The ways of computer use and its role in the commission of criminal acts.

Linert Lirëza, Joniada Musaraj, Ersida Teliti

1.Department of Law, UAMD, Durrës-ALBANIA
linert_lireza@yahoo.com
2. Department of Law, UAMD, Durrës-ALBANIA
joniada_d@hotmail.com
3.Civil Department, Law Faculty, Tirana University, Albania
erisdateliti@yahoo.com

ABSTRACT

In this article there is presented the role of computer use in the commission of offenses, serious consequences from these illegal acts, as well as measures to prevent them. Through this paper we have attempted to handle the computer in relation to crime in four different plans: Computer systems are presented as targets when they are attacked, in order to change the data or crush them. These systems are introduced as a means of committing criminal acts (modus operandi) because computer processes used to enable, facilitate and expedite the realization of certain criminal acts. Computer often used as a mechanism of stash, planning and organization in the commitment of criminal action. Offenders in the computer field, by using computer systems perform criminal acts in the form of fraud, by manipulating data in order to benefit illegally. These illegal actions affect electronic commerce, banking, private investments etc. A special attention in this paper is devoted the computer system, as an instrument that prevent and prove criminal acts. Through information technology, state domestic authorities and overseas exchange accurate and rapid information in order to precede criminal acts. At the end of the paper are identified computer offences and legal measures that authorities should take in order to isolate the criminal acts.

Keywords: *Computer systems, Offence, Information, Form of criminality, Prevention*

INTRODUCTION

The development of Information Technology and its application in the automation of work processes represents a common phenomenon nowadays. The use of IT is part of the daily activities of a range of people. Using the computer to perform many functions in economy, health, industrial and science has brought progress so fast, that way of life has changed irrevocably. This development, in contemporary society has brought a large number of facilities and in turn the misuse of technological achievement, has violated and continues to affect different social relations. As a consequence the increase of criminal behavior is widespread. Computer systems offer some new possibilities with regard to the violations of the law mainly being the instruments of crime.

So this form of crime is very hard to distinguish the exact period of occurrence of the first criminal acts. Criminologist Edwin.H. Sutherland, in his thesis "White Collar Crime", the beginnings of the introduction of computer crime to depict the appearance of criminality to "white collar" in the early twentieth century. Other authors associate computer crime with the development of the Personal Computer in the second part of the 20th century. Ever since with the help of computers there has been a substantial rise of computer crime. The first case presented, regarding computer misuse was recorded in 1958 and only eight years later, is marked the first time that the computer is used as a means to commit theft of a bank in Minnesota (USA) [**1]**

As regards the concept of computer crime, given its dimensions is difficult doctrine formulation of a definition generalizing. The difficulties of defining computer crime are not only due to the diversity of forms of crime but also the speed of computer crime spread. [2] However in an attempt to give a autonomy statement, is noticed that this phenomenon is "a new form of crime, conducted by entities that enjoy special affinity computer, who use the computer as an instrument for carrying out illegal or object on which directed the attacks. " As above, the definition of an illegal action as computer crime is not necessarily associated with material benefits from the perpetrator. These criminal acts are difficult to determine in time and space, as can be performed in a particular jurisdiction without being physically there doing illegalities not so understandable.

In these conditions, the Albanian Parliament has ratified the "Convention for the crime in the area of cybernetics", with some reservations to avoid criminal liability provided in certain circumstances where may be required civil liability. The convention aims to deter actions directed against property, confidentiality, integrity and availability of computer systems, networks and data. Concerning to the role of computer in the emergence of criminal responsibility required an analysis in four plans.

1.1 Computer system as an object of attack

The computer is presented as an object of attack in the case when it is stolen or sabotaged. The author of the computer crime attacks the computer on purpose to change the data or destroy them. In many cases, the computers have been attacked and burned by certain mechanisms thus putting them out of functioning. The consequences caused by the attack against the computer can be serious and international. This way the attack effects the data in the computer system and the values of the software and the hardware, thus damaging no only "the service provider" but also its receiver.
As a result, the reliability on the information truthfulness and the service quality becomes suspicious.

1.2 The computer as an object of performing a penal criminal offences (modus operandi)

A computer criminal offence can not be performed without the help of computers. In the present case, the computer enables or facilitates the work of the author in realization of certain fields, very day and more is risking the monetary means, goods, services, intellectual property, privacy, racial acts or pedophilia.

