XXII International Scientific Conference „Legal days – Prof. Slavko Carić"
"LAW AND JUSTICE"

The University of Business Academy in Novi Sad
The Faculty of Law for Commerce and Judiciary in Novi Sad
October 10th and 11th 2025 in Novi Sad

Proceedings of XXII International Scientific Conference
"Legal days – Prof. Slavko Carić"
"LAW AND JUSTICE"
October 10th and 11th 2025 in Novi Sad
Organized by the University of Business Academy in Novi Sad
The Faculty of Law for Commerce and Judiciary in Novi Sad

The Publisher:
The University of Business Academy in Novi Sad
The Faculty of Law for Commerce and Judiciary in Novi Sad
Geri Karolja Street no.1, telephone: 021/ 400 - 499
Web: www.pravni-fakultet.info

For the Publisher:
Milan Počuča, PhD, Full Professor

The Editor-in-Chief:
Milan Počuča, PhD, Full Professor

Printed by:
Štamparija FELJTON

Circulation:
100

ISBN 978-86-86121-84-4

Scientific Committee:

PROF. MILAN POČUČA, PhD – President of the Scientific Committee
Dean of the Faculty of Law for Commerce and Judiciary in Novi Sad,
University Business Academy in Novi Sad | Republic of Serbia

PROF. MARKO CARIĆ, PhD
Dean of the Faculty of Economics and Engineering Management in Novi Sad,
University Business Academy in Novi Sad | Republic of Serbia

PROF. MARIJANA CARIĆ, PhD
President of the Council of the University Business
Academy in Novi Sad | Republic of Serbia

PROF. MIRKO KULIĆ, PhD
Professor Emeritus at the Faculty of Law for Commerce and Judiciary in
Novi Sad, University Business Academy in Novi Sad | Republic of Serbia

PROF. MARIJANA DUKIĆ MIJATOVIĆ, PhD
Full Professor at the Faculty of Law for Commerce and Judiciary in Novi Sad,
University Business Academy in Novi Sad | Republic of Serbia

PROF. PREDRAG MIRKOVIĆ, PhD
President of the Council of the Faculty of Law for Commerce and Judiciary in Novi
Sad, University Business Academy in Novi Sad | Republic of Serbia

PROF. MARIJANA MLADENOV, PhD
Vice-Dean for International Cooperation at the
Faculty of Law for Commerce and Judiciary in Novi Sad,
University Business Academy in Novi Sad | Republic of Serbia

PROF. ZORAN PAVLOVIĆ, PhD
Head of the Department of Criminal Law at the
Faculty of Law for Commerce and Judiciary in Novi Sad,
University Business Academy in Novi Sad | Republic of Serbia

PROF. DARKO GOLIĆ, PhD
Head of the Department for Public Law and Legal Theory at
the Faculty of Law for Commerce and Judiciary in Novi Sad,
University Business Academy in Novi Sad | Republic of Serbia

PROF. ŽELJKO BJELAJAC, PhD
Full professor at the Faculty of Law for Commerce and Judiciary in Novi Sad,
University Business Academy in Novi Sad | Republic of Serbia

PROF. JELENA MATIJAŠEVIĆ, PhD
Vice-Dean for Science at the Faculty of Law for Commerce and Judiciary in Novi
Sad, University Business Academy in Novi Sad | Republic of Serbia

Organizing Committee:
PROF. JOKO DRAGOJLOVIĆ,
PhD - PRESIDENT OF THE ORGANIZING COMMITTEE
PROF. IVAN JOKSIĆ, PhD
PROF. JELENA STOJŠIĆ DABETIĆ, PhD
PROF. NENAD BINGULAC, PhD
PROF. NENAD STEFANOVIĆ, PhD
PROF. MARKO STANKOVIĆ, PhD
GORAN MILOJEVIĆ, PhD
ANJA KOPRIVICA, LLM
MARA DESPOTOV, LLM
TAMARA KRSTIĆ, LLM
ANAMARIJA POPOVIĆ, LLM

Conference Secretary:
ANJA KOPRIVICA, LLM, Teaching Assistant

UDC:343.377:004.056.5
DOI: 10.5937/PDSC25424D

Joko Dragojlović, PhD Associate Professor
Faculty of Law for Commerce and Judiciary in Novi Sad.
University Business Academy in Novi Sad
email: jdragojlovic@pravni-fakultet.info

CRIMINAL LIABILITY FOR THE ABUSE OF COMPUTER VIRUSES – STATUS AND PROSPECTS[1]

Abstract:

Given the increasing prevalence of the almost daily use of computer programs, data, or systems in various spheres of human, social, and economic life, it is necessary to ensure, and subsequently improve, their effective, lawful, and high-quality protection—both technical and legal. In this way, overall computer security is raised to a qualitatively higher level. It is particularly endangered by various unlawful activities involving the misuse of computer programs, data, or systems.

