ANALYSIS OF THE OFFENCE OF ILLEGAL OPERATIONS WITH COMPUTER DEVICES OR SOFTWARE IN ROMANIAN LEGISLATION

Adrian Cristian MOISE [*]

Abstract

The study performs an analysis of the offence of illegal operations with computer devices or software, provided by the article 365 of the Romanian Criminal Code. When performing the analysis of the offence of illegal operations with computer devices or software, it was taken into account the text in force of the offence of illegal operations with computer devices or software, provided by the article 365 of the Romanian Criminal Code, the provisions of the article 6 of the Council of Europe Convention on Cybercrime which refers to the misuse of devices and the provisions of the article 7 of the Directive 2013/40/EU on attacks against information systems, which refers to the tools used for committing offences.

The analysis aims to determine whether the texts of the article 6 (misuse of devices) of the Council of Europe Convention on cybercrime and the article 7 (tools used for committing offences) of the Directive 2013/40/EU on attacks against information systems were transposed in the article 365 of the Romanian Criminal Code.

By the article 365 of the Romanian Criminal Code, the Romanian legislator intends to limit the access to the tools (computer devices, programmes, passwords, access codes) allowing to commit the offences regulated by the articles 360-364 of the Romanian Criminal Code.

Key Words: *computer system, computer programme, computer data, cybercrime, computer applications, illegal operations with computer devices or software.*

JEL Classification: [K14]

1. Introduction

The offence of illegal operations with computer devices or software is provided by the article 365 from Chapter VI, entitled *Offences against the safety and integrity of computer systems and data* from the Romanian Criminal Code. The legal text states:

"(1) The act of the person that, without right, makes, imports, distribute or makes available, under any form:

a) computer devices or programmes conceived or adapted in order to commit one of the offences referred to in the articles 360-364;
b) passwords, access codes or other similar computer data allowing total or partial access to an information system, in order to commit one of the

[*] University Lecturer, PhD., Spiru Haret University of Bucharest, Faculty of Juridical, Economic and Administrative Sciences, Craiova, Romania; Attorney-at-law, Dolj Bar Association, Romania.

offences referred to in the articles 360-364, shall be punishable by imprisonment from 6 months to 3 years or by fine.

(2) Possession, without right, of a computer device, programme, password, access code or other computer data among those referred to in paragraph (1), in order to commit one of the offences referred to in the articles 360-364, shall be punishable by imprisonment from 3 months to 2 years or by fine."

By the article 365 (Picootti, Salvadori, 2008: 25-27) of the Romanian Criminal Code, the Romanian legislator intends to limit the access to the tools (computer devices, programmes, passwords, access codes) allowing to commit the offences regulated by the articles 360-364 of the Romanian Criminal Code.

2. The pre-existing conditions

2.1 The object of the crime

The special legal object is the social relations related to the trust in computer data, devices and software, for the correct and lawful use thereof, as well as for the proper and legal carrying out of the commercial operations in relation to them (Dobrinoiu, Pascu, Hotca, Chiş, Gorunescu, Neagu, Dobrinoiu, Sinescu, 2014: 851).

The material object of the offence of illegal operations with computer devices or software are the material entities (computer systems or data storage supports) in which are stored both computer programmes specially created or adapted for use as means for committing the cybercrimes provided by the articles 360-364 of the Romanian Criminal Code, as well as computer data that protect the computer system (passwords, access codes or other computer data).

2.2 The subjects of the crime

The active subject of the offence can be any person who fulfils the general conditions provided by the law for criminal liability.

Criminal participation is possible in all its forms: co-author, incitement and complicity.

The passive subject of the offence is the natural or legal person as rightful owners of the computer system, but also the owner or the holder of the copyright for hardware or software adapted for criminal purposes. At the same time, the passive subject will also be the natural or legal person holding the right or ownership of passwords, access codes or other such computer data that have been used to allow access to the computer system (Dobrinoiu, 2006: 203).

3. The constitutive content

3.1 The objective side

The material element consists of the variants provided for in paragraphs 1 and 2 in the following actions: production, import, distribution, making available

in any form, possession of tools specially designed or adapted for the purpose of committing offences against the safety and integrity of computer systems and data covered by the articles 360-364 of the Romanian Criminal Code (Dobrinoiu, 2006: 6). All these incriminated actions must be carried out without right.