One of the misusing forms of the computers in the use of computer to execute a criminal act such as that of fraud by manipulating of data. The manipulation consists in insertion and registration of incorrect data, on purpose to profit personal property or to the benefit of the thirds. Today, such actions present the largest number of the computer's bad users, considering the number and kinds of forms through it is presented. These frauds are numerous in the control of the movement of financial capital and usually appear in the form of fraud related to accounting and business banking, fraud in connection with investments, insurance, tax obligations, declaration of bankruptcy, money laundering etc.. "[**3]**

Practice has proved that computer fraud usually have taken place via Internet in case of "Electronic Commerce". Based on the findings of consumer protection agencies through the Internet, according to the agency's 2003 Security APIs Consulting determined that "every 44 seconds one of the buyers becomes victim, after deciding to purchase merchandise whose opportunities notified via the Internet." Only in 2003, were discovered more than 1400 web site (website) only in the medical field where a number of companies have propagated and sold capsules to increase energy in the human body, healing of AIDS, various types of hormones etc., which have cost from 30 to 1095 dollars but by deceiving buyers for their effects**.[4]** As you can see, the classic means

for carrying out of the deceit acts are being replaced with modern and efficient means by facilitating the consumption of this illegal action. Authors of this deceit, this way, avoid the direct conflict to be damaged by worsening the act by putting him under the penal responsibility.

It is worth mentioning that the computers often appear in a double role, as an object of the criminal act and as a means of its realization, as they are realized in such a manner that the computer is used to attack the other one.[3-4]

1.3 Computer system as a means of stash, planning, organization and leading.

The importance of the computer for a moment not to be questioned, as not only brought rapid economic development but every day more and more is improving the quality of life.

However, despite the advantages and opportunities brought about, the computer in many cases it is found as a tool of abuse at the hands of different criminal groups or organizations. This instrument has become a "weapon" precisely in the planning, organization and leading of the criminal groups. In this sense computer more and more is being used in the field of the organized crime, especially in the phase of preparation, and organization of activity as well in the progress of inspection and administration of such activity.[**5]**

If an analysis of perpetrators of crimes recorded three categories of subjects to perform criminal acts. The first group of authors of criminal acts is composed by persons who interfere with the computer, to test their capacity in the computer field. The second group of authors intervenes in systems, on purpose to destroy, disorganize, change or block the functioning of the computer. The third group of authors intervenes into the computer on purpose of material profit or promotion of the ideologies which infringe the human's rights and freedoms. Under such conditions, can be said that utilization of the computer from the part of criminal act's subjects, has enabled them to plan their criminal actions and organize them in a quick, precise and quality manner. An increasing role in this context is playing the electronic mail service (E-mail), which provides communications anywhere in the world so fast and safe.

1.4 Computer System as a means for the prevention, investigation and examination of the crime.

The evolution of information technology has enabled computers with their capacity, to be evaluated as effective mechanisms in the prevention,

investigation and examination of criminal acts. Insertion of the data of the authorities of justice into computer system, swiftness of transfer and the capacity to elaborate them provide the possibility to these authorities to be correct during the investigation process. In this context, especially thanks to the Internet computer system which operates in real time, the subjects of crime are almost impossible to avoid criminal liability. The justice institutions of different countries via Internet exchange information identify the wanted persons and in certain cases they conclude in arrests. These institutions operate through the internet addresses by exchanging different photos, trials and acts. [5]

In 2008 at the General Directorate of Police, was created the section of the computer Economic Investigation as a structure specialized in clarification of the computer criminal acts.

Although this structure functions as a special body in the investigation of computer, the intelligence and computer preparation of the criminal acts' authors in many cases excludes them from evidencing or detention as the author of the crime. Under the data of 11-month period of 2010, it results that only 31 computer crimes have been evidenced. **[6]**
As it is observed, identification and verification of the computer criminality is a difficult task and quite complicated. Unauthorized intervenes into the computer system can be performed without leaving any traces by the author's part and the operation may have been performed in one place, but the consequences has been in another place, at a very big distance. To perform criminal act, they use technical methods, which can be hardly identified since they do not hinder the process of the system work, and they can be often proved only in case they are identified just at the moment. All the studies in this field indicate that the mysterious number of criminality in this field is large. None of the computer installations is absolutely resistant against the criminal acts, because of none absolute protection exists. So, the number of cases, recorded and published, presents a true archive, although criminal chronicle revealed a small portion of these works.

