DOI: 10.7251/GFP2414005S

UDC: 343.533:004.738.5(497.6)

Originalni naučni rad

Datum prijema rada:
3. april 2024.

Datum prihvatanja rada:
21. maj 2024.

Computer Fraud in the Law of Bosnia and Herzegovina and International Standards

Miodrag N. Simović
Academician, full member of the Academy of Sciences and Arts of Bosnia and Herzegovina, full professor at the Faculty of Law, University of Bihać, professor emeritus, msimovic@anubih.ba; https://orcid.org/0000-0001-5116-680X

Vladimir M. Simović
Prosecutor's Office of Bosnia and Herzegovina; full professor at the Faculty of Security and Protection of the Independent University in Banja Luka, vlado_s@blic.net; https://orcid.org/0009-0002-9640-6488

Abstract: In the modern criminal legislation in general, and also in the positive law of Bosnia and Herzegovina, several different criminal offenses of fraud are prescribed. These criminal offenses are systematized in different groups of offenses according to different protective objects, but with more or less identical acts of execution with the intention/goal of obtaining benefits for oneself or for another person, i.e. with the intention/goal of causing harm to another person. These are: a) voting fraud (or election fraud), b) fraud in business operations (or insurance fraud), c) fraud, d) service fraud, and e) computer fraud. In the system, a set of several different forms of manifestation of criminal offenses of fraud, a criminal offense of computer fraud prescribed by three criminal laws (except the Criminal Code of Bosnia and Herzegovina) has specific character, nature and content. This incrimination is based on relevant international standards contained in the Council of Europe Convention on Cyber (computer) crime (Budapest, 2001). This paper presents the concept, characteristics, elements and content of the criminal offense of computer fraud in accordance with legal solutions with application in Bosnia and Herzegovina.

Key words: computer fraud, law, criminal offense, responsibility, international standards.

1. INTRODUCTION

In the positive criminal legislation of Bosnia and Herzegovina, three laws (except the Criminal Code of Bosnia and Herzegovina[1]) in different groups of offenses provide for responsibility and punishment for several criminal offenses of fraud. The basic criminal offense of this type - "fraud" is otherwise a property crime, a crime against the property, property rights or property interests of other physical or legal persons. It is prescribed in Article 294 of the Criminal Code of the Federation of BiH (CCFBiH)[2], Article 288 of the Criminal Code of the

[1] *Official Gazette of Bosnia and Herzegovina* nos. 3/2003, 32/2003, 37/2003, 54/2004, 61a/2004, 30/2005, 53/2006, 55/2006, 32/2007, 8/2010, 47/2014, 22/2015, 40/2015, 35/2018, 46/2021, 31/2023 and 47/2023.

[2] *Official Gazette of the Federation of Bosnia and Herzegovina* nos. 36/2003, 37/2003, 21/2004, 69/2004, 18/2005, 42/2010, 42/2011,

Brčko District of BiH (CCBDBiH)[3], and Article 230 of the Criminal Code of the Republika Srpska (CCRS)[4].

In addition to fraud, as a property crime, the criminal law of Bosnia and Herzegovina also provides for several specific, special forms of fraud crimes. These are:

1) voting fraud - article 196 of the CCFBiH and article 193 of the CCBDBiH (crimes against the freedoms and rights of a human and citizen), i.e. election fraud - article 222 of the CCRS (crimes against electoral rights),

2) fraud in business operations - Article 251 of the CCFBiH, Article 245 of the CCBDBiH and Article 272(a) of the CCRS (crimes against the economy, business and security of payment transactions - CCFBiH and CCBDBiH, i.e. crimes against the economy and payment transactions - CCRS),

3) creditor fraud - Article 299 of the CCFBiH and Article 293 of the CCBDBiH (crimes against property),

4) insurance fraud - Article 273 of the CCRS (crimes against economy and payment transactions),

5) fraud in office - Article 385 of the CCFBiH, Article 279 of the CCBDBiH and Article 317 of the CCRS (crimes of bribery and crimes against official and other responsible functions - CCFBiH and CCBDBiH, i.e. crimes against official duty - CCRS), and

6) computer fraud - Article 395 of the CCFBiH, Article 389 of the CCBDBiH and Article 410 of the CCRS (crimes against electronic data processing systems - CCFBiH and CCBDBiH and crimes against computer data security - CCRS).

The basis of the incrimination of computer fraud, which represents a form of computer (cyber, information) crime, are the relevant standards of the Budapest Convention of the Council of Europe from November 2001 - the Convention on Cyber (computer) crime[5] (ETS 185).

2. CONVENTION ON COMPUTER CRIME AND COMPUTER FRAUD

2.1. System of international standards

The Convention on Cybercrime is a basic international document that lays the foundation for the prevention and suppression of various computer crimes in the legislation of the member states of this most numerous European regional organization[6]. In several provisions of the second Chapter entitled: "Substantive Criminal Law", it defines the concept, content, elements and characteristics of several different criminal offenses related to computers contained in individual national criminal legislation of member states of the Council of Europe[7]. Thus, the following computer crimes are systematized there:

59/2014, 76/2014, 75/2017 and 31/2023.

3 *Official Gazette of Brčko District of Bosnia and Herzegovina* no. 19/2020.

4 *Official Gazette of Republika Srpska* nos. 64/2017, 104/2018, 15/2021, 89/2021 and 73/2023.

5 Convention on Cybercrime, Budapest, 23 November 2001, entered into force on 1 July 2004, entered into force with regard to BiH on 1 September 2006; published in *Official Gazette of BiH – International Treaties* no. 6/2006.

