TECHNIUM
SOCIAL SCIENCES JOURNAL

Vol. 26, 2021

A new decade for social changes

www.techniumscience.com

ISSN 2668-7798

Technium Social Sciences Journal
Vol. 26, 944-949, December, 2021
ISSN: 2668-7798
www.techniumscience.com

Theoretical and practical considerations regarding the illegal access to a computer system in the Romanian Criminal Law

Zafer Sadîc

Ovidius University of Constanta, Romania – Faculty of Law and Administrative Sciences

Abstract. The article analyzes the legal framework for regulating the crime of illegal access to a computer system in the Romanian legal system, with a brief foray into the history of criminalization of unauthorized access to a computer system, continues with the indication of the normative text in force, after which it describes the structure and legal content of the crime, with specific references to recent relevant criminal jurisprudence.

Keywords. illegal access, unauthorized access, criminalization, computer system, computer data, criminal liability

1. History of crimination

The development of computer systems at the end of the second millennium has inherently created a favorable ground for the emergence of a new type of crime, of illicit activities carried out in the virtual world of computers, but which are likely to produce one of the most dangerous consequences, in the real world.

Cyber attacks have caused substantial damage globally, by shutting down or disrupting the functionality of information systems and telecommunications, by losing or altering confidential information of economic or socio-cultural value or other important data stored in the virtual environment.

The desire for effective protection of information systems and data generated or processed by them, both nationally and internationally, has required the creation of a complex framework of security and prevention measures for the unauthorized access to computer systems, including those provided by criminal law, in response to the phenomenon.

In Romania, Law no. 161/2003 on certain measures to ensure transparency in the exercise of public dignity, public office and in the business environment, the prevention and sanctioning of corruption[1] has for the first time criminalized the act of unauthorized access to a computer system, in Article 42:

(1) *Access, without right, to a computer system constitutes a crime and is punishable by imprisonment from 3 months to 3 years or by a fine.*

(2) *The act referred to in paragraph (1), committed for the purpose of obtaining computer data, shall be punishable by imprisonment from 6 months to 5 years*.

[1] Published in M.OF. no. 279 of April 21, 2003;

Technium Social Sciences Journal
Vol. 26, 944-949, December, 2021
ISSN: 2668-7798
www.techniumscience.com

(3) *If the act referred to in paragraph (1) is committed in breach of security measures, the penalty shall be imprisonment from 3 to 12 years*.

The text of the law has implemented a content of the crime according to the definition in the 2001 Budapest Council of Europe Convention on Cybercrime[2].

Article 2 of the Convention on Illegal Access stated that: "*Each Party shall adopt such legislative and other measures as may be necessary to criminalize, in accordance with its domestic law, the intentional and unlawful access of all or part of an information system. A party may make such an offense conditional on the breach of the infringement by breach of security measures, with intent to obtain computer data or other criminal intent, or by the connection between the breach and a computer system connected to another computer system*".

2. Normative regulations in force

With the entry into force on the 1st of February 2014 of the new Criminal Code[3], illegal access to a computer system was criminalized in Chapter VI of Title VII, entitled "*Crimes against the security and integrity of systems and data information technology*", which in Article 360 provided the following normative content:

(1) *Accesul, fără drept, la un sistem informatic se pedepseşte cu închisoare de la 3 luni la 3 ani sau cu amendă.*

(2) *Fapta prevăzută în alin. (1), săvârşită în scopul obţinerii de date informatice, se pedepseşte cu închisoarea de la 6 luni la 5 ani.*

(3) *Dacă fapta prevăzută în alin. (1) a fost săvârşită cu privire la un sistem informatic la care, prin intermediul unor proceduri, dispozitive sau programe specializate, accesul este restricţionat sau interzis pentru anumite categorii de utilizatori, pedeapsa este închisoarea de la 2 la 7 ani*.

It can be seen that the Romanian legislator intervened in defining the original incrimination text, by taking over in the third paragraph the explanations regarding the notion of security measures, which he expressly inserted, in order to ensure the quality of the law, in the light of European case law in the field of human rights and the recent judicial practice of the national constitutional court, explanations similar to the text of Directive 2013/40 / EU of the European Parliament and of the Council of 12 August 2013 on attacks against computer systems and replacing Framework Decision 2005/222/JAI of the Council[4].