A particularly dangerous form of such computer misuse appears in the creation, insertion, distribution, or dissemination of different types of computer viruses. These are malicious computer programs designed to cause damage to a computer, network, or data, and are introduced into a system with the intention of compromising the confidentiality, integrity, or availability of computer data, or with the aim of disrupting the functioning of a computer or computer network in other ways. The criminal legislation of Serbia, as well as several comparative legal systems, prescribes specific incriminations for the creation or dissemination of computer viruses. This paper addresses their elements, characteristics, forms of manifestation, and substantive content.

Keywords: *computer program, computer virus, misuse, criminal offense, liability*

INTRODUCTION

In the modern world, increasing attention is devoted to the establishment, strengthening, and improvement of systems of computer (information, cyber) security. This is particularly due to their growing vulnerability to numerous unlawful activities carried out by individuals or groups. The entirety of such diverse activities, which violate or endanger computer systems, programs, or data - thereby undermining computer security to a greater or lesser extent-constitutes cybercrime.[2]

1 The paper is the result of a long-term scientific research project "Progressive development of law in modern digital society",which is financed by the Provincial Secretariat for Higher Education andScientific Research activity (decision number 003069523 2024 09418 003 000 000 001-01003069523 2024 09418 003 000 000 001-01, 21.11.2024).

2 Dragojlović, J., Koprivica A., (2023). Osvrt na računarski kriminalitet u zakonodavstvu Republike

Namely, cybercrime refers to various activities that compromise the security of computer data, whereby the criminal offenses it encompasses are committed by means of, or through, the use of computers, with the computer serving as the instrument of their commission. However, this concept also includes criminal offenses consisting of the disabling of computers or computer networks, in which the computer itself becomes the object of attack.[3] Within the framework of cybercrime, two categories of criminal offenses can be distinguished:

a) offenses that directly target computer technology systems by disabling, damaging, or destroying computer data or programs, interfering with their use, or engaging in unauthorized access to a computer network or electronic data processing itself and

b) offenses in which computer technology is used as a means for committing other types of criminal offenses.[4]

In practical terms, cybercrime, in the broadest sense of the term - or crime related to the use of computers - is defined in legal theory as the commission of criminal offenses through the misuse of computers or computer systems. This means that the very act of committing such offenses necessarily involves the use of computers or computer systems either as the means or as the target of the offense. A specific manifestation of cybercrime, which in recent times has been gaining increasing significance, scope, and prevalence-while also producing pronounced negative and harmful consequences - is the misuse of computer viruses in various forms.

ON COMPUTER VIRUSES

A computer virus is a malicious computer program (or "code") characterized by a broad capacity for self-replication (copying, reproducing) within other files with which it comes into contact. It may reside in and infect any computer program, boot sector, or macro-enabled document, thereby altering the content of such a file or inserting (copying) its own code into it. A computer virus typically consists of two parts: a) self-replicating code that enables the multiplication of the virus and b) a payload, which may be "harmless" or harmful. In some cases, the virus may consist solely of self-replicating code.

Computer science today represents a highly dynamic field undergoing rapid development and continuous advancement.[5] Consequently, it is not surprising that the number and types of computer viruses are multiplying on an almost daily basis. Nevertheless, certain categories of computer viruses can be distinguished, such as: a) **Boot sector viruses** – targeting the Master Boot Record (MBR) or the boot sector of a computer, b) **Parasitic viruses** – infecting executable files by inserting their code into the structure of the program, c) **Multipartite viruses** – simultaneously attacking both boot sectors and executable programs, d) **Companion viruses** – creating a ".com" file using the name of an existing ".exe" program into which they implant their code, e) **Link viruses** – rapidly infecting computer systems or programs, f) **Macro viruses** – exhibiting extensive

Srbije, U: Počuča, M., (urednik), Zbornik radova, Dve decenije razvoja pravne misli, Pravni fakultet za privredu i pravosuđe, Novi Sad, str. 410-420.

3 Mrvić Petrović, N. (2005). *Krivično pravo*, Beograd: Službeni glasnik, str. 322.

4 Đorđević, Đ. (2011). *Krivično pravo. Posebni deo*. Beograd: Kriminalističko-policijska akademija, str. 177.

