DE GRUYTER OPEN

International Conference KNOWLEDGE-BASED ORGANIZATION
Vol. XXI No 2 2015

COMPUTER RELATED FORGERY, BETWEEN CONCEPT AND REALITY

Silviu JÎRLĂIANU

"Dunărea de Jos" University, Galaţi, Romania
jirlaianu@yahoo.com

Abstract: *The reality today proves beyond any doubt a manifestation of an exacerbation of cybercrime in all its manifestations, the most common being those of unauthorized access to a computer system, theft of confidential data and their use for criminal purposes, modification of websites without permission from holders and others. Computer forgery is a criminal offense stipulated in the current Romanian Penal Code, the art. 325 and covers an area of specialized crime – acts committed in this context are likely to harm the production of materials, with very high costs and sometimes difficult to recover. In this case, combating or preventing the committing of such crimes represents a necessity of our days.*

Keywords: computer forgery, computer crime, computer system, prevention.

1. Introduction

The latest publicly accessible activity reports, presented by the General Inspectorate of the Romanian Police and by the Directorate for the Investigation of Organized Crime and Terrorism Offences, confirm that the outbreak of crimes committed by ways of unlawfully accessing a computer system, using the internet to commit various crimes and frauds, cards skimming, theft of personal information and others, is a confirmed fact. Persons specialized in the use of computers increasingly commit criminal acts and the damages resulted are not to be neglected.

It is however noted that the facts, punishable under the current Penal Code which fall within computer-related offenses, are dangerous to society. For this reason the legislator felt the need to attach it under serious offences, and thus, severe sanctions, up to and including imprisonment, need to be applied in order to repress it.

It is known that introduction within the sphere of crime of some acts which were found to bring serious damage to the social relationships protected by the State is the result of strong signals coming from within the society, which requires the law authority, the penal regulation of these acts. Computer forgery, in its regulated form, is one example of this kind of offense.

Such an act had been punished until 2012, after which the offense was no longer considered as being a criminal offense when the current Penal Code was introduced.

2. Legal classification and penalty

Thus, in article 325 of the Penal Code, legally named ***Computer Forgery*****,** the act of *unlawfully inserting, altering or deleting computer data or of restricting the access to these data, resulting in false data with the purpose of issuing a legal outcome*, is considered a criminal offence and is punished with imprisonment from one to five years.

This article was newly introduced in the Penal Code, a previous regulation being

DOI: 10.1515/kbo-2015-0075

identified in article 48 from Law no. 161/2003 on some measures that ensured transparency and public exercise of senior civil service and in business environment, corruption preventing and punishing. This last article is currently abrogated [1].

A part of the criminal doctrine considered that it is correct to place computer forgery under forgery crimes, arguing that there will be more and more cases in which forgery is performed in a virtual, electronic space involving the use of a wide range of equipment or computer programs.

We are of the opinion that including this offense within forgery offenses can be argued upon, being more appropriate to include it under chapter IV from the Penal Code *Crimes against integrity and safety of computer systems and data.*

We base our opinion on the fact that this offense, by the very way in which it is committed, implies above average social skills and technical knowledge regarding the use of computers, knowledge regarding accessing protected data and information, altering and implicitly forging it with the purpose of obtaining some intended results.

In terms of punishment, it falls into line with the general penalty system of the current Penal Code, thus observing a reduction in the limits of punishment, from two to seven years in prison in the previous regulation to one to five years in prison in the current regulation.

3. Content of punishment

As stipulated in the current Penal Code, the offense can be committed by one of the alternative ways, respectively introducing, altering or deleting computer data or restricting access to these data.

Tampering with computer data leads to the occurrence of negative effects on these data that are meant to affect their operating capacity, especially to show incorrect facts or situations; the person benefitting from these data is able to issue or show false documents or facts or even to forge authentic documents.

The following examples of this type of offense can be given:

- inserting, altering or deleting data from certain key fields from the databases of the Directorates for Personal Records, from the databases of banks, medical laboratories, institutes of research, institutes for public opinion survey etc.;
- changing, in any way, the Word documents by altering their content or even by completely removing them from the system's memory;
- unauthorized copying of confidential data on an external port;
- simulation of electronic mail;
- simulation of hyper-connections;
- Web simulation.

