CRIMINAL OFFENSES AGAINST SECURITY OF COMPUTER DATA IN THE REPUBLIKA SRPSKA ACCORDING TO THE CRIMINAL LAW OF 2017

Academician Miodrag N. Simović, PhD[1]
Constitutional Court of Bosnia and Herzegovina;
Faculty of Law, University of Banja Luka, Republic of Srpska, B&H

Vladimir M. Simović, PhD[2]
Prosecutor's Office of Bosnia and Herzegovina;
Faculty of Security and Protection, Independent University, Banja Luka, B&H

Dragan Jovašević, PhD[3]
Faculty of Law, University of Niš, Serbia

Abstract: In 2003, new criminal legislation came into force in Bosnia and Herzegovina. It is established on the basis of international standards, legal traditions, domestic and foreign legal theory and court practice, but also according to the needs of criminal policy. Of the four criminal laws (Bosnia and Herzegovina, the Federation of Bosnia and Herzegovina, the Brčko District of Bosnia and Herzegovina and the Republika Srpska) with numerous novelties, in 2017, the Republika Srpska passed a completely new Criminal Code. This Code, starting from international obligations, in the first place the Convention on Cyber (computer) Crime from Budapest (2003), establishes a system of criminal offenses against the security of computer data, with a system of criminal responsibility and sanctions for natural and legal parties as perpetrators of these criminal offenses. The concept, elements, characteristics and forms of computer crimes in new legislation of the Republika Srpska are discussed in this paper.

Keywords: computer, abuse, criminal offense, responsibility, punishment.

1 vlado_s@blic.net
2 vladimir.simovic@tuzilastvobih.gov.ba
3 jovashana@ptt.rs

INTRODUCTION

In July 2017, the Republika Srpska passed a new Criminal Code[4] (hereinafter: the Code) which had replaced previously valid Criminal Code[5] from 2003 with numerous amendments. After a short period *vacatio legis*, the Code entered into legal force.

On the basis of numerous international standards, this Code, though based on previous legal tradition applicable at a time of existence of Socialist Federal Republic of Yugoslavia, court practice, understandings of domestic and international legal theory, but also the requirements of modern policy of fight against crime, contains numerous new and original solutions in general, and even more in special part (at incriminations of particular criminal offenses, i.e. their forms and kinds).

Therefore, this Code, in Chapter thirty two under title: „Criminal offenses against security of computer data" stipulates several criminal offences of this kind called computer, information or high-tech criminal offenses.

GENERAL CHARACTERISTICS OF CRIMINAL OFFENSES OF COMPUTER ABUSE

The object of protection of these crimes is security of computer (information) data and systems, that is of computer network (Jovašević, Ikanović, 2012: 185-194). Today, it is common that the concept of computer crime includes these criminal offences. Aside from this name for criminal offenses systematized at this place, they can also be called hi-tech crimes. This concept understands commission of criminal offenses which have computers, computer networks, computer data, computer systems, and their products in material or electronic form, as objects or means of commission of criminal offenses.

Computer represents one of the most significant and most revolutionary products of technical and technological development from the end of 20th Century. However, even besides the advantages the computer has and its huge benefit for the humanity, it soon became a means of abuse of unscrupulous individuals or groups. That is how computer crime appeared as special and specific form of modern crime. Thanks to a huge power of computers in memorizing and fast processing of enormous amount of data, automatized information systems became more and more numerous and irreplaceable follower of the entire human and social life of natural and legal persons.

Various forms of application of computers (Jovašević, 2011: 419-421) in all spheres of life, economy and other social activities, have not remained unspot-

4 "Official Gazette of the Republika Srpska", No. 64/2017.
5 „Official Gazette of the Republika Srpska", Nos. 49/2003, 108/2004, 37/2006, 70/2006, 73/2010 and 49/2013.

ted by unscrupulous and malicous individuals or groups who are trying, without choosing means and ways, to obtain illegal material gain for themselves or other, or to cause damage to another person. Thus a computer becomes a means, a tool for execution of criminal offenses. There are various terms used in theory for different forms and kinds of computer abuse, such as: computer abuse, delicts committed with help of computers, information crime, computer crime, cyber crime, techno crime, etc.

The concept of computer crime understands all various forms, kinds and types of illegal behaviors directed against security of computer and information systems, in their entirety or parts of them, in different ways and with different means, with the intention to obtain gain (of pecuniary or non-pecuniary nature) for themselves or others, or to cause damage to another person.