5 Zirojević, M., Ivanović, Z. (2022). *Cyber law*. Beograd: Institut za uporedno pravo, str. 98-112.

self-replication capabilities, thereby deleting or altering existing computer data, g) **Power viruses** – designed to maximize CPU energy consumption.[6]

Computer viruses spread in numerous ways, including through local networks, Bluetooth connections, e-mail, downloads from various Internet sources, portable media (USB drives, memory cards, CD/DVD discs), and other types of "peripherals" that connect two or more software-controlled computer devices or systems. The stages of viral infection caused by computer viruses are generally described as follows:

a) **Dormant phase** (optional) – during which the virus program remains inactive even though it has gained access to a computer and is present in the system, it does not yet take any action;

b) **Propagation phase** – when the virus begins to spread by replicating itself, placing copies into other programs or certain system areas. Such copies ("clones") need not always be identical to the original version;

c) **Triggering phase** – when the previously inactive virus is activated, initiating the computer operations for which it was primarily designed;

d) **Execution phase** – when the full activity of the virus manifests, resulting in various harmful consequences such as file deletion, data theft, system crashes, file corruption, and similar effects.

In order to combat or prevent such unlawful activities - namely the creation, insertion, dissemination, or distribution of computer viruses - modern criminal legislation establishes, within the system of computer-related criminal offenses, criminal liability, i.e., the punishability of their perpetrators. This specific incrimination, titled **"creation and insertion of computer viruses,"** is prescribed not only by the criminal legislation of Serbia but also by the legal systems of several countries in the region (Montenegro, Republika Srpska – BiH, and North Macedonia). In this way, the computer virus itself becomes the object of attack in computer-related criminal offenses.

INTERNATIONAL STANDARDS FOR COMBATING THE MISUSE OF COMPUTER VIRUSES

The foundation for a unified approach to combating the misuse (creation, insertion, dissemination) of computer viruses at the national legislative level is provided by relevant international standards established through regional (European) instruments, such as:

a) The Council of Europe Convention on Cybercrime (Budapest, 2001); and

b) Directive 40/2013/EU of the European Parliament and of the Council (2013).

The Convention on Cybercrime serves as the primary source of international standards for the prevention and suppression of cybercrime in European countries.[7] This

6 Dulčić, K. (2007). Oblici štete od računalnih virusa i odgovornost za štetu, *Zbornik Pravnog fakulteta Sveučilišta u Rijeci,* 28(1), str. 189-228.

7 Dragojlović J., Krstinić D., (2015). Evropski standardi u borbi protiv visokotehnološkog kriminaliteta i njihova implementacija u zakonodavstvu Republike Srbije, Evropsko zakonodavstvo, 14(51), str. 92-103.

Convention (Article 1), in its first chapter entitled "Use of Terms," defines the basic concepts related to cybercrime, such as: a) computer system – any device or group of interconnected or interdependent devices, of which one or more, based on a program, automatically processes data, b) computer data – any representation of facts, information, or concepts in a form suitable for processing by a computer system, including the relevant program that enables the computer system to perform its functions, c) traffic data – any computer data relating to communication via a computer system, generated by a computer system forming part of the communication chain, and containing information on the origin, destination, route, time, date, size, duration, or type of the service involved.

In Chapter Two, entitled "Measures to be Adopted at the National Level," Part One: "Substantive Criminal Law" provides for several computer-related criminal offenses. In this section, "Offenses against the Confidentiality, Integrity, and Availability of Computer Data and Systems" are prescribed, including an offense relevant to the subject of this paper, entitled "Misuse of Devices" (Article 6).[8] Based on this international standard, all European countries are obliged to incorporate this incrimination into their domestic criminal law/code.

According to these provisions, this criminal offense occurs if any of the following activities are intentionally (with intent) and unlawfully carried out:[9]

1. The production, sale, procurement for use, import, distribution, and other forms of making available of: a) devices, including computer programs, that are primarily designed or adapted for the purpose of committing one of the computer-related criminal offenses, or b) computer passwords, access codes, or similar data enabling access to a computer system as a whole or to any part of it (including computer viruses).

2. Possession of any of the aforementioned items with the intent to use them for the commission of one of the computer-related criminal offenses. Any state adopting this incrimination may, by law, stipulate that a certain quantity of such items constitutes a qualifying condition. However, actions involving these activities are exempt from liability if they are not intended for the commission of a computer-related criminal offense (e.g., when used for authorized testing or protection of a computer system).