3. Structure and legal content of the crime

In the structure of the crime we will submit to the analysis the legal object, the subjects and the legal content, respectively the premised situation, the objective typicality and the subjective typicality.

3.1.The legal object of the crime

The generic legal object is the social relations regarding the protection of the security, confidentiality and integrity of data and information systems[5].

The special legal object is the social relations that are born and develop in connection with the security of information systems.

[2] Council of Europe Convention of 23 November 2001 on Cybercrime, published in the M. OF. no. 343 of April 20, 2004.
[3] Law no. 286/2009 on the Criminal Code, published in the M.OF. no. 510 of July 24, 2009.
[4] Published in OJ L 218, 14.8.2013, p.8
[5] S. Bogdan (coordinator), D.A. Şerban, G. Zlati, *The New Criminal Code. The special part. Analyzes, explanations, comments.* The Cluj perspective, 2014, page 677.

Technium Social Sciences Journal
Vol. 26, 944-949, December, 2021
ISSN: 2668-7798
www.techniumscience.com

The material object can be a computer system or network, ie hardware (motherboard, server, cables, keyboard, mobile phone) or software (databases, applications, programs), against which the action of the perpetrator is directed.

3.2. Subjects of the crime

A directly active subject can be any natural or legal person who meets the general conditions of criminal liability. In practice, the perpetrator can only be an expert in the field of information technology[6].

Criminal participation is possible in all its forms (co-authorship, instigation or complicity).

The passive subject of the crime is the natural or legal person who owns or uses the computer system, but there may also be an adjacent passive subject who may suffer damage by accessing his personal data held or processed automatically by the computer system.

3.3. The premise situation

The premised situation of the crime of illegal access to a computer system presupposes the existence of a functional computer system or of some computer data that the perpetrator can access in his illicit action. It is possible that only one or more components of a computer system (devices, software, access codes, passwords, procedures) constitute the premise of this offense against the security of computer systems.

Jurisprudence: in a case in which he rejected as unfounded an exception of unconstitutionality of art. 360 para. (1) Criminal Code, the Constitutional Court of Romania has ruled that the legal provisions criticized are sufficiently clear, precise and predictable, meaning that the legislator has defined in unequivocal terms that unauthorized access to a computer system protected by security measures is prohibited, and the premise of the crime is the existence of the computer system or computer data[7].

3.4. The objective typicality of the crime

3.4.1. The material element, in the standard version, is the action of access to a *computer system*[8], ie the functional interaction, at a logical level, and not material, of the author with the targeted computer system, through peripheral control equipment (keyboard, mouse, touchscreen). Logical interaction means the ability of the perpetrator to give commands, to cause the introduction, obtaining, displaying, storing or disseminating computer data or otherwise using the resources of a computer, system or computer network or communicating with its arithmetic, logic or memory[9].

The penetration of information from the computer system can be done physically, but also remotely (intranet, internet) and through any type of connection (electric cable, telephone, optical, radio, satellite, etc.).

The Explanatory Report to the Budapest Convention of 2001 detailed the definition of the concept of computer system as a device composed of computer equipment and software, designed for automatic processing (without direct human intervention) of data (data from the

[6] ME. Hotca, M. Dobrinoiu, *Offenses provided in special laws. Comments and explanations*, vol. I, Bucharest, C.H. Beck, 2008, page 598.
[7] Decision no. 27 of January 19, 2021, published in the M.OF. no. 325 of March 31, 2021
[8] According to art. 181 of the Criminal Code, *computer system means any device or set of devices* interconnected or in a functional relationship, one or more of which ensures the automatic processing of data, using a computer program, and computer data means any representation of facts, information or concepts in a form that can be processed by a computer system.
[9] I. Vasiu, L. Vasiu, *Computer contaminants as a vector of illegal access*, article published in the Journal of Criminal Law, no. 2/2006, page 37.

