints, DNA) or any other physical evidence that should be preserved until the arrival of the crime scene investigation group and their sequestration. Meanwhile also the storage drives of the computer, weather internal or removable and also other electronic devices found in the crime scene can contain valuable information for the investigation. To be aware of the crime scene under investigation in order to ensure the physical evidence from any possible deterioration. Until the arrival of the investigation team, the police officer should not examine the content of any evidence. The only thing he is allowed to do is to record any visible evidence. To be informed and to value as evidence also other things found in the crime scene like: electronic devices, software, storage devices and any other technology that can function independently or that can be attached to a computer system. These devices can be used to provide the users more access and to expand the functions of the computer systems or other devices. These devices can be : data storing tapes, spying devices, digital cameras, video-cameras, digital video recorders, digital audio recorders, electronic games devices, keyboards, mouse, switches for video exchanges, SIM card adaptor, GPS, GPS receiver and explanatory materials related to them. To refer to the prosecutor before sequestrating or starting to examine the content of electronic devices, because only the prosecutor is entitled with the power of issuing warrants of examination in the cases of accelerated storage of computer data. In any other case the control and the examination can be done only with a court warrant. To search for papers possibly containing passwords, hand-written notes, notebooks with blank pages where can be found traces of what has been written in the removed pages; user manuals for the software or computer devices, calendars, literature material, texts or printed graphics from the computer which can give away information related to the investigation. To preserve with caution the digital evidence during the transportation making them apt for examination. It should be taken into account the fact that

the digital evidences are obtained, packaged and transported through special techniques because they can be easily be altered or damaged by the magnetic field generated from static electricity, radio transmitters and other devices. In these cases special gloves, anti-static bags and other non-magnetic materials should be used.

6 Conclusion and recommendations

The specialists of the sector against computer crimes in the General Directorate of State Police and the ones in the Police Directorates of the Districts should undergo special training courses related to Informatics. This is necessary because the perpetrators usually possess certain knowledge on the technology of transmission of information and cybernetics. The law enforcement entities, mainly the police court, prosecutors' office and the tribunals should inform the public opinion, on the methods used in computer fraud, through press conferences and other means. Special projects should be prepared on the exchange of information and the enforcement of the collaboration between the state institutions, law enforcement agencies, the stakeholders and private entities for the prevention of the criminal activity related to the information technology area. There should be founded an interministerial administration committee for the classification of information and the reinforcement of the provisions for the processing and storing of data as an important element of national security.

References

1. Council of Europe. "Convention on Cybercrime".
2. The Budapest Convection on Cybercrime, November the 11th 2001
3. Directive 2011/92/EU of the European parliament and of the Council on combating the sexual abuse and sexual exploitation of children and child pornography.
4. Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, Lanzarote, confirmed with the law nr. 10071, of the date ,06.03.2009
5. Penal Code of the Republic of Albania.
6. Law no. 10023, date 27.11.2008. " Changes in the Penal Code of Albania"
7. Law no. 144/2013, " Changes on the Penal Code of the Republic of Albania"
8. Criminal Procedures Code of the Republic of Albania.
9. Law no.10054, date 29.12.2008, "Changes on the Penal Code of the Republic of Albania"
10. Law no. 9918, 19.05.2008 &no. 102/2012 on "Electronic communication in the Republic of Albania".
11. Manual on the investigation of corruption and financial crime. Tiranë, 2010,