Law Review ● vol. VII, issue 2, July-December 2017, pp. 66-71

LEGAL PROVISIONS REGARDING THE JUDICIAL ANALYSIS OF COMPUTER FORGERY AND COMPUTER FRAUD

Senior Lecturer PhD Maria-Magdalena BÂRSAN
Transilvania University, Department of Law
E-mail: maria.m.barsan@unitbv.ro

Abstract

The current article aims to analyze the legal provisions regarding the Criminal Code regulation of computer forgery and computer fraud. At the beginning of this study we will point out some general notions regarding the concept of computer forgery. The analysis will further present a comparative study of these two crimes as regulated in the Criminal Code and in special laws. According to the new Criminal Code provisions, the lawmaker regulated in Title II, Chapter IV named " Fraud committed through computer systems and electronic payment means", the crime of computer fraud (article 249 Criminal Code); the regulating text of this crime is the adjusted version of the one found in Law no 161/2003. Title VI, Chapter III named "False statements" and it regulates the crime of computer forgery as stated in article 48 of Law no 161/2003 regarding a series of measures to ensure transparency in exercising public office, public functions and sanctioning of corruption. In the end, we will list a practical section and we will provide examples.

Key words: *cyber crime, computer forgery, computer fraud, computer data, computer system, computer software.*

Introduction

In an age where all areas of activity are conducted on computers, we can't imagine our daily life without the presence of a computer, an indispensable tool for daily activities. The computer is currently used in contemporary society in all police stations in urban and rural communities, in crime laboratories, in all judicial analysis and statistics offices, in all authorities which fight cyber crimes, in courts of law, in all institutions of the state, thus providing data bases of diverse information. The technological revolution in computer science created several advantages in all areas of social life; at the same time, this evolution caused a series of social, economic and legal issues. The appearance of computers created the possibility of committing crimes regulated by criminal law.

Committing such antisocial deeds, as regulated by criminal law, with the use of computers, with the purpose of creating prejudice to people or companies represents a real social danger. The first laws against cyber crimes regulated provisions against acts of unjust access to data bases, unauthorized use of a

computer, fraud, sabotage, forgery. However, these crimes are just a small part of possible crimes which can be committed by using a computer, as time has proven that other crimes can be committed with the use of a computer; we mention the most common ones: computer fraud, drug traffic, selling illegal weapons, child pornography, computer forgery, but also some crimes regarding environmental protection.

We can state that cyber crimes are international crimes as they know no boundaries; such crimes can be committed on the territory of one country but cause effects on another country's territory; in such situations, international cooperation is vital in order to fight this rod.

However optimal we consider protection for the automated handling of data, regardless of how many protection tools are implemented and activated, we must be convinced that, one way or another, sooner or later, these tools of protection are to be deteriorated and those who commit such crimes will succeed. In the fight against cyber crime, there is a surprising phenomenon: while there is sustained effort to increase the security of computer systems and to discover new means to prevent attacks from unauthorized people, the so-called "maniacs" of computers permanently discover new means and new techniques of attack. The attack of a hacker does not entail only internet connected computers. He acts on any computer which is connected to a network and does not have a strong security system. Computer science, being so diverse and in permanent change and evolution led to a diversity of abuse by automated handling of computer data; thus the number so such crimes increased significantly.

The black number of cyber crimes is the result of several causes, among which" the sophisticated technology used by criminals; lack of adequate training for police officers; lack of a concentrated plan of reaction from the victims of such crimes in case of "attacks", a situation which makes it impossible to estimate the loss; the lack of adequate internal legislative instruments which must be actualized from time to time depending on the time frame and speed of this developing rod; the defective prioritization of the research operation of computer crimes.

One of the oldest protection measures is the technique of using a password when entering a system, an application or simply for reading important information. The password, as means of limited access to certain files and apps, is frequently used in order to ensure the security of information. However, it is not an infallible tool. Judicial practice shows that, for those who commit cyber crimes, the password does not represent an obstacle, as they can decrypt it.

Along with technological evolution, contemporary society faces a series of issues which created real possibilities of committing crimes against the patrimony, crimes which are diverse and multiplied. The number of such computer crimes is increasing permanently, an issue which has drawn attention of all worldwide countries. Acknowledging the social danger of cyber crimes has drawn incrimination of these deeds in most states of the world.