From such determined concept of computer crime are derived its characteristics (Jovašević, 2017: 211-216):

a) object of protection is security of computer data or information system as a whole or part of it (segment),

b) special, specific character and nature of illegal actions of an individual,

c) special knowledge and specialization of a perpetrator of these criminal offenses which excludes the possibility that every, or any person is found in such a role,

d) special way and means of executioin – with the help or by use (abuse) of computer and

e) intention of a perpetrator, as subjective element at a time the action, which reflects in intention to obtain gain for himself or another person or to cause damage to another natural or legal person, was taken.

Computer crime (Jovašević, 2003: 351-361) is characterized with great dynamics and exceptional variety of shapes, types and forms of its manifestation. It is understandable since this is a new technology with great possibilities for application in a wide scope of human, social and economic activities, and, thus, the possibility of computer abuse is growing from day to day. In addition to new forms of its appearance from before, already known criminal offenses which change traditional, classical way and model of appearance under influence of computer abuse, new forms of illegal behavior, which know no boundaries between the states, appear.

Harmful consequences of computer criminal offences are huge and are manifested in the occurrence of material damage to natural or legal persons (sometimes for the whole country), in the loss of business reputation, the loss of confidence in the safety and truthfulness of computer business and computer data in general, the danger of abuse of freedoms and the rights of a man and citizen in various ways, the disclosure of personal, business and other types of secrets and similar.

The perpetrators of these criminal offenses constitute a specific category of persons. These are mostly non-delinquent and socially adaptable, non-violent

persons. They must possess certain special, professional and practical knowledge and skills in the field of information and computer techniques and technologies for commission of criminal offenses by use of computers. In addition, these are the persons whom such technological means are available in a physical sense.

These criminal offenses are concealed, often without visible spatial and temporal close connection between the perpetrator and the injured party (passive subject). In practice, there is a greater or lesser time difference between the action taken and the moment of the occurrence of the consequence.

These offenses are hard to detect, and even more difficult to prove, they remain practically undiscovered for a long time, until the injured party has suffered damage in the domain of information and computer data or systems. It is a crime that quickly and easily changes forms and shapes of manifestation, the borders between the states, and the type of injured party (Jovašević, Mitrović and Ikanović, 2018: 722-733).

As to guilt, these offenses are committed with intent.

Provisions of Articles 407-413 of the Code provide for the following computer criminal offenses. These are:

a) damagining computer data and programmes,
b) computer sabotage,
c) generating and introducing computer viruses,
d) computer fraud,
e) unauthorized access to protected computers, computer networks, telecommunication network and electronic data processing,
f) preventing or restricting access to public computer network,
g) unauthorized use of computer or computer network.

DAMAGING COMPUTER DATA AND PROGRAMMES

Concept and elements of criminal offense

This is the first computer crime stipulated under Article 407 of the Code. It consists of unauthorized deletion, alteration, damage, concealement or otherwise making unusable computer data or programme (Petrović, Jovašević, 2005: 278-285).

Object of protection is security of computer data or computer programme, and object of the attack is: a) computer data, and b) computer programme.

Computer data is any representation of facts, information or concept in a form that is suitable for their processing in a computer system, including an appropriate programme on the basis of which computer system performs its function.

Computer programme is a set of commands that governs the operation of computers, as well as to solve a specific task with a computer.

Execution has multiple alternative determinations. It consists of (Jovašević, Mitrović and Ikanović, 2017: 357-367): a) deletion, b) alteration, c) damage, d)

concealement and f) making unusable a computer data or programme. For the existence of this offence it is important that the action be taken without authorization, and accordingly, by unauthorized persons, in a manner and by action that are not allowed and not stipulated by the law.

Deletion is removal of computer data, entirely or partialy, or computer programme.

Alteration is partial change of existing data or entry of new data by persons in the proceedgins not being prescribed under appropriate provisions or under appropriate procedure.

Damage is provisional, partial or short-term disabling of use of computer data or programme by causing malfunctions or by tearing of some parts, connections or circuits, so that computer data or programme cannot be used during a certain period of time for the purpose they were intended.

Concealement is the transfer of data or programme from a place it was stored or confined and its removal to another, most often, unknown place.

Making computer data or programme unusable in another way is any other disabling for shorter or longer time or disabling its use to a greater or lesser extent.

The consequence of this offense is the violation of protected goods – computer data or programme which belongs to a natural or legal person in sense of its usability, usefulness in general or for a particular time, at a particular place or for a particular purpose.

