DOI: 10.5937/voidelo1905085J

COMPUTER CRIMES IN SERBIA

Dragan Jovašević*
University of Niš, Faculty of Law

Criminal Legislation of the Republic of Serbia, which started applying as of 1 January 2006, provides for criminal responsibility and punishment for several criminal offences against the safety of computer data. Those are computer criminal offences, which a perpetrator (who obviously has unique, special knowledge of information technology, computing – IT sector) commits by the abuse of computers, computer systems or network, thereby causing material or non-material damage to other natural or legal persons, as well as the whole social community. The basis of those incriminations is the European standards established under the Budapest Convention on Cybercrime and Additional Protocol to this Convention, as well as many other European documents. The paper analyses the basic characteristics of computer criminal offences in Serbia and the degree of their compatibility with the European standards.

Key Words: *computer abuse, European standards, crime, responsibility, sanction*

Introduction

When adopting the Convention on Cybercrime, ETS 185 of 23 November 2001 the Council of Europe tried to set up the basis of a unique European system of substantial and procedural criminal law in the field of necessary cooperation of the State members in fighting various forms and kinds of cyber crime[1]. The Convention itselft (Articles 2-13) stipulated five such crimes directed against the security, entirety and availability of computer data and computer systems. Hereby, the basis for some national legislations has been set more precisely in terms of defining the features and characteristics of individual computer crimes, their basic, minor and more severe forms, and prescribing criminal sanctions for their perpetrators (natural and legal persons)[2].

An additional Protocol on criminalisation of the acts of racist and xenophobic nature committed through computer systems has been adopted with this Convention. In Articles 3-7 this Protocol stipulates criminal responsibility and penalties for the abuse of computers in committing crimes out of racial and xenophobic impulses (motives)[3].

* Dragan Jovašević, PhD, Full Professor at the Faculty of Law, University of Niš, Serbia

[1] B. Petrović, D. Jovašević, Međunarodno krivično pravo, Sarajevo, 2010, pp.178-181.

[2] D. Jovašević, Međunarodno krivično pravo, Niš, 2011, pp.211-214.

[3] D. Jovašević, V. Ikanović, Međunarodno krivično pravo, Banja Luka, 2015, pp.116-118.

By accepting the above - mentioned Convention, and amending the Criminal Code of the Republic of Serbia[4] in April 2003, numerous computer crimes have been introduced into the criminal and legal system in Chapter 16a, under the title „Crimes against security of computer data". The same crimes were introduced into the 2003 Criminal Code of Montenegro in Chapter 28 under the same title[5].

General Characteristics of Criminal and Legal Protection of Computer Data

The object of protection from these crimes is the security of computer data and systems, that is, computer network. The legislator uses the term computer crime for it. However, besides this term, the legislation of the Republic of Serbia uses the term hi-tech crime for crimes that are systematized here.

Article 112 of the 2005 Criminal Code of the Republic of Serbia[6] (hereinafter: the Criminal Code) defines the term and characteristics of computer data, computer network, computer programme, computer virus, computer and computer system in terms of the object of attack in case of these crimes. The term computer crime encompasses all various shapes, kinds and forms of the expression of illegal behaviors directed against the security of computer and information systems as a whole or some of their parts, in different ways and with different means, with the intention to gain the benefit for themselves or other person (of material or non-material nature) or to cause damage to other person. The characteristic of computer crime is huge dynamics and extreme variety of its forms and kinds and manifestation forms[7].

Perpetrators of these crimes belong to a specific category of persons. They are mostly nondelinquents and socially adjustable, non-violent persons. They should have certain special, expert and practical knowledge and skills in the domain of information and computer techniques and technologies[8].

In practice, there is a greater or lesser time difference between the action taken and the moment when the consequences occur. These crimes are difficult to detect and even harder to prove.They remain practically undiscovered for a long time, until the damaged person suffers harm in the domain of information and computer data or systems.

Individual Computer Crimes

Damaging computer data and programmes

The crime under Article 298 involves the unauthorized deletion, alteration, damage, concealment or otherwise making computer data or programme unusable[9].

