VIII INTERNATIONAL SCIENTIFIC PROFESSIONAL CONFERENCE
SECURITY AND CRISIS MANAGEMENT – THEORY AND PRACTICE (SeCMan)
-SAFETY FOR THE FUTURE-
29th and 30th September 2022, Sremska Kamenica, Republic of Serbia

SECURITY OF COMPUTER DATA IN THE CRIMINAL POLICY OF THE REPUBLIC OF SERBIA

Slavica Dinic[1]
[1] University of Educons, Faculty of security studies, Vojvode Putnika 67, Sremska Kamenica, Republic of Serbia, slavicadinic@yahoo.com

Received: 26th July 2022
Accepted: 17th August 2022

Review paper

Abstract: *The paper presents the results of a research aimed at determining teachers' attitudes regarding the problems and possibilities of online teaching in emergency situations. The COVID-19 pandemic has caused extraordinary living and working conditions that have left some impact on the teaching and education systems. Therefore, the problems and opportunities of online teaching have been observed in the context of the pandemic. The research sample included 102 teachers from higher education institutions on the territory of the Republic of Serbia. For the needs of the research, a questionnaire with an assessment scale was prepared and shared with the teachers through a link. The teachers expressed their perceptions, attitudes, opinions and experiences related to personal competencies, preparation and support for online classes, practical implementation of online teaching and their relationship with students, as well as to didactic and methodological aspects of learning in an online environment.*

Key words: *law, security, cybercrime*

1. INTRODUCTION

The protection of information systems in general, and especially before the security of computer data, is provided by the incrimination of terrorism from Art. 391, Chapter XXXIV of the Criminal Code - Crimes against humanity and other goods protected by international law. However, this incrimination is, among other things, aimed at protecting the infrastructure of information systems from the most severe form of consequences in criminal law - from destruction (another type of violation), as a result of which we can classify it in a broader group of so-called political offenses, ie in the group of incriminations whose primary object of protection is the protection of the constitutional order and security of the state (criminal offenses from Chapter XXVIII of the Criminal Code; criminal offenses from Chapter XXXIV Articles 391, 391a, 391b, 391c, 391g, 392, 393 and 393a; criminal offenses under Chapter XXXVI Articles 292, 293 and 294, criminal offenses under Chapter XXV Article 287, criminal offenses under Chapter XXVII Articles 299, 300, 301 and 302). Part of the incrimination from Art. 391. CC Art. 1, item 3, which deals with the protection of information systems infrastructure, reads: "Whoever intends to seriously intimidate the population, or to force Serbia, a foreign state or an international organization to do or not do something, or to seriously endanger or violate basic constitutional, political , economic or social structures of Serbia,

foreign states or international organizations destroy a state or public facility, traffic system, infrastructure including information systems, immovable platform in the continental shelf, public good or private property in a way that may endanger human lives or cause significant damage to the economy, shall be punished by imprisonment for a term not less than twelve years or by imprisonment for a term between thirty and forty years."

The primary object of protection of the presented part of the incrimination from Article 391, however, is not the security of computer data, but humanity and other goods that are protected by international law. The international community is interested in the issue of computer data, but only in the field of protection of the mentioned values, and from the most severe type of consequences for them, while it does not deal with the issue of endangering and damaging computer data. This is supported by the fact that a significant number of relevant international documents are moving in the direction of understanding terrorism as a crime that, although directed against a specific state or international organization, affects values of interest to the entire international community.

Therefore, from the aspect of protection of our country in this domain, as well as the international community, in addition to the mentioned incrimination, the following criminal acts from the group that has criminal acts against computer data security as its object of protection should be analyzed. These are: computer sabotage from Art. 299 of the Criminal Code, creation and introduction of computer viruses from Art. 300 of the Criminal Code, computer fraud under Art. 301 of the Criminal Code and unauthorized access to a protected computer, computer network and electronic data processing referred to in Art. 302. CC.

Thus, even milder forms of consequences of crimes committed with (mis) use of computers and computer data, ie computer systems, manifested in the form of damage, concrete or abstract danger, can significantly affect the issue of security of the constitutional order and security of our country. Certainly, the above also applies to destruction, as the most severe type of consequence, which can occur even when the act is not undertaken in order to achieve the already mentioned terrorist intentions. Actions that are covered by incriminations from the group of offenses against computer data security, especially criminal offenses from Art. 299, 300, 301 and 302 of the Criminal Code, which is the subject of this paper, with implications for our social order, certainly have a relevant impact on issues in the security segment of the international community.