As a result, on an international level, the European Council initiated a series of regulations regarding cyber crime. Similarly, the Romanian lawmaker incriminated in the second title, chapter IV of the Criminal Code "patrimonial fraud committed with the use of computer systems and electronic means of payment". The text regulating the crime of computer fraud, as stated in article 249 of the Criminal Code represents an adjustment of article 49 of Law no 161/2003[1], as the only difference is the one regarding the sanctions; title VI generically called "Forgery crimes", in chapter III "Document forgery" incriminates in article 325 of the Criminal Code, the crime of computer forgery, thus corresponding to the provisions of article 48 of Law no 161/2003.

On November 23rd, 2001, member states of the European Council have drafted and signed the "Convention on cyber crime". Subsequently, on January 28th, 2003, all member states signed "The additional protocol for the convention on cyber crime for the incrimination of racial and xenophobic crimes committed with the use of computer systems".

Romania signed this additional protocol on October 9th, 2003. The Convention and the Additional Protocol establish the background for investigating and criminally sanctioning computer crimes, as well as interstate cooperation, necessary for ending this rod. The Convention emphasizes the necessity of criminally regulating deeds such as: illegal access to a computer system, the illegal intercept of computer transmissions, computer forgery, computer fraud, internet child pornography, violation of property rights and other connected rights and so on.

The Romanian Parliament attempted to pass these directives by Law no 161/2003 regarding some measures for ensuring transparency in exercising public offices and in business environment, the prevention and sanction of corruption.

In fighting cyber crime, we need a strong legislative background in regard to the prevention, discovery and sanction of these deeds. Through the international Conventions adopted as law, Romania is forced to develop a legislative system specific for these types of crimes. Law no 161/2003 was the first step; subsequently the lawmaker incriminated these deeds in the Criminal Code but, in order to maintain the same rhythm of the fast and diverse evolution of these crimes, the legislative activity must not stop.

In continuing with this article, I would like to analyze, from a judicial-criminal perspective, the crimes of computer fraud and computer forgery, as regulated by the provisions of the Criminal Code and special laws.

The crime of *computer fraud* is regulated in article 249 of the Criminal Code and article 49 of Law no 161/2003. The text of the Criminal Code states the following: "the deed of causing a patrimonial prejudice to a certain person by entering,

[1] Law no 161/2003 regarding a series of measures to ensure transparency in exercising public office, public functions and the sanctioning of corruption, published in the Official Bulletin no 279 of April 21st, 2003, with subsequent changes.

altering or deleting computer data, or by restricting access to these information or hindering in any way, the normal functioning of a computer system in order to obtain a material benefit for oneself or for another, is a crime and shall be punishable by no less than 3 years and no more than 12 of imprisonment"; article 249 of the Criminal Code states the following: "entering, altering or deleting computer data, restricting access to such data or hindering in any way the operation of a computer system in order to obtain a benefit for oneself or another, if it has caused damage to a person, shall be punishable by no less than 2 and no more than 7 years of imprisonment".

For a better understanding of the terms of this crime, I believe it would be useful to mention the definitions of certain terms used by the special law, which were subsequently introduced in article 181 of the Criminal Code. According to the provisions of Law 161/2003, a **computer system** is any device or an ensemble of devices which are interconnected of in a functional relation, among which one or more ensure the automated handling of data, with the help of a computer program"; **computer data** is any representation of facts, information or concepts in a form which can be handled by a computer system. This includes any computer program which can help a computer system function.

By committing this crime, the patrimony of a person or a company suffers a prejudice, which can be caused either by the counterfeiting and altering of computer data, by restricting access to it or by hindering, in any way, the normal functioning of a computer system. I believe that, even though the active subject of this crime can be any person who is criminally liable, still only one person with certain qualification in computer systems or a person who, by the nature of their job, has access to certain data and computer systems, can commit this crime.

The lawmaker lists, within the legal text, the means by which this crime can be committed, which we will discuss as follows. *Entering computer data* entails the action of inserting computer data in a computer system which belongs to another person, data which did not exist before in that computer system.

Altering computer data is the action of the perpetrator of entering or deleting certain information or parts of computer data which result in producing new computer data.