Also regarding the material element of the offence, having regard to the provisions of the article 6 of the Council of Europe Convention on Cybercrime[1] which refers to misuse of devices and to the provisions of the article 7 of the Directive 2013/40/EU[2] on attacks against information systems, which refers to the tools used for committing offences, we can note that the Romanian legislator has failed to include in the category of criminalised acts of the action of *procurement for use* of these instruments in the text of the offence of illegal operations with computer devices or software, provided by the article 365 of the Romanian Criminal Code.

This action (*procurement for use*) is covered by the article 6 (1) (a) of the Council of Europe Convention on Cybercrime and by the article 7 of Directive 2013/40/EU on attacks against information systems (Schjolberg, Ghernaouti-Helie, 2011: 41-42).

However, instead of doing *procurement for use*, the Romanian legislator included the activity of *possession* of such instruments in the article 365 (2) of the Romanian Criminal Code.

We also noticed that the action of *sale* of such instruments specially designed or adapted for the purpose of committing offences against the safety and integrity of computer systems and computer data is not provided for in the provisions of the article 365 of the Romanian Criminal Code, as it is currently covered by the provisions of the article 7 of the Directive 2013/40/EU on attacks against information systems, but also in the provisions of the article 6 (1) (a) of the Council of Europe Convention on Cybercrime (Féral-Schuhl, 2010: 910).

Therefore, regarding the offence of illegal operations with computer devices or software provided by the article 365 of the Romanian Criminal Code, we underline that the provisions of the article 6 of the Council of Europe Convention on Cybercrime which refers to misuse of devices and the provisions of the article 7 of the Directive 2013/40/EU on attacks against information systems, which refers to the tools used for committing offences, have not been fully transposed into the text of the article 365 of the Romanian Criminal Code (Savin, 2013: 238). Thus, we propose *de lege ferenda* the modification of the provisions of the article

[1] The European Council Convention on cybercrime was adopted at Budapesta 23rd of November 2001. Retrieved 20th of November 2017 from: http://www.conve ntions.coe.int/ Treaty/EN/ Trea ti es/Html/185.htm The European Council Convention on cybercrime was ratified by Romania through the Law no. 64/2004, published in the Romanian Official Gazette no. 343 from the 20th of April 2004.

[2] Directive 2013/40/UE of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JAI, Official Journal of the European Union, 14.08.2013, L218/8.

65 of the Romanian Criminal Code by introducing the action of *sale* of these instruments specially designed or adapted for the purpose of committing offences against the safety and integrity of computer systems and data regulated by the articles 360-364 of the Romanian Criminal Code, because the action of *sale* of these instruments is a common way of committing the offence of illegal operations with computer devices or software.

Immediate consequence

The immediate consequence consists of a state of danger, of threat to the integrity, safety and availability of computer data or information systems by increasing the possibility of committing the offences provided by the articles 360-364 of the Romanian Criminal Code.

Causality link

There must be a *causality link* between the activity of the offender and the consequence that results from the materiality of the crime.

3.2 The subjective side

For the existence of the offence of illegal operations with computer devices or software, it is necessary that the act be committed with guilt. In this situation, the form of guilt necessary is both the direct and indirect intention (Vasiu, Vasiu, 2007: 144).

For the existence of the offence under the subjective aspect it is necessary to fulfil an essential condition: the actions described in paragraphs (1) and (2) shall be carried out for the purpose of committing one of the offences provided in the articles 360-364 of the Romanian Criminal Code (Hotca, Dobrinoiu, 2008: 602). Thus, in the absence of this purpose, this act will not be considered the offence provided by the article 365 of the Romanian Criminal Code.

4. The forms of the offence

The preparatory acts are possible, but they are not criminalised and thus they are not punishable.

The attempt is possible and is punished according to the article 366 of the Romanian Criminal Code.

The consumption of the offence of illegal operations with computer devices or software occurs at the time of production, import, distribution, making available or possession, without right, a computer device, computer program, password, access code or other type of computer data for the purpose of committing the offences provided by the articles 360-364 of the Romanian Criminal Code.

The exhaustion of the offence occurs at the time of committing the last act criminalised by law. The offence can be committed in continuous or continued form.

5. Modalities

The offence of illegal operations with computer devices or software presents five regulatory modalities, according to the provisions of the article 365 of the Romanian Criminal Code: producing, importing, distributing, making available in any form and holding without right a device, computer program, password, access code or other computer data.

To these normative modalities may correspond various fact modalities.