Another international instrument in this field - Directive 40/2013/EU of the European Parliament (2013) - prescribes punishable attacks directed against information systems. This directive amended Council Framework Decision 2005/222/JHA,[10] this directive, as part of the "acquis communautaire," aims to harmonize the criminal legislation of the European Union member states in the field of attacks against information systems by establishing minimum rules concerning the definition of computer-related criminal offenses and the prescription of criminal sanctions for their perpetrators. Within the framework of this directive, information systems are identified as a key element of political, social, and economic interaction in the European Union. The uninterrupted use of

8 Dragojlović, J., (2023). Jurisdiction for criminal offenses of cybercrime – international and national standards, Pravo teorija i praksa, 40(1), str. 63-83.

9 Vojković, G., Štambuk Šunjić, M. (2006). Konvencija o kibernetičkom kriminalu i Kazneni zakon Republike Hrvatske. *Zbornik Pravnog fakulteta u Splitu*, 43(1), str. 123-136.

10 Marković, I. (2012). Evropsko krivično pravo. *Pravni život,* 61(12), str. 503-520.

information systems, as well as their security, quality, efficiency, and proper functioning within individual EU member states, is of vital importance for the development of both the internal market and a modern, innovative, and competitive market economy.

Directive 40/2013/EU of the European Union (2013) establishes a system of criminal liability and punishability for offenses involving the creation and use of so-called botnets, which consist of remotely controlling a significant number of computers by infecting them through the installation of malicious software, thereby facilitating precisely targeted cyberattacks.[11] These are situations in which such a network - a botnet - is established or created, and can be activated without the knowledge or consent of the owner or user of the computers, in order to initiate attacks on a large scale. Such attacks typically have the capacity, capability, and power to cause significant harm to any natural or legal person. These types of extensive attacks can result in substantial economic damage, both through the disruption of information systems and communications, and through the loss or alteration of commercially sensitive confidential information and data.

THE MISUSE OF COMPUTER VIRUSES UNDER THE LAW OF THE REPUBLIC OF SERBIA

Criminal liability for the creation and dissemination (distribution) of computer viruses, based on international standards, is currently provided for in only a small number of modern criminal legislations. In the countries of Southeastern Europe, this incrimination is prescribed by the Criminal Code of the Republic of Serbia. Apart from Serbia, only three other legal systems in the region recognize this incrimination: Montenegro, North Macedonia, and Republika Srpska – Bosnia and Herzegovina. Under the law of the Republic of Serbia, the Criminal Code[12] in Chapter Twenty-Seven, entitled "Criminal Offenses against the Security of Computer Data," the Criminal Code of the Republic of Serbia provides, among other offenses, the computer-related criminal offense "Creation and Insertion of Computer Viruses" (Article 300). This offense consists of creating a computer virus with the intent of inserting it into another person's computer or computer network.[13]

Apart from the security of computer data, in terms of the protected object, the computer virus itself constitutes the object of attack in this criminal offense. A computer virus is a program that, once loaded into a computer's memory, can spread uncontrollably and destroy existing data or programs on that computer. In the broadest sense, computer viruses are defined by electrical engineering experts as a specific type of computer program capable of self-replication, spreading covertly, and infecting other programs in order to achieve a goal predetermined by the virus author.

It is important that the object in question is a "virus," that is, a computer program which is suitable, appropriate, or sufficient to cause certain changes or damage to the use or functionality of another person's computer, either wholly or partially.[14] The concept of a computer virus is defined by the Criminal Code itself (Article 112, point 20) as a computer

11 Bača, N., Ćosić, J. (2013). Prevencija računalnog kriminaliteta. *Policija i sigurnost*, 22(1), str. 146-158.

12 Službeni glasnik RS, br. 85/2005, 88/2005, 107/2005, 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016, 35/2019 i 94/2024.

13 Dragojlović, J. (2025). *Krivično pravo. Posebni deo.* Novi Sad: Pravni fakultet za privredu i pravosuđe, str. 241-242.

14 Stojanović, Z., Delić, N. (2013). *Krivično pravo. Posebni deo*. Beograd:Pravni fakultet, str. 256-257.

program or another set of instructions introduced into a computer or computer network, designed to replicate itself and affect other programs or data in the computer or network by adding this program or set of instructions to one or more computer programs or data. Since it represents only a specific type of computer program, it is also important to note the concept of a computer program (Article 112, point 19), defined as an organized set of instructions used to control the operation of a computer and to solve a specific task with the help of the computer.

