Bulletin of the *Transilvania* University of Braşov
Series VII: Social Sciences • Law • Vol. 14(63) Special Issue
https://doi.org/10.31926/but.ssl.2021.14.63.3.25

SOME REMARKS REGARDING THE CRIMINALIZATION AND THE FORENSIC INVESTIGATION OF THE CRIME OF COMPUTER FORGERY IN THE ROMANIAN LEGISLATION

Adrian Cristian MOISE[1]

Abstract: *The article presents and analyzes issues related to the criminalization of the offence of computer forgery, provided by the Article 325 of the Romanian Criminal Code, as well as issues related to the criminalization of the offence of computer forgery in the main legal instrument in the field of combating cybercrime at the European level: the Council of Europe Convention on Cybercrime.*
Moreover, the article also mentions some aspects related to the criminalization of the crime of computer forgery in some countries of the European Union. Finally, this study also presents the main issues to be clarified in the forensic investigation process of the crime of computer forgery.

Key words: *cybercrime; computer forgery, investigation, criminalization, the European Union.*

1. Introduction

The crime of computer forgery is provided by the Article 325 of the Romanian Criminal Code, the legal text being the following: "The act of entering, modifying or deleting, without right, computer data or of restricting, without right, the access to these data, resulting in data inappropriate to the truth, in order to be used in order to produce a consequence legal, constitutes a crime and is punishable by imprisonment from one to five years". We note that the provisions of the Article 325 of the Romanian Criminal Code correspond in the text of the Article 7 of the Council of Europe Convention on Cybercrime, which deals with the crime of computer forgery.

The legal text of the Article 7 of the Council of Europe Convention on Cybercrime states: "Each Party shall adopt such legislative and other measures as may be necessary

[1] Spiru Haret University of Bucharest, Faculty of Juridical, Economic and Administrative Sciences, Craiova, adriancristian.moise@gmail.com.

to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches".

We emphasize that the crime of computer-related-forgery is a purpose-offence from the point of view of the manner of commission, this having an illicit purpose of a patrimonial nature (Savin, 2013, p. 238-239). The crime of computer forgery is stipulated by the Article 325 of the Romanian Criminal Code and is regulated in a single standard variant, which consists in the introduction, modification or deletion, without the right of computer data, as well as by the action of restricting without right access to these data, resulting in untrue data in order to be used in order to produce legal consequences.

The *input* of correct or incorrect computer data refers to the action of making of a false document. For example, the input of malicious codes, such as viruses and trojan horses leads to the action of modification of the computer data (The Explanatory Report to the Convention on Cybercrime, 2001, para. 61). Moreover, the term *alteration* means the modification of existing data (The Explanatory Report to the Convention on Cybercrime, 2001, para. 61). The action of *suppressing* of computer data refers to the actions that terminate the availability of the computer data (The Explanatory Report to the Convention on Cybercrime, 2001, para. 61).

The action of *deletion* of computer data refers to the actions that remove computer data from the information technology storage equipment.

2. The pre-existing Conditions

2.1. The object of the crime of computer forgery

The general legal object of the offence of computer forgery is represented by the social relations related to public confidence in the security and reliability of information systems, in the integrity and authenticity of computer data and in the modern process of storage and processing of computer data (The Explanatory Report to the Convention on Cybercrime, 2001, para. 81).

The special legal object of the offence of computer forgery refers to the protection of the legal interest of the owner, holder or legal user of the computer system or of the computer data that are stored in the respective computer system (Dobrinoiu &al., 2014, p. 668).

The material object of the crime of computer forgery consists in the computer data as they were defined by the Romanian legislator, as well as by the legislator of the Council of Europe Convention on Cybercrime. According to the provisions of the Article 181 (2) of the Romanian Criminal Code, computer data represents "any representation of facts, information or concepts in a form that can be processed by a computer system".

Also, according to the provisions of Article 1 (b) of the Council of Europe Convention on Cybercrime *computer data* means "any representation of facts, information or

concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function".

2.2. The subjects of the crime of computer forgery

The active subject of the offence of computer forgery can be any person who meets all the conditions to be criminally liable (Zlati, 2020, p.492).

The criminal participation in the case of the offence of computer forgery is possible in all its forms: co-author, instigation and complicity.

The passive subject of the offence of computer forgery is the natural or legal person who has been harmed by the forgery of the computer data. In the case of the crime of computer forgery, we also have a *secondary passive subject*, which is the owner, the right holder or the authorized user of the computer system (Zlati, 2020, p.497).