6. Sanctions

The punishment provided for this offence in the case of paragraph 1 of the article 365 is imprisonment from 6 months to 3 years or fine, and for the paragraph 2 of the article 365 the prescribed penalty is imprisonment from 3 months to 2 years or a fine.

7. Procedural Aspects

The criminal prosecution initiates ex officio.

Below, we will briefly analyze the offence of illegal operations with computer devices or software, considering the action of *sale* on the free market of certain devices or software that can be used to commit crimes against the safety and integrity of the systems and computer data provided by the articles 360-364 of the Romanian Criminal Code. Thus, in the literature (Dobrinoiu, 2010: 1-31); (Féral-Schuhl, 2010: 917-918) in the field of cybercrime, several situations have been presented and analyzed regarding the purchase from certain websites of software (Gercke, 2012: 33) specially designed for monitoring an information or communication system, with emphasis on both the criminal liability of the buyer, and on the criminal liability of the seller for such applications.

The first case concerns the computer device or software that, once purchased from a website, is installed by the buyer in his/her own computer system in order to monitor the online work of his/her children or his/her employees at work. In this case, the computer system of the person concerned is used in the family or at the workplace where the buyer is an employer. We believe that the person who bought such a computer program to monitor the online activity of their children or their employees did not commit any of the offences covered by the article 365 of the Romanian Criminal Code. In the situation where the purchaser of the computer device or software is in possession of computer data belonging to a family member, friend or employee who had access to the buyer's computer system, then we consider that he/she has committed with the form of guilt of direct or indirect intention the following criminal offences:

- the offence of illegal interception of a computer data transmission provided by the article 361 (1) of the Romanian Criminal Code;

- the offence of illegal operations with computer devices or software provided by the article 365 (2) of the Romanian Criminal Code.
- the offence of violation of the secrecy of correspondence provided by the article 302 (2) of the Romanian Criminal Code.

Regarding the criminal liability of the seller in the case presented above, we believe that the seller of such computer applications committed the offence of illegal operations with computer devices or software provided by the article 365 (1) (a) of the Romanian Criminal Code with the form of guilt of indirect intention, taking into account the following considerations:

- the seller knows the characteristics of the computer device or software presented on that website and also knows the possibility of illegal actions that may be committed with the help of the computer device or software;
- the seller foresee the result of his/her act and, although he/she does not follow it, accepts that by the sale of the computer device or software may be possible committed an offence;
- the sale of such computer devices or software designed or adapted for the purpose of committing cybercrimes must be carried out without right;
- the seller will try to prepare his/her defence, claiming that the buyer is solely responsible for the purpose for which the computer application is used as a result of the purchase from the website.

We consider that the seller of such computer devices or software has committed the offence of illegal operations with computer devices or software provided by the article 365 (1) (a) of the Romanian Criminal Code with the form of guilt of indirect intention, by the action of *making available in any form* of these computer applications, even if the action of *sale* of such computer applications is not expressly provided in the provisions of the article 365 of the Romanian Criminal Code.

A second case is that relating to the computer device or software that is presented on the website by the seller for sale in a way from which clearly results the purpose and the conditions of its use, such as, for example, a possible ad posted on a website: “the programme installed in the computer system of the person concerned will give you access to the content of the data transmitted or received by the person concerned without knowing it”. In this case, the seller of the computer device or software committed the offence of illegal operations with computer devices or software provided in the article 365 (1) (a) of the Romanian Criminal Code with the form of guilt of direct intention. Depending on the details of each situation, it is possible to retain the seller's liability and the criminal participation in committing other offences (for example, the offence of illegal interception of a computer data transmission, the offence of illegal access to a

computer system, the offence of violation of the secrecy of correspondence, etc.) in the form of incitement or complicity.

Conclusions

In conclusion, we believe that the seller sells the computer device or software, without right, only if, with the aid of these computer applications, the buyer, without right, commits the offences provided by the articles 360-364 of the Romanian Criminal Code (article 360- illegal access to a computer system; article 361- illegal interception of a computer data transmission; article 362- alteration of computer data integrity; article 363- hindering of the functioning of computer systems; article 364- unauthorized transfer of computer data).

The offence of illegal operations with computer devices or programmes criminalises acts similar to those referred to in the article 314[3] (2) of the Romanian Criminal Code. Due to the overlap of activities in the field of new technologies developed with a view to falsifying electronic payment instruments, in judicial practice was identified a concurrence of several offences in one action between the offence stipulated at the article 314 (2) of the Romanian Criminal Code in the modality of transmission of hardware and software equipments and the offence stipulated at the article 365 (1) (a) and (b) of the Romanian Criminal Code.

