sciendo
JOURNAL OF LEGAL STUDIES
"Vasile Goldiş" Western University of Arad
J. L. S.
2019 – 23(37)
DOI: 10.2478/jles-2019-0003

ILLEGAL ACCESS TO A COMPUTER SYSTEM FROM THE STANDPOINT OF THE CURRENT CRIMINAL CODE

Alin Teodorus Drăgan *
"Vasile Goldiş" Western University of Arad, Romania, e-mail: alinteodorus@yahoo.co.uk

(Received: February 2019; Accepted: April 2019; Published: June 2019)

Abstract: One of the forms that cybercrime can take at present is illegal access to a computer system. From the very beginning, the world of computers and of the Internet was based on imperfections, defects, and sometimes on poorly understood processes. We might even call this fact "the original sin" of the Internet. In the end, it is not only computer scientists who have come to exploit such defects, but also criminals. In the real world, there are people who break into homes and take away everything they find valuable. In the virtual world, there are individuals who penetrate into computer systems and steal all valuable data.

Keywords: computer system, computer data, software, illegal access.

1. Introduction

The modern practice of putting so much personal and financial information on computers, on data storage devices and online has turned data theft into a much easier to commit and, therefore, more profitable crime. It is much safer and more convenient for the offender, since, by illegally accessing a computer (IT) system, he/she can assume the identity of someone else, located on the other side of the world, thus reducing the chances of being caught to almost zero. Computer systems are not only the target of certain crimes, but also the instrument by which other crimes are committed, or they simply facilitate through their features the commission of traditional crimes.

Computer systems play a vital role in modern organizations because they provide the necessary information and the processing and dissemination capacities that are strictly needed in order to meet functional/operational requirements, regardless of context or field of activity [1].

*Corresponding author: Alin Teodorus Drăgan. *E-mail: alinteodorus@yahoo.co.uk*

The cybercriminality phenomenon consists, in a narrower sense, of deeds that are strictly directed against computer systems or the data they contain, whereas, in a broader sense, it may also include behaviours circumscribed by the notion of computer-related criminality [2].

Up until now, the law has dealt with tangible goods, because the real world used to consist of tangible items: however, at present, an actual process of "dematerialization" is under way, with the progressive and unstoppable spread of software, electronic circuits, semiconductors, data, information, radio frequencies, domain names and transmission protocols [3].

Cybercriminals circumvent the physical limitations that govern real-world crimes, given that physical proximity between the victim and the perpetrator is not necessary.

An important element of the cybercrime is that – generally, but not always – criminal acts are carried out from a distance, so there is a distance between the offender and the victim. For example, someone who is spreading a computer virus – this being a classic cybercrime – could do this from the palm tree-bordered beach of a remote island, many hundreds of miles away from their closest potential victim [4].

In the real world, there are people who break into homes and can take away everything they find valuable. In the virtual world, there are individuals who penetrate into computer systems and steal all valuable data. Just as in the real world there are uninvited guests and people who enjoy the pleasure of appropriating or destroying the property of others, the world of computers cannot avoid this phenomenon either.

2. Illegal access to a computer system under the regulation of the Romanian Criminal Code

2.1 Legal content

Article 360. (1) Unlawful access to a computer system shall be punishable by no less than 3 months and no more than 3 years of imprisonment or by a fine.

(2) The act set out in par. (1), committed in order to obtain computer data, shall be punishable by no less than 6 months and no more than 5 years of imprisonment.

(3) If the act set out in par. (1) was committed on a computer system to which, through processes, devices or specialized programs, access is restricted or prohibited for certain categories of users, it shall be punishable by no less than 2 and no more than 7 years of imprisonment.

2.2 The current Criminal Code in relation to the previous criminal law

The crime was not regulated in the Criminal Code, but has a correspondence in the offence provided for by Art. 42 of Law no. 161/2003 concerning some measures for ensuring transparency in exercising public office, public functions and in the business environment, the prevention and punishment of corruption [5].

The aspect regarding the commission of the act by violating security measures has been replaced by the phrase "through processes, devices or specialized programs, access is restricted or prohibited for certain categories of users".