6 See Pavišić, B. (2016). *Kazneno pravo Vijeća Evrope*, Zagreb: Golden marketing -Tehnička knjiga, 261-265.

7 See Hilgedorf, E.,Valerius, B. (2012). *Computer und Internet Strafrecht*, Heidelberg: Springer, 107-125.

1) criminal offenses against the confidentiality, integrity and availability of computer data and systems (Art. 2-6) where the following offenses are foreseen: a) illegal access, b) illegal interception, c) data interference, d) system interference, and e) misuse of the devices,

2) computer-related offenses (Art. 7-8), which include two crimes: a) computer-related forgery, and b) computer-related fraud,

3) content-related offenses (Article 9) - offenses related to child pornography, and

4) offenses related to infringements of copyright and related rights (Article 10) without further specifying which criminal offenses of this type or nature are involved in the specific case.

Two protocols were adopted to the Convention on Cybercrime: the Additional Protocol concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems[8] from 2003 and the Second Additional Protocol on enhanced co-operation and disclosure of electronic evidence[9] from 2022. Although adopted within the framework of the Council of Europe, the Convention on Cybercrime is also open to non-member states and is currently the only international treaty of global scope, which reflects its particular significance.

The Additional Protocol Concerning the Criminalization of Acts of a Racist and Xenophobic Nature Committed through Computer Systems (Articles 3-7) prescribes the criminal liability of natural or legal persons, as well as their punishment for the misuse of computers with the aim of committing criminal offenses based on racist and xenophobic impulses (motives).

However, these three regional documents are not the only international documents that regulate the domain of prevention or suppression of computer crime in different forms or types of manifestation. Thus, the following European recommendations can be cited here, as acts of lower legal force[10]: a) Recommendation No. R(85)10 on the practical application of the European Convention on Mutual Assistance in Criminal Matters regarding the provision of international criminal law assistance in the interception of communications; b) Recommendation No. R(88)2 on piracy in the field of copyright and related rights, c) Recommendation No. R(87)15 which prescribes the use of personal data in the field of police activities; d) Recommendation No. R(95)4 on the protection of personal data in the area of telecommunication services with particular reference to telephone services, e) Recommendation No. R(89)9 on computer-related crime, which provides guidelines to national authorities in terms of defining certain computer crimes, and f) Recom-

---

[8] Additional Protocol on the Convention on Cybercrime, Concerning the Criminalization of Acts a Racist and Xenophobic Nature Committed through Computers Systems, Strasbourg, 28 January 2003, entered into force on 1 March 2006, entered into force with regard to BiH on 1 September 2006; published in *Official Gazette of BiH – International Treaties* number 6/2006.

[9] Council of Europe Treaty Series – No. 224. Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence, *https://rm.coe.int/1680a49dab*. Adopted in 2022 and has not entered into force yet. The purpose of this Protocol is to supplement: a) The Convention on Cybercrime, whose signatories are the contracting states of this protocol, and b) The First Additional Protocol between contracting parties of this protocol, which are, at the same time, signatories of the First Protocol.

[10] See Jovašević, D. (2014). Računarski kriminalitet u Srbiji i evropski standardi. Beograd: *Evropsko zakonodavstvo*, *47-48*, 40-56.

mendation No. R(95)13 on the problems of criminal procedural law related to information technology.

The Convention on Cybercrime foresees legal means, measures and procedures for preventing illegal activities that are directed against the secrecy, integrity and availability of computer-related systems, networks and computer data, as well as for deterring any form of their abuse[11]. This contributes to the detection, research and proof of criminal offenses of computer abuse, i.e. the criminal prosecution of their perpetrators[12].

Article 1 of the Convention on Cybercrime under title: "Definitions" defines basic terms of computer-related crime, which gives definitions of the following concepts: a) computer system, b) computer data, c) service provider, and d) traffic data.

A computer system means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data. The term "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function. The term "service provider" includes: a) any public or private entity that provides to users of its service the ability to communicate by means of a computer system, b) any other entity that processes or stores computer data on behalf of such communication service or users of such service. Finally, the term "traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service.

2.2. Computer-related fraud as an international crime

The Convention on Cybercrime in the second chapter entitled: "Substantive criminal law" defines the concept, content, elements and basic characteristics of computer-related fraud (Article 8) under the name "Computer-related fraud". This offense is systematized in the group of "computer crimes", in addition to the offense of Computer-related forgery (Article 7) – forgery related to computers.

"Computer-related fraud" consists in input (entering, writing a new, previously nonexisting data), alteration (change, alteration of a form or content of already existing, previously entered data), deletion (physical removal of data from the place where it previously existed) or suppression (moving the data from the place where it was located to another unknown, most often hidden place that is not accessible or known to other persons) of computer data or in making computer data unusable or in any interference with the functioning of the computer system with intent to defraud, or dishonest intent, in order to unlawfully obtain an economic benefit for oneself or for another person[13]. The mentioned activities included in the description of the execution action are undertaken in relation to

[11] See Pavišić, B., Kamber, K., Parenta, I. (2016). *Kazneno pravo Vijeća Europe*, Rijeka: UGent, 127-141.

[12] See Zvrlevski, M., Andononova, S., Miloševski, V. (2014). *Priračnik za kompjuterski kriminal*, Skopje: OSCE, 78-93.

[13] See Atanasov, R. (2021). *Priračnik za zaštitata od izmami i kompjuterski kriminal*, Skopje: Akademik, 114-127.

computer data[14].

In addition to these activities, the Convention on Cybercrime prescribes "any interference with the functioning of a computer system" as an action of execution of this criminal offense[15]. It is the activity of doing (positive, active action) or not doing (negative, passive action) which temporarily or partially hinders or complicates the efficient, quality and timely functioning of a computer system.