Taking into consideration the carried out analysis, we notice that the text of the article 365 of the Romanian Criminal Code which provides the offence of illegal operations with computer devices or software adapted to the provisions of the article 6 (misuse of devices) of the Council of Europe Convention on cybercrime and to the provisions of the article 7 (tools used for committing offences) of the Directive 2013/40/UE of the European Parliament and of the Council of 12 August 2013 on attacks against information systems. These two regulatory documents represent the most important legal instruments on preventing and combating cybercrime at the European Union level.

Moreover, we emphasize that the text of the article 4 (offences related to specifically adapted devices) of the Council Framework Decision 2001/413/JAI[4] of 28 May 2001 combating fraud and counterfeiting of non-cash means of payment was transposed too in the article 365 of the Romanian Criminal Code.

Bibliography

1. Dobrinoiu, Vasile; Pascu, Ilie; Hotca, Mihai Adrian; Chiş, Ioan; Gorunescu, Mirela; Neagu, Norel; Dobrinoiu, Maxim; Sinescu, Mircea Constantin (2014). *Noul Cod penal comentat. Partea specială*, Second Edition, Bucharest: Universul Juridic Publishing House, *in Romanian*.

[3] The article 314 (2) of the Romanian Criminal Code states: "Making, receiving, possession or transmission of equipments, including hardware or software, in order to serve for falsifying electronic payment instruments shall be punishable by imprisonment from 2 to 7 years".

[4] The Council Framework Decision 2001/413/JAI[4] of 28 May 2001 combating fraud and counterfeiting of non-cash means of payment, Official Journal of the European Union, 02.06.2001, L149/1.

2. Dobrinoiu, Maxim, (2010), *Operaţiuni ilegale cu dispozitive sau programe informatice*, article presented at Târgu-Jiu Workshop. Retrieved 20th of November 2017 from: http://www.legi-internet.ro/articole-drept-it.html#c162, *in Romanian*.
3. Dobrinoiu, Maxim, (2006), *Infracţiuni în domeniul informatic*, Bucharest: C.H. Beck Publishing House, *in Romanian*.
4. Dobrinoiu, Maxim, (2006), *Analiza infracţiunii de operaţiuni ilegale cu dispozitive sau programe informatice*, in Revista Română de Dreptul Proprietăţii Intelectuale no.4, *in Romanian*.
5. Féral-Schuhl, Christiane, (2010), *Cyberdroit. Le droit à l' épreuve de l' Internet*, Sixième Édition. Paris: Dalloz, *in French*.
6. Hotca, Mihai Adrian; Dobrinoiu, Maxim, (2008*), Infracţiuni prevăzute în legi speciale. Comentarii şi explicaţii*, Bucharest: C.H. Beck Publishing House, *in Romanian*.
7. Gercke, Marco, (2012), International Telecommunication Union, *Understanding Cybercrime: Phenomena, Challenges and Legal Response*. Geneva, Retrieved 20th of November 2017 from: www.itu.int/ITU D/cyb/cybersecurity/legislation.html.
8. Picotti, Lorenzo, Salvadori, Ivan, (2008), Council of Europe. Project of Cybercrime**,** *National legislation implementing the Convention on Cybercrime. Comparative analysis and good practices*, Strasbourg, Retrieved 20th of November 2017 from: http://www.coe.int/t/dghl/ cooperation/economiccrime/cybercrime/documents/reports-presentations/567%20study2-d-version 8%20_2 8%20 august %2008 .pdf.
9. Savin, Andrej, (2013), *EU Internet Law*. Cheltenham, Glos: Edward Elgar Publishing Limited.
10. Schjolberg, Stein, Ghernaouti-Helie, Solange, (2011), *A Global Treaty on Cybersecurity and Cybercrime*. Second Edition, Oslo: AIT.
11. Vasiu, Ioana, Vasiu, Lucian, (2007*), Informatică juridică şi drept informatic*, Cluj-Napoca: Albastră Publishing House, *in Romanian.*
12. The Council Framework Decision 2001/413/JAI[1] of 28 May 2001 combating fraud and counterfeiting of non-cash means of payment, Official Journal of the European Union, 02.06.2001, L149/1.
13. Directive 2013/40/UE of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JAI, Official Journal of the European Union, 14.08.2013, L218/8.
14. The European Council Convention on cybercrime.
15. The Romanian Criminal Code.