2. Criminal offenses in the computer field as an obligation to be provided by the Albanian legislation.

One of the criminal offences in the field of computer criminology provided by "the convention on crime in the field of cybernetics" is the "illegal access" which provides access to a part or the whole computer system without permission. According to this provision, the subject of the criminal act might have violated or not the computer security measures. In this way, the

convention enables the contractual parties to draft the provision according to the appropriate context.

The Albanian government has the obligation to adopt in its legislation the provision as a criminal offense, "the illegal interception conducted with technical means against the computer data". However, "the Convention on crimes in the field of cybernetics" enables the contractual party in the convention to provide as a criminal offense cases in which "the offense is done on unfair purpose". (Act 3)

Another criminal offense in the computer field is "data interference". [6] In this provision are included all the illegal acts which are conducted which the purpose to harm, delete, modify, change or erase the computer data with no permission.

Although the Albanian state is obliged to adopt this provision, the Convention permits the contractual party to classify these acts as criminal in nature when they have resulted in serious damages. (Act 4)

This international agreement provides even "misuse of devices" as an obligatory provision to be applied by the contractual party. According to this provision, the selling, use, import or distribution of a device (computer program) or a computer password through which the illegal access or data violation is intended should be considered computer crime.

According to this international act, the Albanian state needs to take the necessary measure in the definition of *"Computer Fraud"* as a separate provision in the penal law. Through the ratification of this provision, the protection of property relations endangered by the use of computer system is required. The perpetrator, through the access, altering, erasing or removal of computer data, causes the loss of property of the victim, with the target of material benefits for oneself or a third party.

In the category of "*criminal offences related to content*", the Albanian authorities need to provide as a crime all the acts committed through computers which aim the possession or distribution of child pornography in a computer system; the meaning of "child pornography" will include pornographic material which visually shows up:

a) a minor under the age of 18 who engages in explicit sexual directions;
b) a person who seems to be a minor engaged in explicit sexual directions;
c) realistic images which present a minor in explicit sexual directions;

In these conditions, the legislator needs to adopt all the obligations of the convention into the domestic criminal legislation.

CONCLUSIONS

The current trends demonstrate that in the future computer crimes will be positioned as main objective in the application of global policies for the prevention and fighting of this form of organized crimes. Practice has demonstrated that there are several factors which hamper the protection from computer crime.

First, perpetrators of these criminal offences have not only a high level of intellect but they also enjoy the support of computer devices in hiding criminal acts. These criminal acts are difficult to be detected, investigated and proved so that their perpetrators can be punished.

Secondly, in contrast to traditional criminal offences which are detected by the victim or the injured party, computer crime, in most cases, is not detected by its victims. As a result, "the victims" realize that they have been the subject of computer attack only after it has been communicated by the authorities of law enforcement.

Thirdly, the prosecuting authorities and the police do not posses the necessary ability and computer knowledge to prove the criminal offence and to detect its perpetrator.

Fourthly, criminal legislation against computer crime is still incomplete and in a lot of cases remains evasive in interpretation.

In these conditions, it is important to adopt criminal offences in the domestic criminal legislation. These provisions need to be drafted under the experts support and in accordance with the Albanian context.

The criminal prosecution bodies and police authorities need to recruit and train specialists in the computing field, as a supporting structure in the investigation and examination of computer crime.

In conclusion, based on the characteristics of these criminal offences, an intensive interstate collaboration is required using special tools for the detection and investigation of computer criminal offences.

REFERENCES

[1]. The Convention on crime in the field of cybernetics ratified by Law Nr.8888, date 04.25.2002

[2]. Criminal Justice Manual, London 1979

[3]. The UN Manual Adapted by Editor M.J. Mike O'Brien, 21 July 2001

[4]. J. Sumida: Computer crime, London 1996

[5] M. Wasik, Crime and Computer, Oxford 1991

[5] Dr.Vesel Latifi, Criminology Pristina, 2004, p288

[6]. Don Parker: "Fighting Computer Crime", New York 1985

[6] Data from the General Directorate of Police, since 2011

[7]. Sieber Urlih, The International Handbook in Computer Crime, John Willey & Sons, since 1986

[8]. August Bequaj "How to Prevent Computer Crime", John Walleye & Sons, Inc., 1983

[9]. Dr.Vesel Latifi: Criminology Pristina, 2004

[10].Agency: Apis Security Consulting, 31.03.2004.

[11].Kriminalistika, Prof. Dr. Skender Begeja,Tirane 2005

[12]. M. Wasik, Crime and Computer, Oxford 1991

[13] D.Jovaševič , lexicon krivicnog prava, Belgrade 2000