Certain social values appear as an object of this international criminal offense (the characteristics of which are prescribed by international documents). Given that the theory of criminal law distinguishes two types of objects, a dual set of values appears as the object of protection in this criminal offense. These are: a) security of computer data, and b) property (movable or immovable) of another natural or legal person. On the other hand, this offense has the following objects of attack: a) computer data, and b) computer system[16].

For the existence of this criminal offense two more constitutive elements have to be met - that the act of execution prescribed by the Convention is undertaken in any of several alternative forms of manifestation that are prescribed[17]:

a) with a certain intention - fraudulent intention or dishonorable (defamatory) intention to obtain in this way an unlawful property benefit for the perpetrator of the offense or for another natural or legal person, without authorization. This intention indicates the existence of direct intent as a form of the perpetrator's guilt. Such an intention must exist on the part of the perpetrator at the time of undertaking the action of execution, but it does not have to be realized in each specific case, and

b) in a particular, specific way - unlawfully, by violating the existing (legal or by-law) rules of behavior[18].

The consequence of the criminal offense of computer-related fraud is reflected as a violation of protected good[19]. It is the occurrence of property (material, economic) damage to any other natural or legal person, regardless of its type, scope or amount. Namely, the amount of property damage is determined as factual issue according to the market conditions that existed at the time of the execution of the offense. Property damage occurs in the form of a reduction (diminution) of existing property (actual damage - *damnum emergens*) or in the form of preventing the increase of existing property (lost profit - *lucrum cesans*).

In addition to directly causing the consequences of the criminal offense of computer-related fraud (in the form of a completed criminal offense), the Convention on Cybercrime recommends the member states of the Council of Europe to prescribe penalties in the fol-

---

[14] Mrvić Petrović, N. (2005). *Krivično pravo*, Beograd: Fakultet za poslovno pravo**,** 324.

[15] See Kareklas, S. (2009). *Priručnik za krivično pravo Evropske unije*, Beograd: Institut za uporedno pravo, Mladi pravnici Srbije, 94-97.

[16] See Jovašević, D. (2021). Računarska prevara - krivična odgovornost i kažnjivost u međunarodnom i nacionalnom pravu, Zbornik radova *Pravo i digitalizacija*, Niš, 51-73.

[17] See Dragićević, D. (1999). *Kompjutorski kriminalitet i informacijski sustavi*, Zagreb: Informator, 71-84.

[18] See Vojković, G., Štambuk Šunjić, M. (2006). Konvencija o kibernetičkom kriminalu i Kazneni zakon Republike Hrvatske, *Zbornik Pravnog fakulteta u Splitu*, Split, *1*, 123-136.

[19] See Završnik, A. (2015). *Kibernetska kriminaliteta*, Ljubljana: IUS Software, GV založba, Institute of Criminology at the Faculty of Law, 81-94.

lowing cases[20]: a) for the attempt to commit the offense (when, despite the committed act of execution with intent, the consequence of the offense is absent, does not occur), and b) for certain forms of complicity (for inciting - leading to its execution or for helping - facilitating, enabling its execution).

Attempt (uncompleted offense), aiding or abetting the commission of a criminal offense (Article 11, Part Five of the Convention on Cybercrime) are punishable actions in case they are undertaken with the intent (intention) of the perpetrator[21]. Thus, each party shall adopt such legislative and other measures as may be necessary to establish as criminal offenses under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offenses established in accordance with Articles 2 through 10 of the present Convention with intent that such offense be committed. In addition, each party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offenses established in accordance with Articles 3 through 5, 7, 8, and 9(1)(a) and (c) of this Convention. Also, each party may reserve the right not to apply, in whole or in part, paragraph 2 of this Article.

In addition to a natural person, legal entities can also be held liable (Article 12 of the Convention on Cybercrime), to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on: a) a power of representation of the legal person; b) an authority to take decisions on behalf of the legal person; c) an authority to exercise control within the legal person.

3. COMPUTER FRAUD IN THE LEGAL SYSTEM OF BOSNIA AND HERZEGOVINA

3.1. Characteristics of the offense of computer fraud in the legislation of the Federation of BiH and of Brčko District of BiH

From the aspect of analysis of the concept, elements, content, elements of existence, characteristics, and form of manifestation of the criminal offense of computer fraud, it should be pointed out that there are three criminal laws in force in Bosnia and Herzegovina[22].

CCFBiH in chapter XXXII: "Criminal offenses against electronic data processing systems" (Article 395) provides for the criminal offense of "Computer fraud". This criminal offense consists in the unauthorized entry, damage, alteration or concealment of computer data or programs or otherwise influencing the result of the electronic data processing with the aim of acquiring unlawful material gain for himself or for another, thus causing (inflicting) material damage to somebody else[23]. This is a specific, special form of the material crime

[20] See Peršak N. *et al*. (2006). *Računalniška/kibernetička kriminaliteta v Sloveniji*, Ljubljana: Inštitut za kriminologijo pri Pravni fakulteti, 104-126.

[21] See Vestbi, Dz. *et al.* (2004). *Međunarodni vodič za borbu protiv kompjuterskog kriminala*, Beograd: Produktivnost AD, 89-101.

[22] See Dedović, A., Stanojković, D. (2021). Kompjuterski kriminalitet – opća razmatranja, Zbornik radova *Sigurnost i društvo*, Mostar, 485-496.

[23] See Budimlić, M., Puharić, P. (2009). *Kompjuterski kriminalitet – kriminološki, krivičnopravni, kriminalistički i sigurnosni aspekt*, Sarajevo: Fakultet za kriminalistiku, kriminologiju i sigurn-

of fraud, which is characterized by a special, specific method, that is, the means of execution - a computer[24].

The object of protection of this offense is the legal, efficient, high quality, orderly and timely functioning, running of the electronic processing of computer data system[25].

The object of the attack is alternatively defined as: a) computer data or program[26], and b) electronic data processing system.