At this point, due to the topicality of the subject, it is important to highlight the solution contained in the Draft Law on Amendments and Supplements to the Criminal Code from November 2024 (Articles 13 and 46), which introduces two innovations in this area:

1. A change in the name of the criminal offense, which would now be called **"Creation and Insertion of a Malicious Computer Program"** (Article 46) and

2. A revised conceptual and substantive definition of a **"computer virus"** (Article 13). According to the proposed solution, it is now termed a **"malicious computer program"** (Article 112, point 20). This is a program created with the purpose of causing harm to a computer, computer network, or computer data, and is inserted into a computer with the intent of compromising the confidentiality, integrity, or availability of computer data, applications, and operating systems, or otherwise interfering with the operation of a computer or network.

In this way, the domestic legal provision is aligned with contemporary needs, international standards, and European Union regulations. The content of a computer virus is specified more precisely, as the concept now comprehensively defines computer programs created with the intent to cause damage to a computer, computer network, or computer data.

The act constituting the basic form of the offense is defined as the **creation**.[15] This involves the preparation, composition, or creation of a new, previously non-existent computer program in the form of a **virus**. For the offense to exist, such activity must be carried out with a specific intent on the part of the perpetrator. This intent refers to the insertion of the newly created computer virus into another person's computer or computer network. This intent, which defines **direct intent** as the form of the perpetrator's culpability, must exist at the moment the act of execution is undertaken, regardless of whether this intent is ultimately realized in the specific case.[16]

For this offense, which may be committed by any person—but in practice most often by a technically trained individual—the law alternatively prescribes either a fine or imprisonment of up to six months. In addition to the penalty, the perpetrator is obligatorily subjected (paragraph 3) to a **security measure** in the form of confiscation of the objects, devices, and tools used to commit the offense, regardless of whether they are in the perpetrator's ownership or not.

A more severe, qualified form of this criminal offense (paragraph 2) exists in cases where a computer virus is inserted or introduced into another person's computer or computer network, regardless of whether the virus was created by the perpetrator or by

15 Dragojlović J., Danojlić, M., (2015). Krivično delo pravljenje i unošenje računarskih virusa kao oblik ugrožavanja računarskih sistema, U: Bejatović, M., (urednik), Zbornik radova, Prilagođavanje pravne regulative aktuelnim trendovima u regionu, Pravni fakultet za privredu i pravosuđe, Novi Sad, str. 639-648.

16 Delić, N. (2021). *Krivično pravo. Posebni deo.* Beograd: Pravni fakultet, str.330-331.

another individual, thereby causing harm to another natural or legal person. Such harm may be of a property (material) nature or non-property (immaterial, affective) nature. This offense is qualified by the **more serious consequence**- the damage caused - which must be in a causal relationship with the act of execution. For this offense, the law alternatively prescribes either a fine or imprisonment of up to two years.

ABUSE OF COMPUTER VIRUSES IN REGIONAL COMPARATIVE CRIMINAL LAW

The Law of Bosnia and Herzegovina

Of the four legislative texts in the field of substantive criminal law in Bosnia and Herzegovina, within the system of computer-related criminal offenses, only the Criminal Code of the Republic of Srpska[17] provides for a specific incrimination under the title: "Creation and Introduction of Computer Viruses" (Article 409). Specifically, in Chapter Thirty-Two, this offense is included within the group of criminal offenses against the security of computer data, highlighting a terminological distinction of these incriminations in comparison with other analyzed comparative legislations (which use the term "računarski" [*computer-related*] rather than "kompjuterski" [*computer*]).

The criminal offense of creating and introducing computer viruses manifests itself in two forms: a) the basic form, and b) the aggravated form of the offense. The basic offense consists of creating a computer virus with the intent of introducing it into another person's computer, computer network, or telecommunication network.

The object of protection of this offense is the security of the proper, efficient, lawful, and reliable functioning of computers, computer networks, or telecommunication networks. The object of attack in this offense is the computer virus. This is a computer program which, once introduced into a computer's memory, spreads uncontrollably and destroys the data or programs stored on that computer.

The act of commission of this offense is understood as the making, creation, production, or composition of a previously non-existent computer virus, carried out in a manner and through procedures by which, in computer technology, a virus as a computer program is generated.[18] The determination of what constitutes a virus, how it is created or composed, and how it is introduced into a computer is made by the court on the basis of expert findings and opinions provided by specialists in computer and information technology. The act of creation involves the application of certain technical procedures through which a new computer virus (with new properties or effects) is generated, or the effect, scope, or functionality of an already existing virus—previously developed by another person - is enhanced.