2. COMPUTER SABOTAGE (Art. 299 CC)

The essence of this crime is: processing of data that are important for state bodies, public services, institutions, companies or other entities. " The criminal act of computer sabotage has two forms. The first form can be achieved by: destroying, deleting, modifying, damaging, concealing or rendering unusable computer data or programs in another way (which is suitable for that), all with the intention of disabling or significantly interfering with the process of electronic data processing that are important for state bodies, public services, institutions, enterprises or other entities. According to Art. 112 para. 17. CC, computer data should define any presentation of facts, information or concepts in a form that is suitable for their fence in the computer system, including the appropriate program on the basis of which the computer system performs its function. Computer program, according to Art. 112 para. 19. CC, is considered an organized set of commands that are used to control the operation of a computer, as well as to solve a specific task using a computer.

The second form will exist if a computer or other electronic data processing device is destroyed or damaged, with the intention of taking action on the first form. The destruction of a computer or other device for electronic data processing is not considered a literal change in the physical

properties of these devices, but a change in their program performance, which is such that as a result these devices can no longer perform their intended function. The issue of destruction should be seen as reducing, not eliminating, the software performance of these devices, and thus reducing the possibility of their use for the purpose for which they are intended. Thus, in both forms, the act of execution is undertaken, exclusively, by doing.

As an example, we cite the conclusion of the judgment of the Court of Appeals in Nis, in judgment 7Kz.1.br.2607 / 11.

"The act of committing the criminal offense of computer sabotage under Article 299 of the Criminal Code implies the conduct of the perpetrator, so this criminal offense cannot be committed by the defendant's omission."

From the explanation:

"According to the actions of committing the criminal offense of computer sabotage under Art. 299. of the Criminal Code, which are alternatively determined, it follows that they imply active action of the perpetrator, where the protective object of this criminal offense is the electronic program itself, ie electronic data, the manipulation of which seems unusable, in order to significantly interfere with electronic processing. data. The first-instance court correctly determined that the factual description of the act from the indictment does not contain such actions, because the defendant is charged with not installing the HIF fund application software, so the first-instance court's correct conclusion is that the defendant's failure to act , does not represent any act of committing the criminal offense he is charged with, considering that his actions did not endanger any program or electronic data.

Therefore, the decision of the first instance court, which found that the actions of the defendant did not have the characteristics of the said criminal offense, as well as any other criminal offense, was correct, so he was acquitted of the charge, by applying Art. 355. point. 1. CPC, about which the first instance court gave sufficient and clear reasons, which are accepted by this court in everything. (Judgment of the Basic Court in Vranje K. No. 388/10 of 07.03.2011 and Judgment of the Court of Appeals in Nis 7Kz.1.br.2607 / 11 of 31.08.2012).

In both forms, a criminal offense is considered completed by taking an enforcement action with the intention of disabling or significantly interfering with the procedure of electronic data processing that is important for state bodies, public services, institutions, enterprises or other entities. The object of action, in the first form is a computer data or program, and in the second a computer or other device for electronic data processing. Any person can report as the perpetrator of this crime. Subjective elements of the criminal offense of computer sabotage are: intent and intent to disable or significantly interfere with the process of electronic data processing that is important for state bodies, public services, institutions, companies or other entities. However, the very realization of the intention, for the existence of this crime, is not important.

3. CREATION AND ENTRY OF COMPUTER VIRUSES (Art. 300 CC)

The crime consists of:

(1) Whoever creates a computer virus with the intention of introducing it into another's computer or computer network,

shall be punished by a fine or imprisonment for a term not exceeding six months.

(2) Whoever introduces a computer virus into another's computer or computer network and thereby causes damage,

shall be punished by a fine or imprisonment for a term not exceeding two years.

(3) the device and means by which the criminal offense referred to in para. 1 and 2 of this Article shall be confiscated. "

This crime has two forms: basic and serious. The basic form is incriminated in paragraph 1. It exists when someone creates a computer virus, with the intention of introducing it into someone else's computer or computer network. The action of the basic form is, therefore, the creation of a computer virus, which is a technological process of procedures by which a computer virus is created. The term "computer" should be treated in the usual sense, a computer network, according to Art. 112 para. 18. CC, as a set of interconnected computers, ie computer systems that communicate by exchanging data.