Depending on the type of object of the attack against which a certain activity is directed, we differ the execution actions undertaken according to: a) computer data or program, and b) according to the electronic data processing system.

The action of execution consists of the following alternatively foreseen activities that differ according to the type of object of the attack against which they are directed. These are[27]:

1) actions performed on computer data or a program. These include: a) entry - entering, displaying new, previously not existing data, whether true/correct or false/incorrect, in whole or in part, b) damage - temporary, partial or short-term aggravation, or making the data unusable for temporary use, but its usefulness can be increased or re-established, c) alteration - change, alteration, modification, transformation of data so that it acquires a different form, meaning, meaning or value, d) concealment[28] - withholding, not entering, not writing down a data, or complete or partial failure to enter a data, in general or within a certain period of time, by a person who is obliged to enter that data into a computer or a computer network.

2) actions directed at electronic data processing - influencing (by doing or not doing), to a greater or lesser extent, the outcome (result) of electronic data processing in any other way[29].

For the existence of this criminal offense, it is necessary that the action of execution in any form of manifestation is undertaken:

a) with a specific aim[30] - to obtain an unlawful property gain for the perpetrator or another natural or legal person. This aim should motivate, activate the perpetrator to undertake the execution action, regardless of whether this aim was achieved in the specific case. The existence of this aim qualifies the perpetrator's form of guilt as direct intent,

b) with a caused consequence in the form of property (economic, material) damage that occurs for any other natural or legal person[31]. It can be damage in any amount or scope,

osne studije, 91-114.

[24] Đorđević, M., Đorđević, Đ. (2010). *Krivično pravo*, Beograd: Gasmi, 193.

[25] See Tanović, R. (2002). Kaznenopravna zaštita informacijskih sustava, *Kriminalističke teme*, Sarajevo, *3-4*, 271-294.

[26] See Protrka, N. (2011). Računalni podaci kao elektronički (digitalni) dokazi, *Policija i sigurnost*, Zagreb, *1*, 1-13.

[27] See Petrović, B., Jovašević, D., Ferhatović, A. (2016). *Krivično pravo 2*, Sarajevo: Pravni fakultet, 434.

[28] Đorđević, Đ., Kolarić, D. (2020). *Krivično pravo, Posebni deo*, Beograd: Beograd: Kriminalističko-policijski univerzitet, 196-197.

[29] See Milošević, M., Putnik, N. (2019). Specifičnosti izvršenja krivičnog djela prevare uz korišćenje informaciono-komunikacionih tehnologija, *Bezbednost*, Beograd, *2*, 68-88.

[30] See Franjić, S. (2017). Kaznena djela računarskog kriminaliteta u Republici Hrvatskoj, *Pravne teme*, Novi Pazar, *10*, 105-114.

[31] See Milošević, M. (2021). Internet prevare – savremeni način izvršenja i mere samozaštite, *Izbor sudske prakse*, Beograd, *2*, str. 5-7.

which is reflected or manifested on someone's property in the sense of its decrease or prevention of its increase. The damage that occurred in this way should be in a cause-and-effect relationship with undertaken action of execution, regardless of whether the injured party (victim) is the owner or just a user of computer network[32], and

c) in a certain way[33] - without authorization, therefore, contrary to existing regulations, unlawfully. The perpetrator's awareness of the illegality of his actions is an element of his intent.

The perpetrator of the offense can be any person, and in terms of guilt, direct intent is required, thanks to the existence of a legally prescribed aim (intention) on the part of the perpetrator at the time of the committing the offense. Namely, specific category of persons can appear as perpetrators[34]. These are mostly non-delinquent and socially adaptable, non-violent personalities. In order to commit the offense via computer, they must possess certain special, specific, professional and practical knowledge and skills in the field of information and computer techniques and technologies. In addition, these are the persons to whom such technical means (computers) are available in a physical sense[35].

These criminal offenses are committed covertly, often without a visible spatial and temporal close connection between the perpetrator and the victim (passive subject). In practice, there is a greater or lesser time difference between the action of committing a criminal offense and the moment of occurrence of its consequences. These offenses are difficult to detect, and even more difficult to prove. They remain practically undetected for a long time, until the injured party suffers damage in the domain of information and computer data or systems[36].

For the basic for of the offense, a sentence of imprisonment for a term of six months to five years is prescribed. Although it is a "classic" criminal offense, whose perpetrator is justified to be imposed a security measure of confiscation of the object - the means of its execution (such as computer data or a program, that is, an electronic computer data processing system), the legislator in Bosnia and Herzegovina does not know such a solution. On the other hand, some criminal legislations of the countries in the region provide for the mandatory imposition of a security measure of confiscation of objects (Article 251b of the Criminal Code of North Macedonia[37] or Article 271 of the Criminal Code of Croatia[38]).

The criminal offense of computer fraud (Article 395 of the CCFBiH) has two serious, qualified forms of manifestation (an offense qualified by a more serious consequence) [39].

---

[32] Pavišić, B., Grozdanić, V., Veić, P. (2007). Komentar Kaznenog zakona, Zagreb: Narodne novine, 562.

[33] See Babić, V. (2009). *Kompjuterski kriminal,* Sarajevo: Rabic, 91-94.

[34] See Kevrić, D. (2017). Visokotehnološki (kompjuterski) kriminalitet – primjena materijalnog prava iz te oblasti, *Pravo i pravda*, Sarajevo, 1, 295-309.

[35] See Franjić, S. (2012). Inkriminisanje nekih kaznenih djela iz područja računalnog kriminaliteta u Republici Hrvatskoj, *Kriminalističke teme*, Sarajevo, *3-4*, 243-254.

[36] Pavišić, Grozdanić, Veić, 559-560.