This offence is classified as falling under Title VII of the current Criminal Code, entitled Offences against Public Security, which is considered by certain authors as an uninspired option. This is because, for example, certain assumptions regulated in Art. 360 of the Criminal Code may have a component that includes public security, but most often the consequences of this crime only affect the private environment [6].

2.3 Concept and characterization

Having regard to the Council of Europe's Convention on Cybercrime of 23 November 2001 and the Framework Decision of the Council of the European Union no. 2005/222/JHA of 24 February 2005 on attacks against information systems, it is clear that, at the time of the criminalization of unauthorized access to a computer system, there was an obligation assumed in this respect having its source in European law.

The reason for such criminalization is due to the risks associated with accessing a computer system, such as the transmission or propagation of viruses or other malicious software, i.e. computer programs designed to infiltrate or cause damage to a computer without the owner's knowledge and consent.

The offence of illegal access to a computer system is not accidentally placed first among cybercrimes, since it is considered to be the most important, an actual "basic offence" which facilitates the commission of other offences, constituting together multiple offences (for example, computer forgery, computer fraud, etc.) [7].

2.4. Preexisting elements

A. The legal object is the social value called "computer system" and the social relationships that arise in connection with the use of automatic data processing systems in society [8].

Computer/information systems play an essential role in contemporary organizations, as they provide the necessary information and the processing and dissemination capacities strictly needed in oredr to meet functional requirements, regardless of the field of activity.

B. The material object is the computer system to which fraudulent access is gained and it is represented by the material entities making up such a system (computers,

computer networks, hardware - peripheral equipment, cables, cards, servers, etc., and software - programs, applications, databases, etc.) and the computer data towards which the perpetrator's attention is directed [9].

The computer is the simplest information system that can work independently [10].

The information/IT/computer system is distinct from software, the latter being limited to certain applications. The computer systems that are the object of the offence may be of public utility or of private interest. From a technical point of view, the illicit action may affect the hardware system or the software components [11].

Computer data means any representation of facts, information or concept in a form that can be processed by a computer system. Also included in this category is any software that could cause a computer system to perform a function. Software means a set of instructions that may be executed by a computer system in order to obtain a determined result, or it means computer programs, procedures and documentation that allow the performance of one or more operations on a computer system.

If, as a result of a deed, computer data are altered, erased or damaged, the deed will meet the constitutive content of the criminal offence of alteration of computer data integrity (Article 362 of the Criminal Code), not that of the offence being analyzed [12].

C. Subjects of the offence

a) The active subject may be any person (individual or legal entity) who has criminal capacity, no special quality being required by the law for such purpose. However, the perpetrator is usually a person who has technical knowledge in the field of computers, is somewhat familiar with computer security systems and with the vulnerabilities of such systems, or is a person employed by the entities that have computer systems.

b) The passive subject of the offence is the individual or legal entity who owns the computer systems and whose right to the integrity, confidentiality and availability of the computer systems or data has been violated or jeopardized [13].

By extension, there may be a collective passive subject, consisting of a large number of individuals or legal entities, when access to the computer system automatically generates illegal access to other similar systems interconnected with the first one [14].

c) Criminal participation is possible in all its forms (as co-perpetrator, instigator, accomplice).

2.5 The structure and legal content of the offence comprises: A. the premise; B. the constitutive content of the offence.

A. The premise

In order for the crime of illegal access to a computer system to be committed, there must be a prior situation, which presupposes the existence of a computer system and of computer data on which the perpetrator acts without right, without authorization or by exceeding his/her authorization.

For the aggravated form mentioned in par. (3), the premise consists in the security measures (procedures, devices or specialized programs) that have been implemented by the IT system owner or by a person authorized by it in order to restrict or prohibit access for certain categories of persons.

Technical security measures may include passwords (the main mechanism for controlling access to an IT system), anti-theft systems (which detect suspicious behaviours, such as an excessive number of unsuccessful login attempts), biometric control systems (such as facial recognition), chip cards (usually encrypted and containing access information), antivirus software, firewall (a program that applies traffic policies set up by the administrator on a computer network), or cryptographic systems [15].