The object of action in the basic form of this crime is a computer virus. Pursuant to the legal provision, ie Art. 112 para. 20. CC, a computer virus is a computer program or other set of commands entered into a computer or computer network that is designed to replicate itself and act on other programs or data in a computer or computer network by adding that program or set of commands to one or more computer program or data.

The legislator "sees" any person as an executor. However, in practice, these are only those persons who have a sufficient level of knowledge (very often informal) to create computer viruses. Subjective characteristics of the being of the basic form of the crime: intent and intent to introduce a virus into someone else's computer or computer network.

Another form of crime, incriminated in paragraph 2, exists when someone enters a computer virus into someone else's computer or computer network and thus causes damage. The action of performing this form consists of introducing a computer virus into someone else's computer or computer network. This form of crime is considered committed when damage occurs, and after the introduction of a computer virus into someone else's computer or computer network. However, it must be determined whether the damage occurred, in this particular case. The perpetrator of this form of tort can also be any person. It doesn’t have to be about who made the computer virus. Subjective element of the legal description of a more serious form of the crime of making and introducing computer viruses: intent.

For both forms of this crime, paragraph 3, provides for the mandatory confiscation of devices and means by which they were committed.

4. COMPUTER FRAUD (Art. 301 CC)

According to the legal description of the criminal offense of computer fraud, this offense is committed: property gain and thus cause property damage to others." This crime has a basic, two more serious and one easier form. The first more serious form exists if by committing the basic form of the criminal offense a property gain exceeding the amount of four hundred and fifty thousand dinars is obtained, while if this amount exceeds one million and five hundred thousand dinars, there will be another more serious form. In the event that the basic form of the crime was committed with the intention of exclusively damaging another person, without the intention of obtaining illegal property gain, it will be a lighter form of the criminal offense of computer fraud.

The action of the basic form can be one of the following activities: entering incorrect data, failing to enter correct data or otherwise concealing or falsely presenting data. The crime is completed when a certain consequence occurs. In fact, it is necessary that some of the envisaged actions of doing or not doing, have an impact on the result of electronic processing or data transfer, in the form of changing the results of processing or data transfer, in the sense that the result is not compatible. Computer fraud can be committed in all situations in which

automated data processing occurs, and these are, today, almost all segments of social life, including security.

Any person can report as the perpetrator. However, it can only be the person who objectively has the ability to perform some of the planned actions. Subjective features of the basic form of being a criminal offense of computer fraud: intent (direct) and the intention to obtain illegal property gain for oneself or another and thus cause property damage to another.

5. UNAUTHORIZED ACCESS TO A PROTECTED COMPUTER, COMPUTER NETWORK AND ELECTRONIC DATA PROCESSING (Article 302 of the CC)

The essence of the crime is realized by:

(1) Whoever, in violation of protection measures, enters into a computer or computer network without authorization, or without access to electronic data processing, without authorization,

(2) Whoever records or uses the data obtained in the manner provided for in paragraph 1 of this Article, or

(3) If, as a result of the act referred to in paragraph 1 of this Article, there has been a delay or serious disruption of the functioning of electronic processing and data transmission or network, or other severe consequences have occurred.

The crime has three forms: basic and two serious. The act of execution of the basic form is: a) unauthorized connection to a computer or computer network or b) unauthorized access to electronic data processing. However, it is necessary that until the inclusion, ie. accession came in violation of some protective measure.

The perpetrator of the basic form of this crime can be any person. However, there is a special category of persons, the so-called hackers, who engage in illegal access to information systems. They are trained to master even the most complex type of computer protection, and the motives for their actions are very dispersive. The subjective feature of the being of this incrimination: intent.

The first serious form of this criminal offense exists if the data obtained by committing the basic form of the criminal offense is recorded or used. The purpose for which this was done, according to the position of the legislator, is not important, nor is the manner of recording or use. However, when sentencing, the importance of this issue is not excluded.