[37] *Official Gazette of the Republic of Macedonia*, nos. 37/1996, 80/1999, 4/2002, 43/2003, 19/2004, 81/2005, 60/2006, 73/2006, 7/2008, 139/2008, 114/2009, 51/2011, 135/2011, 185/2011, 142/2012, 166/2012, 55/2013, 8272013, 14/2014, 27/2014, 28/2014, 28/2014, 41/2014, 115/2014, 132/2014, 160/2014, 199/2014, 196/2015, 226/2015, 169/2016, 97/2017, 170/2017, 248/2018, 36/2023 and 188/2023.

[38] *Official Newspapers of the Republic of Croatia,* nos. 125/2011, 144/2012, 56/2015, 61/2015, 101/2017, 118/2018, 126/2019, 84/2021, 114/2022 and 114/2023.

[39] See Stanić, S. (2012). Savremeni oblici kompjuterskog kriminaliteta, Zbornik radova *Društvena*

The first serious form of the offense (paragraph 2.) exists if, by committing the basic offense, the perpetrator acquired for himself or for another natural or legal person a material gain exceeding the amount of 10,000 KM. The amount of acquired gain, in fact, reflects the scope and intensity of the caused consequences by the offense, so it is determined as a factual issue in each specific case. It is determined according to the market conditions that existed at the time of undertaking the action of execution of the offense. This more serious consequence must be in a cause-and-effect relationship with the action taken to commit the basic offense[40]. A sentence of imprisonment for a term of two to ten years is prescribed for this offense.

The most serious form of the offense (paragraph 3), for which a sentence of imprisonment for a term of two to twelve years is prescribed, exists if, by the criminal offence a material gain exceeding 50,000 KM is acquired. Therefore, the offense is qualified (the qualifying circumstance is) the level (amount, scope, intensity) of property damage caused to another natural or legal person[41].

An interesting legal solution is that it provides for a less serious, privileged form of criminal offense of computer fraud (paragraph 4). This offense exists the criminal offence was perpetrated only with an aim of causing damage to another person, regardless of whether such damage occurred at all. Alternatively, a fine or imprisonment for a term not exceeding three years is prescribed for this offense.

In an identical manner, the CCBDBiH in Chapter XXXII: "Criminal offenses against systems of electronic data processing " (Article 389) provides for the criminal offense: "Computer fraud" in the basic, two more serious and one less severe form of manifestation in an identical legal description and content, i.e. with the same prescribed penalties as in the CCFBiH.

3.2. Characteristics of the offense of computer fraud in the legislation of the Republika Srpska

In a different way, CCRS in Chapter XXXII under title: "Criminal offenses against the safety of computer data" (Article 410) provides for the criminal offense: "Computer fraud". This offense consists of entering incorrect data, failing to enter correct data, or concealing or falsely presenting data in another way, thus affecting the result of electronic processing and data transmission with the intention of acquiring unlawful material gain for himself or for another, and thus causes material damage to somebody else[42].

In this case, the object of protection is a system of electronic processing and transmission of computer data. On the other hand, the object of the attack is computer data, which can be true (correct) or false (incorrect).

The act of committing this criminal offense consists of the following alternatively prescribed activities[43]: a) entry – writing of incorrect (completely or partially false) data, b) fail-

*reakcija na savremene oblike ugrožavanja bezbjednost*i, Banja Luka, 125-134.

40 Petrović, Jovašević, Ferhatović, 434-435.

41 Simović, M., Simović, V. (2021). *Krivično pravo Brčko distrikta BiH*, *Posebni dio*, Laktaši: Grafomark, 169-170.

42 See Jovašević, D., Ikanović, V. (2012). *Krivično pravo Republike Srpske, Posebni dio*, Banja Luka: Fakultet pravnih nauka, 178-187.

43 See Lazarević, Lj., Vučković, B., Vučković, V. (2010). *Komentar Krivičnog zakonika*, Tivat: Fakultet za mediteranske poslovne studije Tivat, 820-821.

ure to enter - inaction (negative, passive activity), failure to write, failure to enter correct (true) data, c) concealment - hiding, making data inaccessible to other persons, and d) false (untrue) presentation – false communication or presentation of data in any other way.

For this criminal offense, it is necessary to undertake the action of execution prescribed by the law[44]:

a) in relation to data that is suitable (by nature, content, significance, time or value) to influence the result of electronic data processing and data transmission. When such computer data is in question, it represents a factual issue that the court, in each specific case, considers its legal qualifications, and

b) with a certain intention - with the intention of the perpetrator to acquire unlawful material gain for himself or for another (natural or legal) person, regardless of whether this intention was realized in the specific case. Nevertheless, the existence of this intention on the part of the perpetrator, at the time the offense was committed, qualifies direct intent as a form of his guilt[45].

The consequence of this offense, which occurs as a result of undertaken action of execution, appears as a violation of protected good - in the form of causing material damage to another (natural or legal) person in any amount, scope or value.

For the basic form of this offense the Republika Srpska prescribes a milder punishment (than CCFBiH or CCBDBiH), with an alternative - a fine or imprisonment for a term not exceeding three years.

CCRS also recognizes two more serious, qualified forms of manifestation of the criminal offense of computer fraud[46]. However, in this case, qualifying circumstances, in relation to the scope of caused material damage, appear in a slightly different way than it is the case in CCFBiH and CCBDBiH.

The first serious form of the offense[47] is characterized by acquired property gain as a result of undertaken action of execution, which exceeds the amount of 10,000 KM. Property (economic, material) damage caused in this way must be in a cause-and-effect relationship with undertaken action of execution, which is determined as a factual issue in each specific case. Prescribed sentence for this offense is imprisonment for a term of one to eight years.