For this criminal offense to exist, it is essential that the computer virus is created with the intent of being introduced into another person's computer or computer/telecommunication network, regardless of whether such introduction actually occurs in a specific case. The consequence of the offense consists in the violation - damage or

17 *Službeni glasnik Republike Srpske, br. 64/2017, 104/2018, 15/2021, 89/2021, 73/2023, 9/2024, 105/2024, 1472025, 19/2025 i 31/2025.*

18 Jovašević, D., Mitrović, Lj., Ikanović, V. (2021). *Komentar Krivičnog zakonika Republike Srpske*. Banja Luka: Službeni glasnik, str. 807-809.

impairment (to a greater or lesser extent) - of other programs within a computer or computer network, the inability to use normally the programs stored in the computer, or the disruption of data processing within the computer.

The perpetrator of this offense may be any person, while in terms of culpability, direct intent is required. This highest form of conscious and voluntary conduct is characterized by a specific subjective element - the intent of the perpetrator to insert the created computer virus into another person's computer. Such intent must exist at the very moment the act of execution - the creation of the virus - is undertaken. In fact, this intent must motivate the perpetrator to commit the act of execution, though it need not be realized in every particular case.

For this offense, the law alternatively prescribes either a fine or imprisonment of up to six months. In addition to the penalty, the perpetrator is obligatorily subjected (paragraph 3) to a security measure consisting of the confiscation of the objects - devices and tools - used to commit the offense, i.e., by means of which the virus was created or deployed (*instrumenta sceleris*).

A more severe form of the offense (paragraph 2) exists if the introduction of a computer virus into another person's computer or computer network results in damage. The qualifying circumstance in this case is the scope, intensity, or nature of the resulting consequence. The consequence appears in the form of injury or damage, which may be either pecuniary or non-pecuniary, of any amount or value, and which is the result of the perpetrator's negligence.

Unlike the consequence of endangering the security of a computer or telecommunication network which constitutes the outcome of the basic form of the offense the aggravated form requires a consequence in the form of actual harm. It is essential that a causal link exists between the harm of any kind, in any amount or value and the act of execution, i.e., the introduction of the computer virus. This causal relationship must be established by the court in each particular case as a matter of fact.

The Law of Montenegro

The second legislative text in the Southeastern European region that explicitly establishes criminal liability for the misuse of computer viruses is the Criminal Code of Montenegro[19] in Chapter Twenty-Eight, entitled "Criminal Offenses against the Security of Computer Data," within the system of computer-related criminal offenses, the Criminal Code of Montenegro provides for the offense titled "Creation and Insertion of Computer Viruses" (Article 351). This offense consists of creating a computer virus with the intent of introducing it into another person's computer system. In addition to the security of computer data, as the object of protection, the computer virus constitutes the object of attack.

The Criminal Code (Article 142, point 22) provides the definitional meaning of this legal concept, according to which a computer virus is considered to be "a computer program that endangers or alters the functions of a computer system and modifies, compromises, or unlawfully uses computer data." This definition of a computer virus remained in force in

19 Službeni list Republike Crne Gore, br. 70/2003, 13/2004, 47/2006, 40/2008, 25/2010, 32/2011, 64/2011, 40/2013, 56/2013, 42/2015, 58/2015, 44/2017, 49/2018, 3/2020, 26/2021, 144/2021, 145/2021, 110/2023 i 123/2024.

Montenegro until 2020, when, following the adoption of an amendment to the Criminal Code[20] a significant amendment was made to this incrimination, removing the term "computer virus" from the definitional description of the object of attack, but not from the title of the offense (which appears to be an oversight by the legislator).

According to the new legal description, the object of attack in the offense under Article 351 of the Criminal Code of Montenegro is a "malicious computer program." A malicious computer program (Article 142, point 22) is defined as a program created to cause harm to a computer, computer network, or computer data, which is introduced into a computer without the user's consent with the intent of compromising the confidentiality, integrity, or availability of computer data, applications, or operating systems, or otherwise interfering with the operation of a computer or computer network.

The offense under Article 351 of the Criminal Code of Montenegro consists of the following constitutive elements: a) act of execution: defined as the creation of a new, previously non-existent malicious computer program (virus); and b) intent: the act must be carried out with a specific intent, which motivates the perpetrator to commit the offense and must exist at the moment the act is undertaken. However, this intent need not be realized in a specific case. The intent consists of inserting the created malicious computer program (virus) into another person's computer system, i.e., a system belonging to any other natural or legal person.