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

A fine or sentence of imprisonment for up to one year is prescribed for this crime. The perpetrator shall be obligatory imposed a security measure of seizure of equipment and devices used for the commission of the criminal offence.

Aggravated forms of criminal offense

Criminal offense from Article 407 of the Code have two aggravated forms for which more severe punishment of perpetrators are prescribed.

The first aggravated form of this crime, for which a sentence of six months to three years of imprisonment is prescribed, exists if the action taken in the execution of the crime caused damage amounting to over KM 10,000. The amount of caused material damage to another natural or legal person, which is determined according to market conditions at a time of commission of the criminal offense in legally prescribed amount, constitutes qualification circumstance.

The second aggravated form of this crime is qualified by scope and intensity of caused consequence. For this offense a sentence of one to five years of imprisonment is prescribed. This criminal offense exists if the action taken in the execution of the crime caused material damage to another natural or legal person, amounting over KM 50,000, whose amount is also established according to market conditions at the time of commission of the criminal offence in question.

COMPUTER SABOTAGE

Article 408 of the Code stipulates criminal offense called „Computer Sabotage". The offense (Petrović, Jovašević and Fehatović, 2016: 428-438) is committed by whoever enters, destroys, deletes, alters, damages, conceals or otherwise makes unusable computer data or programme 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 important for republic authorities, public services, institutions, economic enterprises or other entities.

The object of protection is determined twofold, as: a) computer data or programme, and b) computer of other device for electronic processing and transfer of data. It is important that these devices and resources belong, i.e. that they are important for republic organ, public service, institution, economic enterprise or other entity.

The action of execution is alternatively determined (Turković et al., 2013: 341-347) as: a) entry, b) destruction, c) deletion, d) alteration, e) damage, f) concealement, and g) otherwise making unusable of computer data or programme, i.e.: a) destruction, and b) damaging of computer or another device for electronic processing and transfer of data.

Entry is input or storing of new, previously unexisting, data or alteration of already existing computer or other data into computer programme.

Destruction is complete or permanent destruction of substance and shape of particular object so it cannot be used for a purpose and intention it was previously used for.

Deletion is removal of computer data or programme most often mechanically or otherwise, in its entirety or partially.

Alteration is partial change of existing data in term of its content, place of its whereabouts or its nature or entering of other false data into computer system.

Damage is termporary, partial or short-term disabling of computer data, programme, computer or other device for the purpose they were intended for.

Concealement is removal of data or objects from a place they were located before, which was known to everyone, and its transfer to another, most often, hidden place, so that another person cannot know about its content at all or for a particular period of time.

Making unusable of computer data or programme constitutes any action affecting the usability of computer data or programme, to a greater or lesser extent.

Depending on the object of attack, which the action of execution of this criminal offense is directed against, two of its forms may be distinguished. These are (Đorđević, 2011: 177-182):

a) destruction or damaging of computer data or programme, and

b) destruction or damaginig of computer or other device for electronis processing and transfer of data.

For the existence of both forms of this criminal offense, it is necessary two more elements are cumulatively fulfilled. These are:

a) that the action of execution is taken in relation to objects that belong to a republic authority, public service, institution, economic enterprise or another entity (legal person with special authorizations). Accordingly, the capacity of the damaged person constitutes an element of criminal offense, and

b) that the perpetrator, at a time of taking the action, has certain intention – to prevent (completely and permanently) or considerably disrupt (makes it more difficult) the procedure of electronic processing and transfer of data. It is not significant whether this intention in the specific case has been achieved, but that it existed at a time the perpetrator took the action of execution.

Consequence of this offense is harm to a computer data, programme, computer or device for automatic transfer or processing of data in term of thier usability and usefulness.

Perpetrator of the offence may be any person, and the guilt requires direct intent characterized by alleged intention.

A sentence of imprisonment for a term of six months to five years is prescribed for this offence.

GENERATING AND INTRODUCING COMPUTER VIRUSES

Article 409 of the Code prescribes a criminal offense which consists of generating a computer virus with intention of its introduction into somebody else's computer, computer or telecommunication network (Babić, Marković, 2007: 206-207).

Object of protection is security of computers, computer or telecommunication network from viruses of different kind and nature, and object of attack is a computer virus. This is a computer programme or other set of orders introduced into a computer or a computer network, which is created to multiply itself and act on other programs or data in a computer or computer network by adding this program or set of orders to one or more computer programmes or data (Kokolj, Jovašević, 2011: 357-369).

