THE PROLIFERATION OF THE ILLEGAL ACCESS TO A COMPUTER SYSTEM

Lecturer **Adriana MOȚATU**[1]

Abstract

As the vast majority of activities took place online, computer-mediated interactions increased. Moreover, new situations arose that required not only a closer connection between people but also a new approach to how to work on the computer. In these conditions, the incidence of computer crimes has increased, such as illegal access to a computer system, violation of privacy, which requires a careful analysis of them, including the relevant cases, which is the subject of this paper.

Keywords*: cybercrimes, violation of privacy, computer system, criminal law, illegal access to a computer system.*

JEL Classification: K14

1. Introduction

Today, the internet has become an essential component of everyday life for most of us, both individuals and legal persons. As the vast majority of activities took place online, computer-mediated interactions increased and required not only a closer connection between people but also a new approach to how to activate in cyberspace.

Moreover, "the COVID-19 pandemic has revealed the importance of internet, as a workable medium for businesses, and other kind of activities. Thus, the online setting, with its own resources, tools and specific rules, requires an increasing attention in order to develop it, to improve the nexus between online and offline environments."[2]

But cyberspace offers, also, the opportunities for development of a very specific crime activities, so called cybercrimes, such as illegal access to a computer system, violation of privacy, data copying, installing virus, adware, or spyware, denial of services, phishing, etc., which requires a careful analysis of them, including the relevant cases, which is the subject of this paper.

2. The analysis of the case

The case study presented herein refers to the commission of the cybercrime of illegal access to a computer system through Team Viewer app., was solved by Focsani First instance Court in 2013[3].

Through the indictment of the Prosecutor's Office, the defendant was sent to trial under the aspect of committing the crimes of unauthorized access to a computer system in order to obtain computer data by violating security measures, deleting and copying computer data and transferring them to their own system and possession without right of a computer application for the purpose of committing crimes.

The defendant was charged with accessing without right, by violating security measures the account of the injured party, on which occasion he deleted and copied computer data, which he transferred to his own computer system using a computer application that he held it without right, for the purpose of committing these deeds.

The injured party found that he could no longer access the personal account opened on his site, indicating that the access password was not correct, noting that some of the emails he had initially

[1] Adriana Moțatu - Faculty of Law, Bucharest University of Economic Studies, Romania, adriana.motatu@drept.ase.ro.

[2] Ene, Ch. (2020). *Smart contracts - the new form of the legal agreements.* Proceedings of the International Conference on Business Excellence, Volume 14: Issue 1. Retrieved from: https://content.sciendo.com/configurable/contentpage/journals$002fpicbe$002f14$002f1$002farticle-p1206.xml, accessed on 1.10.2020.

[3] The Criminal Decision no.1794/2013 issued by Focsani First instance Court in the File no. 6981/231/213 regarding to the illegal access into a computer system through Team Viewer app.

been inexplicably deleted.

The verifications performed by the specialized workers established the access to the e-mail account belonging to the injured party that was accessed from the computer system connected to the Internet network.

The searches carried out at the defendant's home identified a computer system for storing computer data, being identified the computer application used to remotely access the computer system through the internet connection of the injured party.

Also, files were found that contained data regarding the account and opening passwords, being found the data of the injured party. The defendant admitted to the crime.

The injured party became a civil party requesting moral damages, the defendant agreeing to compensate him. Because the deeds committed are in real competition, the sentences applied were merged according to the rule of legal cumulation into the heaviest sentence of 1 year and 4 months in prison.

As a way of executing the sentence, the court ordered the conditional suspension of the execution of the sentence. The court ordered the confiscation from the defendant of the goods used to commit the crimes.

So, the legislator sought by criminalizing this crime to protect computer systems, data stored by illegal access to a computer system.