Another serious form of the offense[48], for which a sentence of imprisonment for a term of two to ten years is prescribed, exists if the commission of the crime resulted in the acquisition of material gain exceeding the amount of 30,000 KM. Here, too, the amount of material gain is determined according to market conditions at the time the action of execution was undertaken.

Finally, a milder, privileged form of the offense (paragraph 4) exists if any of legally prescribed actions for the execution of the basic offense was undertaken only (solely, exclusively) with the intention of causing damage to another person[49]. The perpetrator's malicious intent to cause property damage to another person in any amount or scope (regardless of

---

[44] Đorđević, Đ. (2011). *Krivično pravo, Posebni deo*, Beograd: Kriminalističko-policijska akademija, 181-182.

[45] Jovašević, D., Miladinović Stefanović, D. (2023). *Krivično pravo, Posebni deo*, Niš: Pravni fakultet, 364-365.

[46] Jovašević, D. (2017). *Krivično pravo, Posebni deo*, Beograd: Dosije, 239-240.

[47] Turković, K. *et al.* (2013). *Komentar Kaznenog zakona*, Zagreb: Narodne novine, 345.

[48] Stojanović, Z., Delić, N. (2013). *Krivično pravo, Posebni deo*, Beograd: Pravna knjiga, 257-258.

[49] Delić, N. (2021). *Krivično pravo, Posebni deo*, Beograd: Pravni fakultet, 331-332.

whether a person acquires material gain in this way) is a privileged circumstance for which the law alternatively prescribes a fine or imprisonment for a term not exceeding six months.

4. CONCLUSION

Computer crime appears in various forms or types of manifestation as a basic factor in either modern crime, classic (general, conventional) or organized, transnational crime. In the efforts of the international community to combat this crime with effective measures, means or procedures, a system of international standards is established within the Council of Europe based on numerous recommendations, which was primarily established in the Convention on Cybercrime (2001). Among the numerous incriminations of computer crimes, this Convention determines the content and characteristics of the criminal offense of computer-related fraud.

On the basis of this Convention, the European criminal legislations, thus the legislation of Bosnia and Herzegovina, established a system of criminal liability and punishment for computer crimes, including the specific criminal offense called "computer fraud" which occurs in the basic, two qualified, and a milder (privileged) form.

Among computer crimes, computer fraud stands out as a special, specific form of the criminal offense of fraud (basic property crime), which is committed in a specific way in this case - with the help, mediation or use of computer programs or data. This criminal offense consists in the unauthorized entry, damage, alteration or concealment of computer data or programs, or in influencing the outcome of electronic data processing in another way with the aim of acquiring unlawful material gain for oneself or for another, thereby causing (inflicting) material damage to another person.

In addition, the criminal offense of fraud is undertaken with direct intention of the perpetrator, which is based on the aim, or the intention of the perpetrator to acquire property (material, economic) gain for himself or for another. At the same time, the consequence of this offense appears in the form of violation - causing material damage to another natural or legal person.

Depending on the amount of acquired gain, that is, the property damage caused to another natural or legal person, there are two serious, qualified forms of manifestation of criminal offenses for which a stricter punishment is prescribed. In addition to sentences of imprisonment of varying durations, only fines are explicitly prescribed (CCRS). Unlike some foreign comparative criminal law systems, the law of Bosnia and Herzegovina does not prescribe mandatory imposition of a security measure of confiscation of an object - computer data or program (in the sense of the object of the attack).

The milder, privileged form of manifestation of the criminal offense of computer fraud is determined by the intention of the perpetrator that motivates him to undertake the action of execution. It is the malicious intent of the perpetrator to cause material damage to another person in any amount, scope or level.

5. LITERATURE

Monographs, articles

Anderson, R., Barton, C., Bohme, R. *et al.* (2012). *Measuring the cost of cybercrime*. Workshop on the Economics of Information Security, Berlin, June 2012. *http://weis2012.econinfosec.org/ papers/ Anderson_WEIS2012.pdf, accessed January 22, 2024.*

Atanasov, R. (2021). *Priračnik za zaštitata od izmami i kompjuterski kriminal.* Skopje: Akademik, 114-127.

Babić, V. (2009). *Kompjuterski kriminal*. Sarajevo: Rabic, 91-94.

Bregant, J., Bregant, R. (2014). Cybercrime and Computer Crime, *The Encyclopedia of Criminology and Criminal Justice,* First Edition, Edited by Jay S. Albanese, *https://doi.org/10.1002/9781118517383.Wb eccj244*.

Brenner, S. (2007). At light speed: Attribution andresponse to cybercrime/terrorism/warfare, *The Journal of Criminal Law & Criminology,* 97(2), 379–475.

Budimlić, M., Puharić, P. (2009). *Kompjuterski kriminalitet – kriminološki, krivičnopravni, kriminalistički i sigurnosni aspekt*, Sarajevo: Fakultet za kriminalistiku, kriminologiju i sigurnosne studije.

Congressional Research Service (2012). *Cybercrime: Conceptual Issues for Congress and U.S. Law Enforce-ment. http://www.fas.org/sgp/crs/misc/R42547.pdf,accessed January 29, 2023.*

Dedović, A., Stanojković, D. (2021). Kompjuterski kriminalitet – opća razmatranja, Zbornik radova *Sigurnost i društvo*, Mostar, 485-496.

Delić, N. (2021). *Krivično pravo, Posebni deo*. Beograd: Pravni fakultet.

Dragićević, D. (1999). *Kompjutorski kriminalitet i informacijski sustavi*. Zagreb: Informator.

Đorđević, Đ. (2011). *Krivično pravo, Posebni deo*. Beograd: Kriminalističko-policijska akademija.

Đorđević, Đ., Kolarić, D. (2020). *Krivično pravo, Posebni deo*. Beograd: Beograd: Kriminalističko-policijski univerzitet..