This action of execution (Pavišić, Grozdanić and Veić, 2007: 554-562) is generating – making of previously non-existing computer virus which is capable, sufficient or which may cause certain changes or damages in use and usability of computers, computer or telecommunication network in its entirety or part of it.

It is importatnt that the action of execution of this crime is taken with certain intention (as subjective element) – intention to introduce such generated

computer virus into somebody else's computer, computer or telecommunication network. The perpetrator has to have the intention at a time the action was taken, notwithstanding whether the intention has been achieved in a particular case.

Perpetrator of the crime may be any person. As to the guilt, a direct intent characterized by mentioned intention is necessary.

A fine or sentence of imprisonment for a term of up to six months is prescribed for this offense. In addition to the sentence, the perpetrator is obligatory imposed a security measure of seizure of equipment and devices used to commit the crime.

More aggravated form of this crime, for which a fine or sentence of imprisonment for a term of up to two years is prescribed, exists if a computer virus is introduced, indirectly or directly, into somebody else's computer or computer network which, thereby, causes damage (pecuniary or non-pecuniary). Accordingly, the consequence of a criminal offence appears in a form of violation – damage caused to another natural or legal person, and even the whole state.

COMPUTER FRAUD

„Computer fraud" is a criminal offense stipulated under Article 410 of the Code. This offense consists of entering of incorrect data, failure to enter correct data or otherwise concealing or false representation of data, thereby affecting the results of electronic processing and transfer of data with the intent to acquire for themselves or another person unlawful material gain and thus causing peroperty damage to another person (Mrvić Petrović, 2005: 321-325).

Object of protection is security of computer systems from entering incorrect and false data and trust in those systems.

The action of execution consists of two alternatively foreseen activities. These are[6]:

a) concealing, and

b) false representation of computer data.

Concealing is failure to enter a data by a person who is obliged to enter it into a computer or computer network. This may be any kind of data.

False representation of computer data exists when incorrect data is presented, published, entered or used in a computer network (notwithstanding whether it is entirely or partially incorrect).

Both activities have to be taken with respect to the data which is capable of affecting the result (course and procedure) of electronic processing and transfer of data in a computer system, by its significance, nature, character, time of entry or use.

6 The Criminal Code of Monte Negro. Podgorica: Official Gazette of Monte Negro, 2016, pgs. 174-177.

For the existence of this criminal offense it is important that the execution be taken as follows (Đorđević and Đorđević, 2016: 191-194):

1. in a certain manner: a) by entering of incorrect (false) data in its entirety or part of it, b) by failure to enter, non-entering, non-registration of some important data (this means not any data, but only the data that is important for a particular case) or c) otherwise,
2. with certain intent of perpetrator at a time they committed the offense, but this intention does not have to be achieved in a particular case – intent to obtain unlawful material gain for themselves or another natural or legal person, and
3. in such a manner that a consequence of committed offense is violation – causing of material damage to another natural or legal person. This may be any amount of damage having cause-and-effect connection with action of execution, notwithstanding whether a damaged party is owner or user of computer network.

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 for a term of up to three years is prescribed for this crime.

Special forms of criminal offense

In addition to its basic form, this criminal offense has two special forms. These are (Lazarević, Vučković and Vučković, 2004: 816-824):

a) less aggravated form, and
b) more aggravated forms.

Less aggravated form of crime, for which a fine or sentence of imprisonment for a term of up to six months is prescribed, exists when a perpetrator committed a crime – concealing or false presentation of data in a computer or computer network in a legally prescribed manner with the intention to cause damage to another person, that is, to cause damage to another natural or legal person.

Malicious intention of the perpetrator to cause material or non-material damage to another person is a privileged circumstance.

This criminal offense also has two more aggravated forms.

The first more aggravated form, for which a sentence of imprisonment for a term of one to eight years is prescribed, exists when material gain (for perpetrator or another person) is acquired by committing this crime in the amount of over BAM 10,000. The amount of acquired material gain is a qualifying circumstance. It has to be in cause-and-effect connection with action taken to committ a crime.

The second form of more aggravated crime, for which a sentence of imprisonment for a term of two to ten years is prescribed, exists if a perpetrator acquired illegal material gain by committing this crime in the amount over BAM 30,000.

UNAUTHORIZED ACCESS TO PROTECTED COMPUTERS, COMPUTER NETWORKS, TELECOMMUNICATION NETWORK AND ELECTRONIC DATA PROCESSING

Concept and elements of criminal offense

The criminal offence set out in Article 411 of the Code consists of access to a computer or computer network without authorization, or access to electronic data processing without authorization by breaching protection measures, or in making, obtaining, sale or giving for use the instructions or devices intended to enter into a computer system (Selinšek, 2007: 424-427).