[4] D. Jovašević, Komentar Krivičnog zakona Republike Srbije sa sudskom praksom, Beograd, 2003, pp.429-431.
[5] Lj. Lazarević, B. Vučković, V. Vučković, Komentar Krivičnog zakonika Crne Gore, Cetinje, 2004, pp.561-566.
[6] The Official Gazette of the Republic of Serbia, No. 85/2005, 88/2005...108/2014 and 94/2016.
[7] D. Jovašević, Krivično pravo, Posebni deo, Beograd, 2017, pp.218-221.
[8] D. Jovašević, Leksikon krivičnog prava, Beograd, 2011, pp.511-513.
[9] B. Petrović, D. Jovašević, Krivično pravo 2, Posebni dio, Sarajevo, 2005, pp.189-191.

The object of protection is the security of computer data or computer programmes, and the object of attack is computer data or programme.

Computer data is every representation of facts, information or concepts in a form suitable for processing by a computer system including appropriate computer software necessary for the functioning of the computer system. A computer programme is a regulated set of orders that serves to control computer operations, as well as solve specific tasks using a computer.

The consequence of this crime is the violation of protected goods – computer data or programme belonging to natural or legal persons in terms of its usability or usefulness in general, or for a specific time, at a specific place or for specific purpose.

The perpetrator of the crime may be any person, and the guilt requires intent.

A fine or sentence of imprisonment of up to one year is prescribed for this crime. The court shall obligatory impose a security measure of the seizure of equipment and devices on the perpetrator if the following two conditions are fulfilled:

1) the equipment and devices have been used for the commission of the crimes and

2) the equipment and devices are the property of the perpetrator.

This crime has two heavier forms[10].

The first form of this crime exists if the action taken in the execution of the basic crime has caused the damage amounting to over RSD 450,000. The amount of material damage caused at the time of the commission of the crime in the amount established under the law constitutes a qualifying circumstance.A sentence of three months to three years of imprisonment is prescribed for this crime.

The second form of this offence, for which a sentence of three months to five years of imprisonment is prescribed, exists if the action taken in the execution of the basic crime has caused the material damage amounting to over RSD 1.500.000.

Computer sabotage

This crime set out in Article 299 of the Criminal Code is committed by whoever enters, destroys, deletes, alters, damages, conceals or otherwise makes computer data or programme unusable or damages or destroys a computer or other device for electronic processing and transfer of data, with intent to prevent or considerably disrupt the procedure of electronic processing and transfer of data that are of importance for government authorities, public service, institution, enterprise or other entities[11].

The entry means entering or storing new, previously non-existing data or alteration of the already existing computer or other data in computer programme. Destroying means complete and permanent destruction of a substance or form of a specific object, so that it cannot be used for any purpose or previous intention it was used for. Deletion means removing computer data or programme in its entirety or a part of it, often by use of mechanical or other means. Alteration is a partial change of the existing data in terms of its substance, whereabouts or nature, or entering other untrue data into computer system. The damage is temporary, partial or short-term disability of computer data, programme, computer or other device to serve its regular purpose.

[10] D. Jovašević, V. Ikanović, Krivično pravo Republike Srpske, Posebni deo, Banja Luka, 2012, pp.221-223.

[11] B. Petrović, D. Jovašević, A. Ferhatović, Krivično pravo 2, Sarajevo, 2016, pp.311-313.

Concealment is the removal of data or object from the place where it used to be, the place known to everyone, and its transfer to other, mostly hidden place, where other persons cannot be introduced to its contents in general or for a certain period of time. Making computer data or programme unusable is any action which, to a greater or lesser extent, affects the usability of computer data or programme.

The perpetrator of the crime may be any person, and the guilt requires a direct intent characterized by mentioned intention. A sentence of imprisonment of six months to five years is prescribed for this offence.

Generating and introducing computer viruses

The specific crime set out in Article 300 of the Criminal Code consists of generating computer virus with intention of its introduction or the introduction into somebody else's computer or computer network[12].