The perpetrator of the offense may be any person, while in terms of culpability, **direct intent** is required, qualifying the perpetrator's intent to insert the malicious computer program into another person's computer system, regardless of whether this was actually carried out in a specific case.

For this offense, the law alternatively prescribes either a fine or imprisonment of up to **one year**. In addition to the penalty, the perpetrator is mandatorily subject to a **security measure** consisting of the confiscation of objects (devices and tools) used to commit the offense (*instrumenta sceleris*).

A more severe form of the offense (paragraph 2) exists if the perpetrator inserts a malicious computer program (virus) into another person's computer system, thereby causing harm. This offense is qualified by the following circumstances: a) act of execution: the insertion (writing, embedding) of a malicious computer program, regardless of whether it was created by the perpetrator or by a third party; b) the malicious computer program is inserted into another person's computer system, i.e., a system belonging to another natural or legal person, not the perpetrator; c) consequence: the act results in harm, causing damage (either pecuniary or non-pecuniary) to another natural or legal person, irrespective of the type, significance, or scope of the damage.

For this aggravated form of the offense, the law alternatively prescribes either a fine or imprisonment of up to **two years.**

The Law of North Macedonia

The last legislative text in the region surrounding the Republic of Serbia that, based on international standards, establishes liability and punishability for the criminal

20 Službeni list Republike Crne Gore, br. 144/2021.

offense titled "Creation and Insertion of Computer Viruses" is the Criminal Code of North Macedonia (Article 251a).[21] However, unlike the previous legal solutions, this offense is, based on the type of protected object, classified within the group of criminal offenses against property (Chapter Twenty-Three). Furthermore, when defining the concept and content of computer-related criminal offenses, the Macedonian legislator uses the term "computer" rather than "computer related".

The criminal offense "Creation and Insertion of Computer Viruses" consists of creating a computer virus or acquiring one from another source with the intent of introducing it into another person's computer or computer network. [22] While the object of protection, according to the group protected object, is property (or the right to property), the object of attack is the computer virus.

However, unlike the previously mentioned legislative texts, the Macedonian legislator does not define this term under "meaning of legal expressions" (Article 122), although related terms are defined in this section, such as: a) computer system – a device or a group of interconnected devices, of which one or more perform automatic data processing according to a specific program (point 26) and b) computer data – a representation of facts, information, or concepts in a form suitable for processing by a computer system, including a program suitable for operating the computer system (point 27).

The act of commission of this criminal offense consists of two alternatively prescribed activities. These are:[23] a) creation – the making, designing, composing, or constructing of a computer virus; and b) acquisition – receiving, accepting, or using a computer virus created by another party.

For the offense to exist, it is essential that any of the alternatively prescribed activities within the act of commission be carried out with a specific intent – namely, the intent to introduce the computer virus into another person's computer or computer network, regardless of whether this intent is realized in the specific case. However, the intent must be present on the part of the perpetrator at the time the act is undertaken, and it should motivate the perpetrator to commit the act.

The perpetrator of the offense may be any natural or legal person, while in terms of culpability, direct intent is required, qualifying the legally prescribed intent with which the perpetrator acts in committing this offense. For a natural person, the law alternatively prescribes either a fine or imprisonment of up to one year. If the perpetrator is a legal entity, a fine is prescribed (paragraph 5).

According to explicit statutory provision, attempt to commit this offense is punishable (paragraph 4).

The criminal offense under Article 251a of the Criminal Code appears in two more severe, qualified forms.

21 Služben vesnik na Republika Makedonija, br. 37/96, 80/99, 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 i 132/2014, 160/2014, 199/2014, 196/2015, 226/2015, 169/2016, 97/2017, 170/2017, 248/2018, 36/2023 i 188/2023.

22 Nikolovska, S. (2013). *Metodika na istražuvanje kompjuterski kriminalitet*. Skopje: Fakultet za bezbednost, str. 143-148.

23 Zvrlevski, M., Andonova, S., Milošeski, V, (2014). Atanasov, R. (2021). *Priračnik za kompjuterski kriminal*. Skopje: OSCE, str. 121-127.

The first aggravated form (paragraph 2) is committed by a person who, through the use of a computer virus, causes damage to another person's computer, computer system, computer data, or computer program. This is a consequence-based offense, meaning the act of commission consists of causing damage (of any kind, pecuniary or non-pecuniary) to another person's computer, computer system, computer data, or computer program. The act is carried out in a specific manner – by using, employing, or inserting a computer virus. For this offense, the law prescribes imprisonment from six months to three years.