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

The action of execution is multiply determined alternatively (Simić, Trešnjev, 2010: 210-214), as:

a) Unauthorized access to a computer or computer network or electronic data processing. That is entry, penetration, access into protected system of computer data, into the system of electronic processing or transfer of data, as well as into entire computer network or part of it.

It is important that this is a computer, computer system or system of electronic data processing, protected by a special security measures. Therefore, the action of execution is taken in a special legally prescribed manner: a) without authorization, thus, unlawfully, and 2) by breaching security measures (acting contrary to all prescribed measures of some of the measures, by doing or failure to do),

a) making – production of previously non-existing device,

b) obtaining – getting in posession of device in any way,

c) sale – exchange of device for domestic or foreign money, and

d) giving for use – helping, making it easier, enabling someone else to get into possession of the device.

For the existence of this form of criminal offence (Jovašević, 2003: 351-361) it is important that the actions of: making, obtaining, sale or giving for use are taken in relation to introduction or device intended to enter into a computer system.

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

A fine or a sentence of impirsonment for a term of up to six months is prescribed for this crime.

More aggravated forms of criminal offense

This criminal offense has two more aggravated forms for which the Code prescribes more severe punishments.

The first more aggravated form of this crime, for which a fine or a sentence of imprisonment for a term of up to two years is prescribed, exists in case of recording or use of a computer data, obtained by accessing somebody else's computer or computer network, or somebody else's system of electronic data processing without authorization, given that it was done by breaching of protection measures. It is not important for which purpose or intention such obtained (recorded) computer data was used.

The second more aggravated form of this crime, for which a sentence of imprisonment for a term of up to three years is prescribed, exists if accessing somebody else's computer or computer network, or somebody else's system of electronic data processing without authorization by breaching protection measures:

a) results in breach – suspending (disabling) or considerately disrupting (making more difficult) the functioning of electronic processing and transfer of data or network, and

b) results in other serious consequences. What are serious consequences is factual issue which the court resolves in each individual case. These consequences are a result of negligence of a perpetrator and are in cause-and-effect connection with taken action to commit a crime.

PREVENTING AND RESTRICTING ACCESS TO PUBLIC COMPUTER NETWORK

Article 412 of the Code prescribes a specific computer criminal offense consisting of unauthorized prevention or obstruction of access to public computer network (Jovašević, Mitrović and Ikanović, 2018: 722-733).

Object of protection is public computer network and free access to it by individually undefined number of persons. Motive of this incrimination is prevention of monopoly in the use of public computer network.

The action of execution is twofold determined alternatively (Petrović, Jovašević, Ferhatović, 2016: 428-437), as:

a) preventing, and

b) restricting free access to public computer network.

Preventing is completely, permanently or for a particular shorter period of time disabling another person to access public computer network. This may be done by physical prevention, by setting of certain conditions or obstacles, or by requiring the fulfillment of certain assumptions.

Restricting is partial complicating, aggravating, making unavailable, or causing another person to access or use public computer network undisturbedly, freely, and at his discretion.

It is important that this action, in any of mentioned forms, is taken without authorization (by unauthorized person, without complying with requirements and assumptions and out of the proceedings pescribed under the law or other pro-

visions regulating this field) in relation to public computer network (Jovašević, Ikanović, 2012: 185-197).

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

A fine or sentence of impirsonment for a term of up to one year is prescribed for this crime.

More aggravated form of this crime, for which a fine or sentence of imprisonment for a term of up to three years is prescribed, exists if the crime is committed by:

a) a particular person - an official, and

b) in a specific manner - in discharge of his or her duty.

Capacity of a perpetrator and manner of their actions to commit the crime, constitute qualifying circumstances.

UNAUTHORIZED USE OF COMPUTER OR COMPUTER NETWORK

Article 413 of the Code stipulates the last computer criminal offense. It is called: „Unauthorized use of computer or computer network". The offense consists of the use of a computer services or computer networks without authorization and with intent to acquire unlawful material gain for himself or another person (Jovašević, Mitrović, Ikanović, 2017: 357-367).

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

Execution (Jovašević, Mitrović and Ikanović, 2017: 357-367) unauthorized use, accordingly, exploitation, making use of the data obtained or stored in somebody else's computer or computer network with greedy intention - the intention of the perpetrator to obtain in this way unlawful material gain for himself or another natural or legal person.