Technium Social Sciences Journal
Vol. 26, 944-949, December, 2021
ISSN: 2668-7798
www.techniumscience.com

computer system are operated by a computer system, ie a set of instructions that can be executed by the computer to obtain the desired result). It has been stated that a computer can run various computer programs and may consist of different peripherals (a device that can perform various specific functions in interaction with the central unit, such as a printer, a video screen, or a CD reader / writer).), distinct from the central processing unit. At the same time, a network consists of the interconnection of two or more computer systems, and the interconnection can be common (via wires or cables) or wireless (via radio, infrared or satellite) or both.

Jurisprudence: The High Court of Cassation and Justice ruled in an appeal in the interest of the law[10] that the installation at an ATM of an autonomous device for reading the magnetic stripe of an authentic card and the corresponding PIN code (skimmer, mini-camcorder or keyboard device does not realize the typicality of the crime of illegal access to a computer system, as such activities do not represent a logical interaction with the bank's computer system and do not give the author the opportunity to give orders, cause entry, obtaining, display, storage or the dissemination of computer data or other use of computer system resources.

In the aggravated version from par. (2), the purpose of obtaining computer data can be materialized by viewing them on the screen and downloading (transferring information) or copying them on various media (magnetic, optical, printing on paper, etc.).

In the aggravated version from par. (3), the action of access by violating security measures (procedures, devices or specialized programs by which access is restricted or prohibited for certain categories of users) can be achieved by forcing or circumventing these measures, which may be physical (isolation of the computer system in a secure place with mechanical protection devices, video surveillance cameras, motion sensors) or logic (data encryption, passwords, codes, etc.).

Jurisprudence: *Accessing a person's Facebook account, using the e-mail address and password without the consent of the holder, is an aggravated form of the crime of illegal access to a computer system*[11].

3.4.2. The **essential requirement** for achieving the objective typicality of the crime is that the access take place without right, in the sense given by art. 35 paragraph (2) of Law no. 161/2003:

- without authorization under the law or a contract;
- by exceeding the authorization limits;
- without the permission of the competent person to use, administer or control a computer system or to carry out scientific research or to carry out any other operation in a computer system.

Jurisprudence: *It has been ruled in the practice of several courts in Romania that the following actions meet the typical conditions of the crime of illegal access to a computer system*:

- use of a bank card without the consent of its holder[12];
- transfer of sums of money to one's own account by using the passwords of a device belonging to the perpetrator's spouse without consent[13];
- the use of a deceased person's card for withdrawing money at an ATM, without the bank being informed about the holder's death[14].

[10] Î.C.C.J., the panel competent to judge the appeal in the interest of the law, decision no. 15/2013, published in the M.OF. (Official Gazette). no. 760 of December 6, 2013.
[11] Arad Court, criminal sentence no. 38/2019, published on http://www.rolii.ro, accessed on 1.06.2021.
[12] Dolj Court, criminal sentence no. 588/2018, published on http://www.rolii.ro, accessed on 3.06.2021.
[13] Dâmbovița Court, criminal sentence no. 670/2017, published on http://www.rolii.ro, accessed on 3.06.2021.
[14] Î.C.C.J., Criminal section, decision no. 19 / A / 2020, published on http://www.scj.ro., accessed on 30.05.2021.

Technium Social Sciences Journal
Vol. 26, 944-949, December, 2021
ISSN: 2668-7798
www.techniumscience.com

3.4.3. Immediate follow-up

Being a dangerous crime, the immediate consequence is to create a state of danger for the general security of computer systems and data. In the case of aggravated forms, the state of danger refers to the confidentiality and protection of computer data processed and stored in the memory of affected computer systems or to additional security measures, protection of computer systems and data, thereby enhancing their security.

Jurisprudence: A decision of the Supreme Court[15] stated that the immediate consequence of the crime of illegal access to a computer system is the transition to a state of insecurity of the computer system and / or its resources, and if the purpose of unauthorized access was to obtain computer data, the insecurity of the system is doubled by the insecurity of the computer data stored or processed by it.

3.4.4. **The causal link** between the perpetrator's action and the consequence produced must have existed and results from the very materiality of the deed (ex re) in the case of the simple form, and in the case of aggravated forms this connection must be proved.

3.5.Subjective typicality

In the simple form of the crime, the act is committed with guilt in the form of direct or indirect intent.

In aggravated variants, the subjective typicality is achieved if the deed is committed with guilt in the form of direct intention, qualified by the purpose pursued by the perpetrator.