The object of protection is the security of a computer and computer network from viruses of different kinds and nature, and the object of attack is a computer virus. That is a computer programme or some other set of commands introduced into the computer or computer network generated to multiply itself and affect other programmes or data in a computer or computer network by adding that programme or set of commands to one or more computer programmes or data.

The perpetrator of the crime may be any person, and in practice those are persons having special knowledge in the scope of computers and information technology. As to the guilt, a direct intent characterized by mentioned intention is necessary.

A fine or sentence of imprisonment of up to six months are prescribed for this crime. Equipment and devices for the commission of this crime are obligatorily seized when applying security measure of the seizure of the object.

The heavier form of this crime, for which a fine or sentence of imprisonment of up to two years is prescribed, exists if the damage is caused by a virus generated in this way and introduced into somebody else's computer or computer network[13].

For the existence of the crime it is important that the perpetrator is aware and knows that during the time of committing a crime – work on a computer, they thereby introduce a computer virus into somebody else's computer or computer network. The damage caused thereby may be of material or non-material character. It is important that the damage caused is a result of the commission of a basic crime and that the perpetrator acts with negligence in relation to it.

Computer fraud

Computer fraud set out in Article 301 of the Criminal Code consists of entering incorrect data, failure to enter correct data or otherwise concealing or falsely representing data, thereby affecting the results of electronic processing and transfer of

[12] M. Kokolj, D. Jovašević, Krivično pravo, Opšti i posebni deo, Bijeljina, 2011, pp. 471-474.

[13] D. Jovašević, Lj. Mitrović, V. Ikanović, Krivično pravo Republike Srpske, Posebni deo, Banja Luka, 2017, pp.289-291.

data with intent to acquire for themselves or other person unlawful material gain and thus cause material damage to other person[14].

The object of protection is securing computer systems from entering incorrect and false data and trust in those systems.

Concealing is the failure to enter data by a person who is obliged to enter it into a computer or a computer network. It may involve any data. The false representation of computer data exists when false data (either entirely or partialy false) is represented, published, entered or used in a computer network. Both actions have to be taken in relation to the data which is, by its significance, nature, character and time of entering or use, capable of affecting the result (course and procedure) of electronic processing and transfer of data in computer system[15].

All the actions in terms of the commission of this crime have to be taken with certain intent – intent of the perpetrators to acquire unlawful material gain for themselves or other person. The perpetrator should have that intent during the commission of the crime, but does not have to be acquired in the concrete case. A result of this crime is the violation causing material damage to other person.

The perpetrator of the crime may be any person, and as to the guilt a direct intent characterized by mentioned intention is necessary.

A fine or sentence of imprisonment of up to three years is prescribed for this crime.

The lighter form of crime exists when a perpetrator commits a crime – hiding or falsely presenting data in a computer or computer network in a legally prescribed manner with intention to cause damage to other person, that is, to cause damage to other natural or legal person. Malicious intention of the perpetrator to cause material or non-material damage to other person is a privileged circumstance for which a fine or sentence of imprisonment of up to six months is prescribed under the law.

This crime has two heavier forms.

The first one, for which a sentence of imprisonment of one to eight years is prescribed, exists when material gain (for perpetrator or other person) is acquired by committed basic crime in the amount of over RSD 450,000. The amount of acquired material gain is a qualifying circumstance. It has to be in cause-and-effect connection with the commission of the crime.

The second form of the heavier crime exists if a perpetrator has acquired illegal material gain by committing the crime in the amount of over RSD 1,500,000. A sentence of imprisonment of two to ten years is prescribed for this crime.

Unauthorised Access to Protected Computers, Computer Networks and Electronic Data Processing

This crime set out in Article 302 of the Criminal Code consists of the access to a computer or computer network without authorisation, or the access to electronic data processing without authorisation by breaching protection measures[16].

[14] M. Simović, D. Jovašević, Leksikon krivičnog prava Bosne i Hercegovine, Sarajevo, 2018, pp.691-694.

[15] S. Petrović, Kompjuterski kriminalitet, Bezbednost, Beograd, No. 1/1994.