The second more severe form predicts the occurrence of certain consequences, caused by the execution of the basic form. These are: interruption or serious disruption of the functioning of electronic processing and data transmission or network, or the occurrence of other severe consequences. The issue of downtime should not be treated as a short-term downtime, which did not result in any harmful consequences, while severe consequences should not include only direct consequences on a computer, computer network or other device intended for electronic data processing, but all those caused by unauthorized access, or what are its result.

6. CONCLUSION

The issue of protection of computers and computer networks, primarily those that are of public importance, is primary for one society, state, is. its security in general, however, must inevitably be dedicated, because today cannot be imagined without numerous "smart" devices that work on the basis of computer programs and networks. On the one hand, it makes our lives much easier, while at the same time, on the other hand, it is a serious threat to both our individual and national security.

The Law on Amendments to the Criminal Code of the Republic of Serbia from April 2003, for the first time, included in our legislation a group of criminal offenses whose object of protection was the security of computer systems and data processing networks. After that, in 2005, the current Criminal Code of the Republic of Serbia was adopted, which has been in force since January 1, 2006. By analyzing the statistical bulletins of the Republic of Serbia, in the first eight years of application of the mentioned law (2006-2013), we come to the conclusion that the number of persons against whom criminal charges were filed and a verdict for these four crimes is extremely small, with the share of minors negligible in this issue, which is surprising given the fact that the younger generations, especially minors, are extremely computer-oriented. In general, they quickly adopt and apply all his innovations to achieve very different goals, the achievement of which is often not motivated by intent of a criminal nature, but can often result in it.

After the observed time interval, in the period from 2014 until today, the situation in this field is changing significantly. Namely, the number of filed criminal charges, but also verdicts, is significantly higher, in relation to both adults and minors. On the one hand, the expansion of computer technology into all segments of society, and thus cybercrime, but also serious steps of our state to counteract this problem, along with monitoring international trends and establishing international cooperation in this area, also contributed to that. The Republic of Serbia established the Prosecutor's Office for Computer Crime, ie the Special Department of the Higher Public Prosecutor's Office for High-Tech Crime in 2006.

However, only in the second half of the second decade of the twenty-first century, the Ministry of Internal Affairs of our country invested significant efforts and resources in the field, primarily prevention, but also the suppression of this type of crime, which greatly affected the efficiency and effectiveness of this prosecution. This problem, in addition to the legal regulations, which we can state is well set, our country actually opposes. Namely, he constantly educates his bodies of formal social control in this area, introduces them to newspapers, but also develops creativity in the employees in this field. Accordingly, the persons employed are "technologically literate", starting from the principle of "predominant interest", ie. by combating and preventing crimes in this area, the negative side of the use of computers and computer networks is trying to be reduced to the lowest possible level, ie, to this end, everything necessary and possible is undertaken to increase the benefits of using this, although today more and no, innovation.

REFERENCES

Delic, N., (2021). Criminal law - special part, Faculty of Law University of Belgrade, ISBN 978-86-7630-948-1, Belgrade.

Ilic, R., (2014). Criminal Procedure Law, Megatrend University, ISBN 978-86-7747-506-2, Belgrade.

Jovasevic, D., (2018). Criminal law - general part, Dosije, ISBN 978-86-6047-273-3, Belgrade.

Stojanovic, Z., Delic, N., (2014). Criminal law - special part, Faculty of Law University of Belgrade, ISBN 978-86-7630-480-6, Belgrade.

Stojanovic, Z., (2009). Criminal law - general part, Faculty of Law University of Belgrade, ISBN 86-86223-10-4, Belgrade.

Skulic, M., (2015). Criminal Procedure Law, Faculty of Law University of Belgrade, ISBN 978-86-7630-577-3, Belgrade.

VukoviC, I., (2021). Criminal law - general part, Faculty of Law University of Belgrade, ISBN 978-86-7630-936-8, Belgrade.

Criminal Code of the Republic of Serbia. “Official Gazette of the Republic of Serbia”, No. 85/2005, 88/2005 – correction, 107/2005 – correction., 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 I 35/2019.

The Code of Criminal Procedure. “Official Gazette of the Republic of Serbia”, No. 72/2011, 101/2011, 121/2012, 32/2013, 45/2013, 55/2014, 35/2019, 27/2021 – the decision of the Constitutional court and 62/2021 – the decision of the Constitutional court.

The Law on minor perpetrators of criminal acts and criminal protection of minors. “Official Gazette of the Republic of Serbia”, No. 85/2005.