3. The Constitutive Content of the Crime of Computer Forgery

3.1. The objective side

The material element of the offence of computer forgery is achieved through an alternative action of entering, modifying, deleting computer data, or restricting access to this data.

We specify that the crime of computer forgery can be committed in the following forms: by inserting, modifying or deleting data from inside computerized bases of some public or private institutions; by copying computer data from an external computer data storage medium; by altering electronic documents, thus modifying or deleting some texts from those documents. In a more technical approach, we emphasize that the crime of computer forgery can be committed in the following ways: spam; identity theft; phishing.

Spam is defined as any unsolicited communication that is made through e-mail (Zlati, 2020, p.495). We note that the Council of Europe Convention on Cybercrime and the Romanian Criminal Code do not explicitly criminalize spam.

The legislators of the Council of Europe Convention on Cybercrime suggested that the criminalization of these acts should be limited to serious and intentional obstructions in communications.

Although spam is not expressly regulated in Romanian criminal law, we believe that this act, which is committed in cyberspace could be incriminated by the provisions of the Article 325 of the Romanian Criminal Code, which refers to the crime of computer forgery.

The term identity theft describes the criminal acts by which the offender fraudulently obtains and uses the identity of another person.

These criminal acts can also be committed through the use of information and communication technology, cases of identity theft committed through the Internet are widespread, based on sophisticated scams and create difficulties for law enforcement agencies when they investigate such acts (Moise, 2020, p.120).

In the case of identity theft, cybercriminals use social engineering techniques regarding the disclosure of identity information. Thus, cybercriminals can use social engineering techniques to persuade the victim to disclose personal information, such as bank account information and credit card data (Moise, 2020, p.122).

Regarding the crime of identity theft, we must emphasize that it is not necessary for the offender to obtain all the data related to the identity of the victim. Certain computer data, such as passwords, account data and information required to access the computer system, which are not elements of the legal identity of a person, provide the offender with the possibility to illegally access other personal computer data that are used to establish the identity of the victim.

The identity theft is used to prepare for subsequent criminal acts, such as computer fraud or computer forgery.

The crime of identity theft is not expressly regulated by the criminal legislation in Romania. However, we consider that the crime of identity theft could be incriminated by the Article 325 from the Romanian Criminal Code, which refers to the crime of computer forgery.

Phishing is a practice of sending fake e-mails, or spam, written to appear as if they had been sent by banks or other reputable organizations, with the intention of enticing the recipient to disclose important information, such as for example, usernames, passwords, account Ids and credit card PINs (Moise& Stancu, 2017, p. 243).

The term phishing covers not only obtaining user account details, but also access to all personal and financial data.

Typically, phishing attacks will lead the recipient to a Web page designed to simulate the visual identity of a target organization and collect personal information about the user, the victim having no knowledge of the attack. Obtaining this type of personal data is attractive to criminals because it allows attackers to play the role of their victims and carry out fraudulent financial transactions.

Therefore, victims often suffer significant financial losses or their entire identity is stolen, usually for criminal purposes (Moise& Stancu, 2017, p. 243).

Finally, phishing could be incriminated by the provisions of Article 325 of the Romanian Criminal Code, which refers to the crime of computer forgery, by the provisions of Article 249 of the Romanian Criminal Code which refers to the offence of computer fraud, as well as by the provisions of Article 244 of the Romanian Criminal Code, which refers to the crime of deceit, in the situation where the act of sending messages in order to obtain the identification data of an account or of a person causes damage.

We consider that phishing cases are very complex, from a technical-scientific point of view, as well as from the point of view of the means and methods used, the forensic investigation process considering a single crime, the crime of computer forgery.

In the specialty literature, it has been considered that there are only two activities that can be legally included in the crime of computer forgery, provided by the Article 325 of the Romanian Criminal Code (Dobrinoiu &al., 2014, p. 669): the falsification of an original web page and the counterfeiting of an e-mail address to produce untrue data and other legal consequences.

In the case of a counterfeit website, the legal consequence is the infringement of a copyright, for example the right of the owner of a website, the owner can be, for example, a public institution, etc.

In the case of the creation of an address or e-mail account by a certain person, using the name of a public institution or a multinational company, we emphasize that the use of this name does not produce any legal consequences for that person, while if the same person uses this e-mail account as a means of transmitting certain text or video message content for the recipient of the e-mail message to send or disclose certain passwords or other non-public personal data, then this action will have certain legal consequences, this fact being legally framed for the crime of computer forgery by the criminal investigation team (Dobrinoiu &al., 2014, p. 670).