[16] D. Jovašević, Lj. Mitrović, V. Ikanović, Komentar Krivičnog zakonika Republike Srpske, Banja Luka, 2018, pp.641-644.

The object of protection is the security of a computer or computer network, or the system of electronic data processing protected by special technical and other measures.

The perpetrator of the crime may be any person having specific knowledge in the field of the protection of computers or computer systems. As to the guilt, a direct intent is necessary.

A fine or sentence of imprisonment of up to six months is prescribed for this crime.

This crime has two heavier forms[17].

The first one exists in the case of recording or using computer data obtained by accessing somebody else's computer or computer network or the system of electronic data processing without authorization, given that this has been done by breaching protection measures. A fine or sentence of imprisonment of up to two years is prescribed for this crime. It has no significance which purpose or intention such obtained (recorded) computer data has been used for.

The second heavier form of this crime, for which a fine or sentence of imprisonment of up to three years is prescribed, exists if computer data (one or more) is obtained by accessing somebody else's computer or computer network or somebody else's system of electronic data processing without authorization by breaching protection measures, and it is subsequently used, which results in suspension or serious malfunction in electronic processing and transfer of data or the network, or other serious consequences have occurred for other (natural or legal) person.

Preventing or Restricting Access to Public Computer Networks

The crime prescribed under Article 303 of the Criminal Code consists of preventing or hindering the access to a public computer network without authorization[18].

The object of protection is a public computer network and its free access to individually undefined number of persons. The motive of this incrimination is the prevention of monopoly on using a public computer network.

Prevention prevents other person to access a public computer network completely, permanently or for certain shorter period of time[19]. It may be done by physical prevention, setting some requirements or obstacles, or requesting fulfillment of certain assumptions. Hindering means partial complication, making difficult or inaccessible, or conditioning other person to access or use a public computer network without disturbances and freely, at its own discretion.

The perpetrator of the crime may be any person, and as to the guilt a direct intent is necessary.

A fine or sentence of imprisonment of up to one year is prescribed for this crime.

The heavier form of this crime, for which a sentence of imprisonment of up to three years is prescribed, exists if the crime is committed by an official in dischargingduties.

---

[17] N. Kitarović, Kompjuterski kriminalitet, Bilten sudske praske Vrhovnog suda Srbije, Beograd, No. 2-3/1998.

[18] V. Vodinelić, Metodika otkrivanja, razjašnjenja i dokazivanja računarskog kriminaliteta, Priručnik, Zagreb, No. 4/1990.

[19] Z. Đokić, S. Živanović, Kompjuterski kriminal kao obeležje progresivnog kriminaliteta, Zbornik radova, Kazneno zakonodavstvo – progresivna ili regresivna rešenja, Beograd, 2005.

Unauthorised Use of Computer or Computer Networks

The crime prescribed under Article 304 of the Criminal Code consists of the use of computer services or computer networks without authorization and with intent to acquire unlawful material gain for themselves or other person[20].

The object of protection is the legality and conscientiousness in the use of computer systems – services or networks, from all forms of abuse and negligence.

There has to be an intent of the perpetrator at a time of the commission of the crime, but it does not have to be conducted in the concrete case.

The perpetrator of this crime may be any person, and as to the guilt a direct intent characterized by mentioned intention is necessary.

A fine or sentence of imprisonment of up to three months is prescribed for this crime.

Manufacture, Procurement and Provision of other Means for Committing Criminal Offences against the Security of Computer Data

This is a new computer crime (Article 304a of the Criminal Code) introduced into the Criminal Code by novelty from 2009. Actually, these are punishable preparation acts for the commission of a computer crime.

The crime itself consists of possession, manufacture, procurement, sale or giving other person computer, computer system, computer data or programme intended for committing crimes against the security of computer data for use[21].

The prescribed sentence for this crime is imprisonment from six months to three years, while the objects of the commission of the crime shall be seized from the perpetrator by use of the special security measure of the seizure of the object.