Deleting computer data is the perpetrator's action of eliminating, completely or partially, certain data stored in a computer system. To the same extent, we know that modern technology allows for data retrieval from certain storage devices which were destroyed or formatted. Deleting data can mean the same as destruction of data and, among the most dangerous means of deleting or destroying data, we mention computer viruses[2].

Restricting access to computer data entails the perpetrator acts on system storage device, so as the rightful user (a person or a company) can no longer retrieve data

[2] I. Vasiu, Judicial computer science and informatics law, Albastra Publishing House, 2007

in its original state. Computer data can no longer be accessed by the rightful user and he can no longer use this data. The most dangerous tools which can alter computer data are viruses or Trojans which can reproduce and endanger other programs or files by turning them in destructive programs.

The *hindering of the normal functioning of a computer system* entails the exercise of any action by the perpetrator, likely to lead to the partial or total, permanent or temporary impossibility of the rightful user to use that certain system.

The crime of computer fraud is only committed with direct intent, qualified by purpose, as the perpetrator aims, by exercising certain actions on a computer system, to obtain a material benefit for oneself or for another person, regardless of whether this benefit was actually achieved, by this causing a patrimonial prejudice to a person.

Also, it is good to know that, in order to ensure adequate protection when working with computer systems but especially stored computer data, a series of security measures are recommended. In article 35 of the law, letter h the lawmaker defines security measures by using procedures, devices or specialized computer programs designed for restricting or forbidding access to a computer system for certain users.

A typical case of computer fraud is the deed of the person who changes the information of a bank's data base thus determining the transfer of money from one person's account to his own account.

The crime of *computer forgery* is regulated in article 48 of Law no 161/2013 and the provisions of article 325 of the Criminal Law. The text of law states the following: "the unlawful inputting, alteration or deletion of computer data, or unlawful restriction of access to such data, resulting in inauthentic data, to be used to produce legal consequences, constitutes an offense and shall be punishable by no less than 2 and no more than 7 years of imprisonment".

The lawmaker lists the alternative means of committing this crime, namely the action of inputting, alteration or deletion of computer data, or the unlawful restriction of access to such data. In order to understand these means of committing the crime, we emphasize to previously mentioned explanations regarding computer fraud.

The lawmaker also points out that it is necessary that the perpetrator's action on computer data was unlawfully executed, as if this condition is not met, the deed will not be considered a crime. Also, using the computer data is not necessary; obtaining such data in order to achieve a purpose, namely that of using data in order to cause legal consequences.

A typical case of computer forgery was that of Patrick J. Schleibaum, former financial director of the disk storage company Miniscribe Corp. He was found guilty of forging the financial results of the company and using fake data in order to obtain a better position for his company on the stock market.

Conclusions

At the end of this article, I would like to emphasize the ampleness to this criminal phenomenon, a thing which was demonstrated by judicial practice which continues to record more and more cases of computer fraud or computer forgery. I believe we must be aware of the danger of such acts committed with the help of computers and with serious consequences in the social environment. In an age of information and technology, the computer is an absolute necessity and those who commit crimes with the help of a computer aim to take revenge, to harm a competitor and draw public attention.

Bibliography

1. M.Dobrinoiu, *Computer crimes*, C.H. Beck Publishing House, Bucharest, 2006

2. M.A. Hotca, M. Dobrinoiu, *Crimes regulated by special laws*, C.H. Beck Publishing House, second edition, Bucharest, 2010

3. I.Vasiu, *Prevention of computer crimes*, Hamangiu Publishing House, Bucharest, 2006

4. Romanian Criminal Code, Law no 286/2009 regarding the Criminal Code, published in the Romanian Official Bulletin, part I, no 510 of July 24th, 2009.

5. P. Rau, *Computer crime*, 2001

6. I.Vasiu, *Judicial computer science and informatics law,* Albastra Publishing House, Bucharest, 2007

7. C.Voicu, Al. Boroi, *Business criminal law,* third edition, C.H. Beck Publishing House, Bucharest, 2006

8. V. Dobrinoiu, M.A. Hotca, M. Gorunescu, M. Dobrinoiu, I. Pascu, I. Chis, C. Paun, N. Neagu, M.C. Sinescu, *Comments of the new Criminal Code, Special Part,* second volume, Universul Juridic Publishing House, Bucharest, 2012