Regarding the *immediate consequence*, it consists in obtaining computer data that do not have a correspondent in reality and thus creating a state of danger for the public trust in the authenticity and validity of computer data.

We also believe that untrue data that has been obtained must be able to produce immediate legal consequences by creating, amending or extinguishing legal relationships.

We emphasize that, between the activity of the cybercriminal and the immediate consequence caused must be *a causality link* that results from the materiality of the offence.

3.2. The subjective side

From the point of view of the subjective element, we mention that the computer forgery offence is committed only with direct intention, being qualified by the purpose.

Moreover, we appreciate that it is not necessary to use these computer data effectively, but only to obtain them in order to achieve the proposed purpose, namely, the use of data that does not correspond to the truth in order to produce legal consequences.

4. The Forms of the Offence of Computer Forgery

In the case of the offence of computer forgery, *the preparatory acts* and *the attempt* are possible, although these are not incriminated by the Romanian Criminal Code.

The consumption of the offence of computer forgery takes place when any of the normative variants contained in Article 325 from the Romanian Criminal Code (entering, modifying, deleting, restricting) was committed.

Hence, the offence of computer forgery is consumed when the material element is carried out and the socially dangerous result is produced.

Exhaustion of the offence of computer forgery takes place at the moment when the last act criminalised by law occurred.

The offence of computer forgery can be committed in continuous form.

5. Modalities

The offence of computer forgery presents the following normative modalities, according to the provisions of the Article 325 from the Romanian Criminal Code: input, alteration, deletion of computer data, and restriction of access to this computer data. To these normative modalities may correspond various fact modalities.

6. Sanctions

The punishment for the computer forgery offence is imprisonment from one to five years.

7. Regulation of the Crime of Computer Forgery in other Countries of the European Union

The offence of computer forgery is stipulated by the Article 323-4 of the French Criminal Code, Title II Other property offences, Chapter III Offenses against automatic data-processing systems. The text of the Article 323-4 provides the following: "Participation in a group formed or an association established regarding the preparation of one or more offences provided by Article 323-1 to Article 323-3-1, and which is demonstrated by one or more material actions, shall be punished with the punishment provided, respectively for this crime, or in case of several crimes the heaviest punishment shall be applied".

Also, another provision related to computer forgery is the one from Article 441-1 of Title IV Undermining public trust, Chapter I Forgery of the French Criminal Code.

Please note that we have remarked that spam and phishing are not expressly criminalized in French criminal law. The offence of computer forgery is criminalized in the German Criminal Code in Section 269, being defined as: "The act of any person who stores or modifies data with the intention of providing evidence so that a forged or falsified document exists after the data recovery process, or uses data stored or modified in such a way, will be punished by imprisonment until at 5 years or with a fine; (2) The attempt is punished; (3) Section 267 (3) and (4) shall apply mutatis mutandis.".

Although the act of spam is not expressly criminalized in German criminal law, I have noticed that the act of phishing is expressly criminalized in Sections 202b and 202c of the German Criminal Code. Thus, according to Section 202b of the German Criminal Code, "any person who unlawfully intercepts data for himself or another person by technical means from a non-public data processing device, or from an electromagnetically transmitted data processing facility, shall be punished with imprisonment for up to two years or with a fine, unless the deed is punished more severely, by violating other legal provisions".

Section 202c deals with preparatory acts for data espionage and phishing and provides the following: "Any person who prepares to commit an offense in accordance with Section 202a and Section 202b by producing, obtaining for himself or for another, selling, supplying to another person, disseminating: 1. passwords or other security

codes that allow access to data; or 2. software for the purpose of committing such an offence, shall be punished by imprisonment for up to one year or by a fine".

8. Aspects related to the Forensic Investigation of the Crime of Computer Forgery

In case of committing crimes of computer forgery, according to the provisions of Article 288 paragraph 1 of the Romanian Criminal Procedure Code, the competent criminal investigation bodies must be notified in the following ways: complaint or denunciation, by acts concluded by other finding bodies provided by law or they are notified *ex officio*. The criminal investigation phase in the case of the offences of computer forgery is carried out by the Service for Combating Cybercrime within the Directorate for the Investigation of Organized Crime and Terrorism of the Prosecutor's Office attached to the High Court of Cassation and Justice of Romania.