The object of protection in this case is also the security of computer systems and data, which is applied in a specific manner – just before the commission of the crime.

Conclusion

When implementing provisions of numerous relevant European documents finally inaugurated by adoption of the Convention on Cybercrime, the State members of the Council of Europe have created in their national legislations the legal basis for the introduction of a specific kind of „computer" crimes, with the aim to enable performance of various tasks and services by use of a computer with confidence and in an efficient, high-quality, lawful and secure manner.

Accordingly, in the Republic of Serbia many crimes of this kind have been introduced into its criminal and legal system and the legislator, having respect for the established European standards, has provided criminal sanctions for some forms and kinds of

[20] D. Jovašević, Obeležja kompjuterskog kriminaliteta, Pravni informator, Beograd, No. 3/1998.

[21] B. Brvar, Pojavne oblike zlorabe računalnika, Revija za kriminalistiko in kriminologijo, Ljubljana, No. 2/1990.

prescribed computer crimes. Thereby, with appropriate process requirements (establishment of special organs for fighting hi-tech crime within the police, public prosecution and the court), the basis for the efficient fight of our state against these modern forms and kinds of criminality knowing no boundaries between the states has been created.

Literature

[1] B. Petrović, D. Jovašević, *Međunarodno krivično pravo*, Sarajevo, 2010.

[2] D. Jovašević, *Međunarodno krivično pravo*, Niš, 2011.

[3] D. Jovašević, V. Ikanović, *Međunarodno krivično pravo*, Banja Luka, 2015.

[4] D. Jovašević, Komentar Krivičnog zakona Republike Srbije sa sudskom praksom, Beograd, 2003.

[5] Lj. Lazarević, B. Vučković, V.Vučković, *Komentar Krivičnog zakonika Crne Gore*, Cetinje, 2004.

[6] *Official Gazette of republic of Serbia*, No. 85/2005, 88/2005...108/2014 and 94/2016.

[7] D. Jovašević, *Krivično pravo, Posebni deo*, Beograd, 2017.

[8] D. Jovašević, *Leksikon krivičnog prava*, Beograd, 2011.

[9] B. Petrović, D. Jovašević, *Krivično pravo 2, Posebni dio*, Sarajevo, 2005.

[10] D. Jovašević, V. Ikanović, *Krivično pravo Republike Srpske, Posebni deo*, Banja Luka, 2012.

[11] B. Petrović, D. Jovašević, A. Ferhatović, *Krivično pravo 2*, Sarajevo, 2016.

[12] M. Kokolj, D. Jovašević, *Krivično pravo, Opšti i posebni deo*, Bijeljina, 2011.

[13] D. Jovašević, Lj. Mitrović, V. Ikanović, *Krivično pravo Republike Srpske, Posebni deo*, Banja Luka, 2017.

[14] M. Simović, D. Jovašević, Leksikon krivičnog prava Bosne i Hercegovine, Sarajevo, 2018.

[15] S. Petrović, Kompjuterski kriminalitet, *Bezbednost*, Beograd, No. 1/1994.

[16] D. Jovašević, Lj. Mitrović, V. Ikanović, *Komentar Krivičnog zakonika Republike Srpske*, Banja Luka, 2018.

[17] N. Kitarović, Kompjuterski kriminalitet, *Bilten sudske praske Vrhovnog suda Srbije*, Beograd, No. 2-3/1998.

[18] V. Vodinelić, Metodika otkrivanja, razjašnjenja i dokazivanja računarskog kriminaliteta, Priručnik, Zagreb, No. 4/1990.

[19] Z. Đokić, S. Živanović, Kompjuterski kriminal kao obeležje progresivnog kriminaliteta, Zbornik radova, *Kazneno zakonodavstvo – progresivna ili regresivna rešenja*, Beograd, 2005.

[20] D. Jovašević, Obeležja kompjuterskog kriminaliteta, *Pravni informator*, Beograd, No. 3/1998.

[21] B. Brvar, Pojavne oblike zlorabe računalnika, *Revija za kriminalistiko in kriminologijo*, Ljubljana, No. 2/1990.