Đorđević, M., Đorđević, Đ. (2010). *Krivično pravo*, Beograd: Gasmi.

Franjić, S. (2012). Inkriminisanje nekih kaznenih djela iz područja računalnog kriminaliteta u Republici Hrvatskoj, *Kriminalističke teme*, Sarajevo, *3-4*, 243-254.

Franjić, S. (2017). Kaznena djela računarskog kriminaliteta u Republici Hrvatskoj, *Pravne teme*, Novi Pazar, *10*, 105-114.

Hilgedorf, E., Valerius, B. (2012). *Computer und Internet Strafrecht*. Heidelberg: Springer.

Hinnen, T. (2004). The cyber-front in the war on terrorism: Curbing terrorist use of the Internet, *TheColumbia Science and Technology Law Review*, *5(5),* 1–42.

Jovašević, D., Ikanović, V. (2012). *Krivično pravo Republike Srpske, Posebni dio*, Banja Luka: Fakultet pravnih nauka.

Jovašević, D. (2014). Računarski kriminalitet u Srbiji i evropski standardi. Beograd: *Evropsko zakonodavstvo*, Beograd, *47-48*, 40-56.

Jovašević, D. (2017). *Krivično pravo, Posebni deo*. Beograd: Dosije.

Jovašević, D. (2021). Računarska prevara - krivična odgovornost i kažnjivost u međunarodnom i nacionalnom pravu, Zbornik radova *Pravo i digitalizacija*, Niš, 51-73.

Jovašević, D., Miladinović Stefanović, D. (2023). *Krivično pravo, Posebni deo*. Niš: Pravni fakultet.

Kellermann, T. (2010). Building a foundation for globalcybercrime law enforcement, *Computer Fraud &Security*, *(5)*, 5–8.

Kareklas, S. (2009). *Priručnik za krivično pravo Evropske unije*, Beograd: Institut za uporedno pravo, Mladi pravnici Srbije.

Kevrić, D. (2017). Visokotehnološki (kompjuterski) kriminalitet – primjena materijalnog prava iz te oblasti, *Pravo i pravda*, Sarajevo, 1, 295-309.

Lazarević, Lj., Vučković, B., Vučković, V. (2010). *Komentar Krivičnog zakonika*, Tivat: Fakultet za mediteranske poslovne studije.

Miladinović Bogavac, Ž. (2021). *Sajber prevare*, Beograd: Zadužbina Andrejević.

Milošević, M., Putnik, N. (2019). Specifičnosti izvršenja krivičnog djela prevare uz korišćenje informaciono-komunikacionih tehnologija, *Bezbednost*, Beograd, *2*, 68-88.

Milošević, M. (2021). Internet prevare – savremeni način izvršenja i mere samozaštite, *Izbor sudske prakse*, Beograd, *2*, 5-7.

Mrvić Petrović, N. (2005). *Krivično pravo*. Beograd: Fakultet za poslovn**o pravo.**

Paunović, N. (2018). Krivično djelo računarske prevare kao oblik finansijskog kriminaliteta – kriminalistički aspekt, Zbornik radova *Finansijski kriminalitet*, Beograd, 265-276.

Pavišić, B., Grozdanić, V., Veić, P. (2007). Komentar Kaznenog zakona. Zagreb: Narodne novine.

Pavišić, B. (2016). *Kazneno pravo Vijeća Evrope*. Zagreb: Golden marketing -Tehnička knjiga.

Pavišić, B., Kamber, K., Parenta, I. (2016). *Kazneno pravo Vijeća Europe*. Rijeka: Ugent.

Peršak N. *et al*. (2006). *Računalniška/kibernetička kriminaliteta v Sloveniji*. Ljubljana: Inštitut za kriminologijo pri Pravni fakulteti.

Petrović, B., Jovašević, D., Ferhatović, A. (2016). *Krivično pravo 2*. Sarajevo: Pravni fakultet.

Protrka, N. (2011). Računalni podaci kao elektronički (digitalni) dokazi, *Policija i sigurnost*, Zagreb, *1*, 1-13.

Simović, M. (1994). *Krivični zakon Republike Srpske – posebni dio, sa objašnjenjima*. Pale: NIO Službeni glasnik Republike Srpske.

Simović, M., Simović, V. (2021). *Krivično pravo Brčko distrikta BiH*, *Posebni dio*. Laktaši: Grafomark.

Simović, M., Babić, M., Simović, V. (2019). *Zbirka sudskih odluka iz krivičnopravne materije (knjiga treća)*. Sarajevo: Privredna štampa.

Simović, M., Todorović, Lj. (2016). *Krivični zakon Federacije Bosne i Hercegovine, uvodna objašnjenja za posljednju novelu Krivičnog zakona Federacije Bosne i Hercegovine, te redakcijski prečišćeni tekst ovog zakona, registar pojmova i sudska praksa*, Sarajevo: Fineks.

Simović, M., Simović, M., Todorović, Lj. (2015). *Krivični zakon Bosne i Hercegovine. Prečišćeni tekst sa uvodnim napomenama, registar pojmova*. Sarajevo: Fineks.

Skibell, R. (2003). Cybercrimes & misdemeanors: Areevaluation of the Computer Fraud and Abuse Act, Berkeley Technology Law Journal, *18(3),* 909–944.

Stanić, S. (2012). Savremeni oblici kompjuterskog kriminaliteta, Zbornik radova *Društvena reakcija na savremene oblike ugrožavanja bezbjednosti*, Banja Luka, 125-134.

Stojanović, Z., Delić, N. (2013). *Krivično pravo, Posebni deo*. Beograd: Pravna knjiga.

Tanović, R. (2002). Kaznenopravna zaštita informacijskih sustava, *Kriminalističke teme*, Sarajevo, *3-4*, 271-294.