The main issues that need to be clarified in the forensic investigation of the crimes of computer forgery refer to the following aspects (Moise&Stancu, 2017, p. 249): identification of digital and physical evidence; identifying the team members participating in the investigation; identifying the tools necessary for the forensic investigation of the crime of computer forgery; identification of the offender and of the circumstances that favored the commission of the crime of computer forgery; establishing the legal and jurisdictional issues in connection with the commission of the crime of computer forgery. Before starting the process of investigating the crime of computer forgery, the investigator must first establish the legal classification of the deed, and then establish the jurisdiction to investigate the criminal case (Shipley&Bowker, 2014, p. 16-17).

Regarding the legal framework of the investigated deed, the investigator must take into account both the criminal provisions contained in the Romanian Criminal Code and the criminal provisions contained in special laws, such as laws on the processing of personal data and the protection of confidentiality in the electronic communications sector, laws on the protection of copyright and related rights, etc (Moise& Stancu, 2017, p. 250). The forensic investigation process of the offences of computer forgery requires the use of specific tools: software tools and hardware tools. We underline that the forensic team of investigators must have data storage media, in sufficient quantity and of superior quality, to allow this data to be copied from the analyzed computer system (Schjolberg& Ghernaouti-Helie, 2011, p. 58-59).

We highlight the very important role of the forensic laboratory for the investigation of the computer forgery offences in the forensic investigation process.

9. Conclusions

Following the analysis, we noticed that the provisions of Article 7 of the Council of Europe Convention on Cybercrime, relating to the crime of computer forgery have been fully transposed into the Criminal Codes of Romania, France and Germany.

We believe that with the changing of technologies and criminal behavior, criminal law must also adapt to these new changes, and it is also necessary to update the Council of

Europe Convention on Cybercrime with the new offences that have emerged since its entry into force, such as, for example, spam, identity theft and phishing.

We therefore consider that the legislators of the Council of Europe Convention on Cybercrime should complement its provisions, in order to establish a legislative framework based on a specific provision relating to the protection of information, especially in relation to identity, therefore covering the identity theft committed through the Internet. I propose that the Romanian legislators complete the Romanian Criminal Code as soon as possible with the new types of cybercrimes: spam, phishing and identity theft.

We believe that French legislators should explicitly criminalize the new types of cybercrimes in the Criminal Code: spam, phishing and identity theft.

I noticed that unlike Romania and France, Germany has explicitly criminalized phishing in the Criminal Code, and regarding spam, I propose that German legislators criminalize spam in the Criminal Code. The process of harmonization of the internal criminal laws of the Member States of the European Union on computer forgery crimes is a living phenomenon, in the sense that it is subject to continuous legislative changes, caused by the continuous development of the new technologies, which are creating new crimes in cyberspace.

Therefore, we believe that the process of the forensic investigation of computer forgery offences must adapt to the new types of threats in the field of cyberspace that arise as a result of the continuous development of information and communication technology.

References

Dobrinoiu, V., Pascu, I., Hotca, M. A., Chiş, I., Gorunescu, M., Neagu, N., Dobrinoiu, M., & Sinescu, M. C. (2014). *Noul Cod penal Comentat. Partea specială* [The new Criminal Code commented. The special part], Second Edition. Bucharest: Universul Juridic.

Moise, A.C. (2020). *Dimensiunea criminologică a criminalității din cybespațiu* [*The Criminological Dimension of Cybercrime*], Second Edition. Bucharest: C.H. Beck.

Moise, A. C., Stancu, Em. (2017). *Criminalistica. Elemente metodologice de investigare a infracțiunilor. Curs universitar* [Forensics. Methodological elements for the investigation of crimes. Academic course]. Bucharest: Universul Juridic.

Savin, A. (2013). EU Internet Law. Cheltenham, Glos: Edward Elgar Publishing Limited.

Schjolberg, S., Ghernaouti-Helie, S. (2011). *A Global Treaty on Cybersecurity and Cybercrime,* Second Edition. Oslo: AIT.

Shipley, T.G., Bowker, A. (2014). I*nvestigating Internet Crimes. An Introduction to Solving Crimes in Cyberspace*. Waltham, Massachusetts: Elsevier Inc.

Zlati, G. (2020). *Tratat de criminalitate informatică* [Cybercrime Treaty]. Volume I, Bucharest: Solomon.

The Explanatory Report to the Convention on Cybercrime, 2001, Retrieved 30 September 2021 from: http://conventions.coe.int/treaty/en/reports/html/185.htm.