B. The constitutive content of the offence

a) The objective side of the offence of illegal access to a computer system comprises the material element, the immediate consequence, an essential requirement and the causal connection between the illicit activity and the outcome produced.

The material element, in all regulatory variants, consists in an action: gaining unlawful access to a computer system. It is not important, for the existence of the crime, whether access is gained through direct (physical) access to the computer system or through remote access (via the Internet, for instance). Illegal access involves attacks against the security of computer systems and data. Access involves the penetration into all or part of a computer system (hardware, components, data stored in the system, directories, etc.) [16].

Unauthorized access to a computer system often takes place through the use of social engineering techniques. For example, the offender might study a company's website and public documents to obtain the names of the managers and then call the company claiming to be the new IT technician. He could tell the person answering the phone that they need to remotely update their computer, but that they lost their password and then politely ask for the password from the interlocutor. From the point of view of security, social engineering may be countered only by educating employees or the users of a system. It is important for all users to be advised about social engineering tactics and avoid falling into the trap.

The deed may also be committed through phishing procedures. Phishing targets many kinds of confidential information, including usernames and passwords, information about bank accounts and credit cards, Personal Numbers (CNPs)/social security numbers, dates of birth, as well as information regarding the secret question, such as one's mother's maiden name or keywords. As a rule, in such situations, the victim does not notice that the information is requested by an unauthorized source. The preferred method consists in the reception by the victim of an e-mail or another notification that appears to be official, asking the person to send that information in order to maintain an account. Then, the victim might send the information to a website that may seem legitimate because it is almost identical to the official website of a bank or card company, but in reality it is just a data collection website where identity thieves gather information from as many victims as possible.

The material element in the case of the first aggravated variant of the offence consists in the unlawful access to a computer system in order to obtain computer data.

The material element in the situation of the second aggravated variant implies that illegal access is gained by using procedures, devices or programs that override the security measures that should restrict illegal access.

A highly publicized case is that of the hacker Marcel Lazăr Lehel from Arad, also known as Guccifer, who repeatedly and unlawfully accessed, by violating security measures, e-mail accounts belonging to public figures in Romania and abroad, in order to take possession of confidential data present in their electronic mail, following which he changed the authentication passwords, thus restricting the lawful user's right of access to their e-mail information. In this approach, cracking is often used, i.e. the activity of using software to penetrate badly chosen passwords, generally referred to as a password cracker.

As an operating mode, he entered some e-mail addresses using the safety questions that are generally asked of a person if one has forgotten their password. He deduced a number of answers to those questions from the Wikipedia pages of the victims where the names of their close relatives were mentioned. He entered some accounts by simply trying out the most popular names of dogs and cats used in the USA.

As far as the essential requirement is concerned, the legislator provides for the need for access to be gained without a right (unlawfully). For the purpose of the Article under consideration, the person who is in one of the following situations is acting without a right: a) he/she is not authorized, under the law or by contract; b) he/she exceeds the limits of the authorization; c) he/she does not have permission from the individual or legal entity having the competence to grant it.

Consequently, there will be no offence of illegal access if there was prior authorization from the owner of the computer system or from the rights holder to the computer system or to part of it (for example, with regard to testing that system). In cases where the computer system allows public access – open and unpaid – access will be lawful [17].

The immediate consequence of the offence consists in the state of danger for the social value the law is defending, namely the security of the computer systems.

In practice, the consequence of the simple form of unlawful access is the transition to a state of insecurity of the computer system and its resources (hardware, software, etc.) [18].

Causal connection. There must be a cause-effect link between the activity of the perpetrator and the outcome produced. This connection results ex re, i.e. from the materiality of the act, in the case of unauthorized access in the simplest form. In the second case, security measures (passwords, access codes, etc.) must be demonstrated [19].

b) The subjective side

The act may be committed with direct or indirect intent.

In the case of the aggravated form stipulated in paragraph (2), the specific form of guilt is direct intent, qualified by purpose [20].

Motive (reason) and purpose.

The incriminating text stipulates the requirement of a purpose only in the case of par. (2): that of obtaining computer data.