3. Legal framework

The cybercrime of illegal access to a computer system is provided for in Chapter VI of the Criminal Code entitled "Offenses against the security and integrity of computer systems and data", Article 360 provides: *"(1) Access, without right, to a computer system shall be punished by imprisonment from 3 months to 3 years or by a fine. (2) The deed provided in par. (1), committed for the purpose of obtaining computer data, shall be punished by imprisonment from 6 months to 5 years. (3) If the deed provided in par. (1) has been committed in respect of a computer system to which, by means of specialized procedures, devices or programs, access is restricted or prohibited for certain categories of users, the penalty is imprisonment from 2 to 7 years.*"

4. The analysis of the cybercrime of illegal access to a computer system

The Council of Europe considers that the concept of cybercrime "*applied to three categories of criminal activities. The first covers traditional forms of crime such as fraud or forgery, though in a cybercrime context relates specifically to crimes committed over electronic communication networks and information systems. […] The second concerns the publication of illegal content over electronic media (i.e., child sexual abuse material or incitement to racial hatred). The third includes crimes unique to electronic networks, that is, attacks against information systems, denial of service and hacking*."[4]

As has been underlined in literature, the term of "cybercrime" covers a large aria of criminal acts that consist in criminal uses of any computer systems.[5]

The computer system represents "*any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data*". (According to Article 1(a) of the Council of Europe's Convention on Cybercrime of 2001).

Thus, cybercrimes generally damage, destroy or interfere with computer data or operation; they also include using or misusing of the data stored on the computer or network.[6]

The software contains data protected by security measures, which are used for a specific

[4] Council of Europe. (2007). *The commission communication "towards a general policy on the fight against cybercrime."* Retrieved from: http://europa.eu/rapid/press-release_MEMO-07-199_en.pdf, accessed on 1.10.2020.

[5] Hill, J., & Marion, N.E. (2016). *Introduction to cybercrime: computer crimes, laws, and policing in the 21st century*. Santa Barbara, CA, USA: Praeger, p. 121.

[6] Bainbridge, D.I. (1989), *Hacking. The Unauthorised Access of Computer Systems; The Legal Implications*, „The Modern Law Review", vol. 52, no. 2., p. 236. Retrieved from: www.jstor.org/stable/1096193, accessed on 1.10.2020.

processing purpose. These are intended only for the person who uses them and has come into their possession under legal conditions, in some cases requiring the person's consent to be processed, and other data or programs being purchased on a license basis. This data is available to the owner and restricted to other users.

The illegal access to a computer system, known as hacking into computer system[7], is also provided by Article 2 of the Council of Europe Convention on Cybercrime and by the Article 3 of the Directive 2013/40/EU as access to a computer system without right, despite all the specific security measures taken by the owners.

Therefore, the active subject is undetermined, and can be anyone, but having very good skills and extensive computer knowledge, especial regarding security systems.[8]

The passive subject is a specific person or persons, meaning the legal owner (owners) of the computer system or of the data contained in it, and support the damage caused by the commission of this cybercrime. Some scholars emphasize the existence of the passive secondary subject, meaning the legal person or individual affected by the cybercrime, other than the owner or the right holder of that computer system.[9]

The material object is determined by the computer system against which the criminal activity was carried out to knowingly gain access to data in a system without permission to access that data.

The special legal object is represented by the social relations protected by law, which refer to the inviolability, security of the information system, which must protect the integrity, confidentiality of the information systems and data.

The objective side is represented by the unauthorized trespassing into a computer system, in order to obtain computer data, by violating security measures. The Romanian Criminal Code provide two aggravated variants of the illegal access into a computer system. First refers to unauthorized access in order to obtain data and the second aggravated circumstances consist in using software or hardware for breaching the security measures.[10]

The subjective side is represented by the dishonest intention of the perpetrator which can be direct or indirect.[11]

The consumption of the crime takes place at the moment of illegal access to the computer system. Attempt to commit this crime is punishable, also.

The sanction is provided gradually according to the three paragraphs, because:

- unauthorized access to a computer system is punishable by imprisonment from 3 months to 3 years or a fine;

- in paragraph 2 shall be punished by imprisonment from 6 months to 5 years for the commission of the act provided for in paragraph 1, carried out for the purpose of obtaining computer data;

- in paragraph 2 shall be punished by imprisonment from 2 to 7 years the same act provided for in paragraph 1, committed in respect of a computer system through specialized procedures, devices or programs that have restricted or prohibited access for certain categories of users.

It is important to underline that the above analyzed cybercrime is followed by additional cybercrimes, in most of the cases: thus, the illegal access to computer system is rather the means not the end goal of the perpetrator.

---

[7] Savin, Andrej (2013), *EU Internet Law*, Cheltenham, Glos: Edward Elgar Publishing Limited, p. 153.

[8] Vasiu, I. & Vasiu, L. (2001), *Totul despre hackeri*, [Everything about hackers], Bucharest: Nemira Publishing House, p. 87.