Jurisprudence: The act of using a person's username and generic password of another person on the Smart Mobile application to make unauthorized transactions in his / her bank account constitutes the crime of illegal access to a computer system, committed with direct intent[16].

4. Forms and modalities of the crime

Being a commissive, dangerous crime, the access to an information system is consumed when the perpetrator can benefit from the resources or functions of the information system that he has accessed without authorization.

The preparatory acts are possible, but they are not punished, but in certain circumstances they may constitute the crime of possession of instruments in order to falsify values, provided by art. 314 Penal Code.

The attempt is possible and is punished in all forms of crime, in accordance with the provisions of art. 366 Penal Code.

The deed provided by the criminal law may take the form of a continuous or continuous crime, and may have an initial moment of consumption and a later moment of exhaustion of the illicit activity.

The three normative ways in the incriminating text can be accomplished in a multitude of factual ways.

Jurisprudence: The Supreme Court held in the appeal decision in the interest of law no. 15/2013, mentioned above, that illegal access to a computer system is usually made for the purpose of committing one or more of the crimes related to electronic commerce, a situation

[15] ICCJ, the panel for resolving legal issues in criminal matters, decision no. 2 of January 20, 2021, published in the M.OF. (Official Gazette). no. 293 of March 24, 2021

[16] Bucharest Military Tribunal, criminal sentence no. 84/2020, published on http://www.rolii.ro, accessed on 1.06.2021.

that justifies the retention of a contest with etiological connection, in which illegal access is the means by which the purpose is to perform fraudulent financial transactions.

5. The penalty regime

In the case of the standard form of crime, illegal access to a computer system is punishable by imprisonment from 3 months to 3 years, alternatively with the penalty of a fine.

In the case of aggravated variants, the law establishes exclusively the prison sentence, in the form provided in par. (2) the punishment being imprisonment from 6 months to 5 years, and in the form provided in par. (3) the punishment being imprisonment from 2 to 7 years.

References

[1] Published in M.OF. no. 279 of April 21, 2003;
[2] Council of Europe Convention of 23 November 2001 on Cybercrime, published in the M. OF. no. 343 of April 20, 2004.
[3] Law no. 286/2009 on the Criminal Code, published in the M.OF. no. 510 of July 24, 2009.
[4] Published in OJ L 218, 14.8.2013, p.8
[5] S. Bogdan (coordinator), D.A. Şerban, G. Zlati, The New Criminal Code. The special part. Analyzes, explanations, comments. The Cluj perspective, 2014, page 677.
[6] ME. Hotca, M. Dobrinoiu, Offenses provided in special laws. Comments and explanations, vol. I, Bucharest, C.H. Beck, 2008, page 598.
[7] Decision no. 27 of January 19, 2021, published in the M.OF. no. 325 of March 31, 2021
[8] According to art. 181 of the Criminal Code, computer system means any device or set of devices interconnected or in a functional relationship, one or more of which ensures the automatic processing of data, using a computer program, and computer data means any representation of facts, information or concepts in a form that can be processed by a computer system.
[9] Vasiu, L. Vasiu, Computer contaminants as a vector of illegal access, article published in the Journal of Criminal Law, no. 2/2006, page 37.
[10] Î.C.C.J., the panel competent to judge the appeal in the interest of the law, decision no. 15/2013, published in the M.OF. (Official Gazette). no. 760 of December 6, 2013.
[11] Arad Court, criminal sentence no. 38/2019, published on http://www.rolii.ro, accessed on 1.06.2021.
[12] Dolj Court, criminal sentence no. 588/2018, published on http://www.rolii.ro, accessed on 3.06.2021.
[13] Dâmbovița Court, criminal sentence no. 670/2017, published on http://www.rolii.ro, accessed on 3.06.2021.
[14] Î.C.C.J., Criminal section, decision no. 19 / A / 2020, published on http://www.scj.ro., accessed on 30.05.2021.
[15] ICCJ, the panel for resolving legal issues in criminal matters, decision no. 2 of January 20, 2021, published in the M.OF. (Official Gazette). no. 293 of March 24, 2021
[16] Bucharest Military Tribunal, criminal sentence no. 84/2020, published on http://www.rolii.ro, accessed on 1.06.2021.