There has to be intent of a perpetrator at a time they committed the crime, but it does not have to be realized in a particular case.

A perpetrator of 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 for a term of up to six months is prescribed for this crime. Prosecution for this crime is conducted upon a proposal.

CONCLUSION

New Criminal Code of the Republika Srpska recognizes several criminal offences, established on the basis of obligations Bosnia and Herzegovina undertook by signing and ratifying of Budapest Convention on Computer Crime.

These are criminal offences against safety of computer data, and the title itself of Head XXXII of the Code points out to the object of protection of these criminal offences.

As objects of attack various legal goods appear, as well as the execution consists of various actions, such as: deletion, entry, alteration, destruction, damage, making the object of attach unusable, or even generating (producing) of computer virus or its introduction into computer system.

Any person may appear as a perpetrator of these crimes, according to legal provisions, but in the practice these are persons having specific, special knowledge in computers or in the field of information technologies. These criminal offences, as a rule, are committed with intent, and in some cases they are expressed as direct intent – due to existence of a certain intention (greedy or malicious) of the perpetrator at a time the crime was committed.

REFERENCES

1. Babić, M. i Marković, I. (2007). *Krivično pravo, Posebni dio*. Banja Luka: Pravni fakultet.
2. Criminal Code of Monte Negro. *Official Gazette of Monte Negro*, 2016.
3. Criminal Code of the Republika Srpska, *Official Gazette of the Republika Srpska*, Nos. 49/2003, 108/2004, 37/2006, 70/2006, 73/2010 and 49/2013.
4. Criminal Code of the Republika Srpska, *Official Gazette of the Republika Srpska*, No. 64/2017.
5. Đorđević, Đ. (2011). *Krivično pravo, Posebni deo*. 2. Izmenjeno i dopunjeno izd. Beograd: Kriminalističko-policijska akademija.
6. Đorđević, M. i Đorđević, Đ. (2016). *Krivično pravo*. Beograd: Organizacija za pravnu edukaciju i kulturu prava Projuris.
7. Jovašević, D. (2003). *Komentar Krivičnog zakona Republike Srbije: sa sudskom praksom*. Beograd: Nomos.
8. Jovašević, D. (2011). *Leksikon krivičnog prava*. 4. Izmenjeno i dopunjeno izd. Beograd: Službeni glasnik.
9. Jovašević, D. (2017). *Krivično pravo, Posebni deo*. Beograd: Dosije.
10. Jovašević, D i Ikanović, V. (2012). *Krivično pravo Republike Srpske, Posebni deo*. Banja Luka: Panevropski univerzitet Apeiron.

11. Jovašević, D., Mitrović, Lj. i Ikanović, V. (2017). *Krivično pravo Republike Srpske, Posebni deo*. Banja Luka: Panevropski univerzitet Apeiron.
12. Jovašević, D., Mitrović, Lj. i Ikanović, V. (2018). *Komentar Krivičnog zakonika Republike Srpske*. Banja Luka: Službeni glasnik republike Srpske.
13. Kokolj, M. i Jovašević, D. (2011). *Krivično pravo Republike Srpske, opšti i posebni dio*. Bijeljina: Univerzitet Sinergija.
14. Lazarević, Lj., Vučković, B. i Vučković, V. (2004). *Komentar Krivičnog zakonika Crne Gore*. Cetinje.
15. Mrvić-Petrović, N. (2005). *Krivično pravo*. Beograd: Fakultet za poslovno pravo.
16. Pavišić, B., Grozdanić, V. i Veić, P. (2007). *Komentar Kaznenog zakona*. 3. izmijenjeno i dopunjeno izd. Zagreb: Narodne novine.
17. Petrović, B. i Jovašević, D. (2005). *Krivično parvo. 2, Posebni dio*. Sarajevo: Pravni fakultet.
18. Petrović, B., Jovašević, D. i Ferhatović, A. (2016). *Krivično pravo II: saučesništvo, krivične sankcije i posebni dio)*. Sarajevo: Pravni fakultet.
19. Selinšek, Lj. (2007). *Kazensko pravo, Splošni del in osnove psoebnega dela*. Ljubljana: GV založba.
20. Simić, I. i Trešnjev, A. (2010). *Krivični zakonik sa kraćim komentarom*. Beograd: Ing pro.
21. Turković, K. et al. (2013). *Komentar Kaznenog zakona*. Zagreb: Narodne novine.