In most cases, good faith users are misled by certain emails that have been very carefully elaborated, and that are sent by electronic mail. Some of these are SPAM emails.

In other cases, the offenders try to hide their true identity, or the locations they are in, or borrow the identity of other people.

To deceive the good faith users, they use email addresses that need to be as reliable as possible, and most importantly, to be as close as possible to the email addresses that the attackers are trying to "clone".

Some of the best-known computer forgery methods, identified by the judicial system, both nationally and internationally, are:

- simulation of hyper-connections;
- Web simulation.

These types of cyber attacks are known under the name of PHISHING.

The technical explanation for this type of cyber attack might be:

- making fictional email accounts or simulating real accounts with the purpose of misleading the good faith users with regard to the identity of the sender;
- using a dedicated message with the direct intent of manipulating the good faith user and determining him to access, through a URL address

connection, a certain fake web page, under the control of the offenders;
- creating a false web page („mirrored", cloned), based on a real web page, and resulting in misleading the targeted victims who are sure that they can safely provide personal, financial or confidential data, which are later used for criminal purposes.

In essence, all of the above-mentioned methods lead to the conclusion that the offender might be investigated for computer forgery only in cases in which he alters the original web page by various counterfeiting methods and alters the content of the email header field, meant to mislead.

Another way of committing this crime is the one known under the name of PHARMING.

This is translated into inserting computer data into the tables that provide IP addresses to the targeted domain names. The purpose is to transfer the traffic of data to a user, from a legal/real resource to another, which is in most cases under the control of the criminals. This method mostly exploits software vulnerabilities of the DNS type servers (domain name system).

In order for the crime to exist, it is necessary that the offender should act ***unlawfully.*** The criminal doctrine explains this phrase as follows:

- the person is not authorized under the law or an agreement;
- the person exceeds the limits of authorization;
- the person does not have permission from the party concerned to use, manage or control a computer system, or to perform scientific research or any other operations in a computer system.

Examples of this kind of crime are:

a) One is considered to have been acted lawfully when, in exercising his work duties, duplicates the web page of the company he works in and loads it onto a server known as "*bait*" or "*honeypot*", with the purpose of identifying possible vulnerabilities of the system exploited through cyber attacks or studying the hackers' operating ways;
b) An offender might be investigated for computer forgery in cases when, by using a social networking website (e.g. Facebook), creates a fictional account in the name of another person, attaches a real or an altered photo in order to show indecent or provocative images accompanied by personal information, which, by their nature, may produce damage, even of judicial nature. In this situation this can also be investigated as identity theft.

4. Conclusions

In the future, this type of offense will give rise to a very high number of victims among the honest internet users, and the intervention of the representatives of the state should be able to combat these criminal manifestations.

The interventions having the purpose of combating criminal outcomes should be made by specialized personnel, the state institutions paying much attention to controlling this phenomenon. Computer system frauds may produce damage that are not to be neglected. One must take into account that these offenses are committed by specially trained criminals, being known the fact that the advanced use of computer systems cannot be accessible to anyone.

References

[1] Art. 48 was abrogated by paragraph 2 from art.130, Title II from Law no. 187 / October 24, 2012, published in the OFFICIAL MONITOR no. 757 from November 12th, 2012.

[2] URL address (uniform resourse locator) or LINK – address indicating to the internet Browser the location of the searched resource (web page, server).

Bibliography

The Penal Code, adopted by Law No. 286 from July 17th , 2009.

Vasile Dobrinoiu, Ilie Pascu, Mihai Adrian Hotca, Ioan Chiş, Mirela Gorunescu, Costică Păun, Norel Neagu, Maxim Dobrinoiu Mircea Constantin Sinescu, *The New Penal Code Commented, Vol.II, Special Part,* Legal Universe Publishing House, Bucharest, 2012, pp.722-726; 900-904.

Evaluations – Activities performed by the Romanian Police in 2013, pp. 22-23, retrieved from www.politiaromana.ro.

Activity report of 2014, pp.72-83, retrieved from www.diicot.ro.