2.6 Forms. Methods. Penalties

A. Forms of the criminal offence

a) Preparatory acts. Preparatory acts (the procurement or making of devices in view of obtaining illegal access) are not punished in the case of this criminal offence and may form the object of a criminal offence if the conditions required by the law (the offence criminalized in Article 365 of the Criminal Code: Illegal operations with devices or software) are met.

For example, such a device is the USB keylogger. It is a small device that is connected between the keyboard plug-in connector and the computer's plug-in connector. Once connected between the keyboard connector and the computer's connector, the keylogger will automatically start recording each keyboard stroke. In order to see what has been typed, a secret combination of keys will be pressed to access the device's memory, so that only the user who has the correct combination of keys can access it. It is hard to notice for an uninformed eye because it is only 38 mm in length and it is the same colour as the keyboard plug-in connector. It does not emit any sound and has no LED light. By using it, one can find out, among other things, what has been talked about on Messenger and what web pages

have been visited, as well as finding out and remembering the passwords used by the user.
b) The offence is liable to present itself in the form of an attempt, which shall be punishable.
c) The offence is consumed at the time when access to a computer system is gained without right (unlawfully). It may also occur in a continuous form.
Thus, the defendant's act of periodically accessing a banking institution's website and sending to multiple users false messages by imitating the official pages of the bank's website and receiving confidential card account data from them meets the constituent elements of the offence of unlawful access to a computer system in a continuous form [21].
B. Methods
a) Regulatory methods – the deed is criminalized in a typical variant and two aggravated variants.
b) Factual methods – the offence may be committed according to a multitude of factual methods.
C. Penalties
In the typical variant, the offence is punishable by no less than 3 months and no more than 3 years of imprisonment or by a fine. In the first aggravated variant, the deed is punishable by no less than 6 months and no more than 5 years of imprisonment, and the second aggravated variant by no less than 2 and no more than 7 years of imprisonment.

2.7 Procedural issues

The criminal proceedings are initiated ex officio. Criminal prosecution is not necessarily carried out by the prosecutor, who only has the obligation to conduct and directly control criminal prosecution by the judicial police. The jurisdiction of the court of first instance lies with the county court (tribunal).

Conclusions

Cybercrimes are largely traditional forms of crime that use modern tools. After all, at some point in the past, highwaymen transitioned from using knives to using firearms, so we should not be surprised that in the 21st century some of them are updating their methods by using computers. The essential nature of the crimes remains the same: bad people who want our money, individuals who want to make victims, or companies and corporations that want to steal the secrets of their competitors.

Acknowledgements

The authors thank the anonymous reviewers and editor for their valuable contribution.

Funding
This research received no specific grant from any funding agency in the public, commercial, or not – for – profit sectors.

Author Contributions
The author conceived the study, carried out the literature review agenda and was responsible for the design, data collection, legislative analysis and case interpretation.

Disclosure Statement
The authors have not any competing financial, professional, or personal interests from other parties.

References
1. Antoniu, A., Toader T. et al. (2016). Explicațiile noului Cod penal (Explanations of the New Criminal Code), Vol. IV, Universul Juridic Publishing House, Bucharest.
2. Barbu, I.A. (2014). Introducere în criminalitatea informatică (Introduction to Cybercriminality), Sitech Publishing House, Craiova.
3. Bogdan, S., Șerban, D. A., Zlati, G. (2014). Noul Cod penal. Partea specială. Analize, explicații, comentarii. Perspectiva clujeană (The New Criminal Code. The Special Part. Analyses, Explanations, Comments. The Cluj Perspective), Universul Juridic Publishing House, Bucharest.
4. Boroi, A. (2011). Drept penal. Partea specială. Conform noului Cod penal (Criminal Law. The Special Part. According to the New Criminal Code), C.H. Beck Publishing House, Bucharest.
5. Brînză, S., Stati, V. (2015). Tratat de drept penal. Partea specială (Criminal Law Treatise. The Special Part), Vol. II, Tipografia Centrală (The Central Printing House), Chișinău.
6. Cuomo, L., Razzante, R. (2007). La disciplina dei reati informatici, Giappichelli, Torino.
7. Dobrinoiu, V., Hotca, M.A., et al. (2014). Noul Cod penal comentat (The New Criminal Code Commented), 2nd Edition, Universul Juridic Publishing House, Bucharest.
8. Dungan, P., Medeanu, T., Pașca, V. (2013). Drept penal. Partea specială (Criminal Law. The Special Part), Vol. II, Universul Juridic Publishing House, Bucharest.
9. Ionaș, A., Măgureanu, A.F., Dinu, C. (2015). Drept penal. Partea specială (Criminal Law. The Special Part), Universul Juridic Publishing House, Bucharest.