[9] Dobrinoiu, M. (2006), *Infractiuni in domeniul informaticii* [Crimes in the IT field], Bucharest: C.H. Beck Publishing House, p. 174.

[10] Drăgan, A. T. (2019), *Illegal access to a computer system from the standpoint of the current criminal code*, „Journal of Legal Studies" Volume 23 Issue 37/2019, p. 33-43, "Vasile Goldis" Western University of Arad. Retrieved from: web: publicatii.uvvg.ro/index. php/jls; accessed on 1.10.2020.

[11] Moise A.C. (2017), *Considerations of criminal law and forensic science regarding the illegal access to a computer system*, „AGORA International Journal of Juridical Sciences", No.2 (2017), p. 49-57. Retrieved from: http://univagora.ro/jour/index.php/aijjs, accessed on 1.10.2020.

5. Conclusions

It is obviously that computer technology continues to evolve and also the criminal activity carried out in cyberspace. In this context, protecting the computer system and data become very difficult and needed a joint effort of individuals and companies; and also, of governments, which have to adopt a new specific legislation and to develop international cooperation in this regard.

On the other hand, the World Economic Forum stated in 2012 that cybercrime become one of the biggest threats to the sustainable global development of society. The sustainable development, understood as intergenerational equity, based on the aggregation of rights and obligation derived from relation between present and future,[12] is endangered by the proliferation of criminal activity on a global scale.

Therefore, several Sustainable Development Goals (SDGs), provided by the 2030 Agenda for Sustainable Development (General Assembly 70/1), refer to crime, justice and security. According to SDGs, enhancing the capacities of the states to combat crimes and to promote the rule of law represent priorities of international community.

Bibliography

1. Bainbridge, D.I. (1989), *Hacking. The Unauthorised Access of Computer Systems; The Legal Implications,* „The Modern Law Review", vol. 52, no. 2.
2. Council of Europe, Convention on Cybercrime, Budapest, (2001).
3. Council of Europe. (2007, *The commission communication "towards a general policy on the fight against cybercrime*" Retrieved from: http://europa.eu/rapid/press-release_MEMO-07-199_en.pdf.
4. Directive 2013/40/EU 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.
5. Dobrinoiu, M. (2006), *Infractiuni in domeniul informaticii* [*Crimes in the IT field*], Bucharest: C.H. Beck Publishing House.
6. Drăgan, A.T. (2019), *Illegal access to a computer system from the standpoint of the current criminal code,* „Journal of Legal Studies" Volume 23 Issue 37/2019, "Vasile Goldis" Western University of Arad.
7. Ene, Ch. (2014), *Precautionary Principle – The key element of Sustainable Development*, „Knowledge Horizons", vol.6, issue 2 (28).
8. Ene, Ch. (2020), *Smart contracts - the new form of the legal agreements*, „Proceedings of the International Conference on Business Excellence", Volume 14: Issue 1. Retrieved from: https://content.sciendo.com/configurable/contentpage/journals$002fpicbe$002f14$002f1$002farticlep1206.xml.
9. General Assembly Resolution 70/1, Transforming Our World: The 2030 Agenda for Sustainable Development, A/RES/70/1(25 September 2015). Retrieved from: www.un.org/ga/search/view_doc.asp?symbol=A/RES/70/1&Lang=E.
10. Hill, J., & Marion, N.E. (2016), *Introduction to cybercrime: computer crimes, laws, and policing in the 21st century*, Santa Barbara, CA, USA: Praeger.
11. Moise A.C. (2017), *Considerations of criminal law and forensic science regarding the illegal access to a computer system*, „AGORA International Journal of Juridical Sciences", No.2.
12. Savin, Andrej (2013), *EU Internet Law*, Cheltenham, Glos: Edward Elgar Publishing Limited.
13. The Criminal Decision no.1794/2013 issued by Focsani First instance Court in the File no.6981/231/213 regarding to the illegal access into a computer system through Team Viewer app.
14. Vasiu, I. & Vasiu, L. (2001), *Totul despre hackeri*, [*Everything about hackers*], Bucharest: Nemira Publishing House.

[12] Ene, Ch. (2014). *Precautionary Principle – The key element of Sustainable Development*. „Knowledge Horizons", vol. 6, issue 2, (28), p. 150-153.