Turković, K. *et al*. (2013). *Komentar Kaznenog zakona*. Zagreb: Narodne novine.

Vestbi, Dz. *et al*. (2004). *Međunarodni vodič za borbu protiv kompjuterskog kriminala*. Beograd: Produktivnost AD.

Vojković, G., Štambuk Šunjić, M. (2006). Konvencija o kibernetičkom kriminalu i Kazneni zakon Republike Hrvatske, *Zbornik Pravnog fakulteta u Splitu*, Split, *1*, 123-136.

Završnik, A. (2009). *Homo Criminalis: Depicting a Criminal in the High-tech Risk Society*. Ljubljana: Institute of Criminology at the Faculty of Law (in Slovenian).

Završnik, A. (2010). *Crime and Technology: How Computers Transform Surveillance and Privacy, Crime and Crime Control?* Ljubljana: Institute of Criminology at the Faculty of Law (in Slovenian).

Završnik, A. (2015). *Kibernetska kriminaliteta*, Ljubljana: IUS Software, GV založba, Institute of Criminology at the Faculty of Law.

Završnik, A. (2017). *Kyberkriminalita*. Praha: Wolters Kluwer.

Završnik, A. (2018). *Big Data, Crime and Social Control*. London: Routledge.

Završnik, A., Selinšek, L. (2018). *Law in the Age of Big Data*. University of Ljubljana: Faculty of Law; and Institute of Crimininology at the Faculty of Law, Ljubljana (in Slovenian).

Zvrlevski, M., Andononova, S., Miloševski, V. (2014). *Priračnik za kompjuterski kriminal*, Skopje: OSCE.

Šelih, A., Završnik, Aleš (eds.) *(2012). Crime and transition in Central and Eastern Europe*. New York [etc.]: Springer.

Legal sources

Additional Protocol on the Convention on Cybercrime, Concerning the Criminalisation of Acts a Racist and Xenofobic Nature Commited through Computers Systems, Strazbourg,

January 28, 2003.

Commission of the European Communities (2007). *Towards a General Policy on the Fight Against CyberCrime*. COM (2007) 267 final.

Council of Europe Treaty Series – No. 224. Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence.

Convention on Cybercrime, Budapest, November 23, 2001.

Criminal Code of the RC, *Official Gazette of the Republic of Croatia*, nos. 125/2011, 144/2012, 56/2015, 61/2015, 101/2017, 118/2018, 126/2019, 84/2021, 114/2022 and 114/2023.

Criminal Code of BiH, *Official Gazette of Bosnia and Herzegovina*, nos. 3/2003, 32/2003, 37/2003, 54/2004, 61/2004, 30/2005, 53/2006, 55/2006, 32/2007, 8/2010, 47/2014, 22/2015, 40/ 2015, 35/2018, 46/2021, 31/2023 and 47/2023.

Criminal Code of BDBiH, *Official Gazette of the Brčko District of Bosnia and Herzegovina*, number 19/2020.

Criminal Code of FBiH, *Official Gazette of the Federation of Bosnia and Herzegovina*, nos. 36/2003, 37/2003, 21/2004, 69/2004, 18/2005, 42/2010, 42/2011, 59/2014, 76/2014, 75/2017 and 31/2023.

Criminal Code of RM, *Official Gazette of the Republic of Macedonia*, nos. 37/1996, 80/1999, 4/2002, 43/2003, 19/2004, 81/2005, 60/2006, 73/2006, 7/2008, 139/2008, 114/2009, 51/2011, 135/ 2011, 185/2011, 142/2012, 166/2012, 55/2013, 8272013, 14/2014, 27/2014, 28/2014, 28/2014, 41/2014, 115/2014 and 132/2014, 160/ 2014, 199/2014, 196/2015, 226/2015, 169/2016, 97/2017, 170/2017, 248/2018, 36/2023 and 188/2023.

Criminal Code of the RS, *Official Gazette of the Republika Srpska*, nos. 64/2017, 104/2018, 15/2021, 89/2021 and 73/2023.

United States Government Accountability Office (2007). *Cybercrime: Public and private entities face challengesin addressing cyber threats*. Washington, DC: Government Accountability Office.

Kompjuterska (računarska) prevara u pravu Bosne i Hercegovine i međunarodni standardi

Sažetak: U savremenom krivičnom zakonodavstvu uopšte, pa tako i u pozitivnom pravu Bosne i Hercegovine, propisano je više različitih krivičnih djela prevare koja su sistematizovana u različitim grupama djela prema različitim zaštitnim objektima, ali sa više-manje identičnim radnjama izvršenja sa namjerom/ciljem pribavljanja koristi za sebe ili za drugo lice, odnosno sa namjerom/ciljem nanošenja štete drugom licu. To su: a) prevara pri glasanju (ili izborna prevara), b) prevara u privrednom poslovanju (ili prevara u osiguranju), c) prevara, d) prevara u službi i e) kompjuterska prevara. U sistemu, skupu više različitih oblika ispoljavanja krivičnih djela prevare specifičan karakter, prirodu i sadržinu ima upravo krivično djelo računalna/kompjuterska prevara koju propisuju tri krivična zakona (osim Krivičnog zakona Bosne i Hercegovine). U osnovi ove inkriminacije se nalaze relevantni međunarodni standardi sadržani u Konvenciji Saveta Evrope o kibernetičkom (računarskom, sajber) kriminalu (Budimpešta, 2001.). U ovom radu se izlažu pojam, karakteristike, elementi bića i sadržina krivičnog djela kompjuterske prevare shodno zakonskim rješenjima sa primjenom u Bosni i Hercegovini.

Ključne riječi: računarska prevara, zakon, krivično djelo, odgovornost, međunarodni standardi.