10. Vasiu, I., Vasiu, L. (2011). Criminalitatea în cyberspațiu (Cyberspace Criminality), Universul Juridic Publishing House, Bucharest.
11. Warren, P., Streeter, M. (2012). Cyber crime and warfare, McGraw-Hill Educational, first edition, Great Britain.

Notes:

[1] Ioana Vasiu, Lucian Vasiu, Criminalitatea în cyberspațiu (Cyberspace Criminality), Universul Juridic Publishing House, Bucharest, 2011, p. 13.
[2] Ionuț Andrei Barbu, Introducere în criminalitatea informatică (Introduction to Cybercriminality), Sitech Publishing House, Craiova, 2014, p. 14.
[3] Luigi Cuomo, Ranieri Razzante, La disciplina dei reati informatici, Giappichelli, Torino, 2007, p. 2.
[4] Peter Warren, Michael Streeter, Cyber crime and warfare, McGraw-Hill Educational, first edition, Great Britain, 2012, p. 2.
[5] Published in the Official Journal no. 279 of 21 April 2003.
[6] Sergiu Bogdan, Doris Alina Șerban, George Zlati, Noul Cod penal. Partea specială. Analize, explicații, comentarii. Perspectiva clujeană (The New Criminal Code. The Special Part. Analyses, Explanations, Comments. The Cluj Perspective), Universul Juridic Publishing House, Bucharest, 2014, p. 674.
[7] George Antoniu, Tudorel Toader et al.., Explicațiile noului Cod penal (Explanations of the New Criminal Code), Vol. IV, Universul Juridic Publishing House, Bucharest, 2016, pp. 853-854.
[8] Vasile Dobrinoiu, Mihai Adrian Hotca et al., Noul Cod penal comentat (The New Criminal Code Commented), 2nd Edition, Universul Juridic Publishing House, Bucharest, 2014, p. 825.
[9] Alexandru Boroi, Drept penal. Partea specială. Conform noului Cod penal (Criminal Law. The Special Part. According to the New Criminal Code), C.H. Beck Publishing House, Bucharest, 2011, p. 555.
[10] Sergiu Brînză, Vitalie Stati, Tratat de drept penal. Partea specială (Criminal Law Treatise. The Special Part), Vol. II, Tipografia Centrală (The Central Printing House), Chișinău, 2015, p. 348.
[11] Petru Dungan Tiberiu Medeanu, Viorel Pașca, Drept penal. Partea specială (Criminal Law. The Special Part), Vol. II, Universul Juridic Publishing House, Bucharest, 2013, p. 291.
[12] Alexandru Ionaș, Alexandru Florin Măgureanu, Cristina Dinu, Drept penal. Partea specială (Criminal Law. The Special Part), Universul Juridic Publishing House, Bucharest, 2015, p. 574.
[13] G. Antoniu, T. Toader et al., op. cit., p. 856.
[14] A. Boroi, op. cit., p. 555.
[15] G. Antoniu, T. Toader et al., op. cit., p. 857.

[16] A. Ionaș, A.F. Măgureanu, C. Dinu, op. cit., p. 575.
[17] G. Antoniu, T. Toader, op. cit., p. 858.
[18] A. Boroi, op. cit., p. 562.
[19] V. Dobrinoiu, M.A. Hotca et al., op. cit., p. 831.
[20] P. Dungan, T. Medeanu, V. Pașca, op. cit., p. 293.
[21] High Court of Cassation and Justice, criminal sentence, decision no. 4399 of 10 July 2006.