The most severe form of this criminal offense (paragraph 3) occurs in two manifestations: a) offense qualified by a more severe consequence – if the use of a computer virus causes "greater" damage to another natural or legal person. "Greater" pecuniary benefit or "greater" pecuniary damage (Article 122, point 34) is defined as benefit or damage corresponding to the amount of five average monthly personal incomes in North Macedonia at the time of the offense; b) offense qualified by a special circumstance – method of execution – collective or group commission, occurring if the offense is carried out by a group of multiple persons specifically formed to commit the computer-related criminal offense. For this offense, the law prescribes imprisonment from one to five years.

CONCLUSION

The development of modern information and communication, as well as computer technology, alongside numerous benefits for individuals, the economy, and society as a whole, has also brought new challenges in the form of their misuse. This has led to the emergence of a new type of computer crime, representing a sophisticated method of committing previously existing "classic" criminal offenses. A particularly dangerous form of such computer misuse, which has become increasingly significant in recent times, manifests in the **malicious creation, insertion, distribution, or propagation of various types of computer viruses**. These are malicious computer programs designed to cause harm to a computer, computer network, or computer data, introduced into a computer with the intent to compromise the confidentiality, integrity, or availability of computer data, or to otherwise disrupt the operation of a computer or computer network.

In order to combat such unlawful activities by individuals or groups, modern criminal legislation in Serbia, as well as comparative legislation in regional states – Montenegro, North Macedonia, and the Republika Srpska (BiH) – based on international standards contained in: a) the **Council of Europe Convention on Cybercrime** and b) **Directive 40/2013/EU of the European Parliament and of the Council,** establishes a specific criminal offense with almost identical content, constitutive elements, and characteristics: the **creation and insertion of computer viruses (or malicious computer programs) into another person's computer or computer network.**

This offense, in addition to protecting the **security of computer data (or systems)** as the object of protection and the **computer virus** as the object of attack, prescribes as the act of commission the activity of **creating a computer virus by any means**, with the intent of introducing or inserting it into another person's computer, computer system, or telecommunications network. For the basic form of the offense, alternative penalties are prescribed: **a fine or imprisonment of up to six months** (Serbia, Republika Srpska), or **imprisonment of up to one year** (Montenegro, North Macedonia).

Beyond the basic form, most of the analyzed criminal codes prescribe only **one aggravated form**, which is qualified by the consequence resulting from the insertion of the computer virus. This aggravated consequence arises in the form of damage caused to another person's computer or computer system (for which a **fine or imprisonment of up to two years** is alternatively prescribed – Serbia, Republika Srpska, Montenegro). Only in the legislation of North Macedonia are **two aggravated forms** established: a) causing any damage (for which a fine or imprisonment of up to two years is prescribed), and b) causing "greater" damage (punishable by imprisonment from **one to five years**).

In addition to the more precise definition of the offense of **creation and insertion of computer viruses** (through the adoption of the Draft amendment to the Criminal Code of November 2024), it is also appropriate to consider the following **de lege ferenda** issues: 1) increasing the statutory maximum imprisonment for the basic form of the offense to **up to one year** and 2) introducing an aggravated qualification of the offense based on the following qualifying circumstances: a) causing **property damage** in the legally prescribed amount of 450,000 or 1,500,000 dinars, b) committing the act with a specific type of intent, namely the intent to **obtain unlawful pecuniary gain** or to **cause pecuniary harm** to another person and c) committing the act against a specific type of **passive subject** – a computer or computer system of significance to state authorities, public services, institutions, enterprises, or other entities of general importance.

Joko Dragojlović, vanredni profesor
Pravni fakultet za privredu i pravosuđe u Novom Sadu,
Univerzitet Privredna akademija u Novom Sadu

KRIVIČNA ODGOVORNOST ZA ZLOUPOTREBU RAČUNARSKIH VIRUSA – STANJE I PERSPEKTIVE

Apstrakt:

S obzirom na sve veću raširenost gotovo svakodnevne primene računarskih programa, podataka ili sistema u različitim oblastima ljudskog, društvenog ili privrednog života, potrebno je obezbediti, a potom i unaprediti njihovu efikasnu, zakonitu i kvalitetnu, ne samo tehničku, već i pravnu zaštitu. Na taj način se opšta računarska bezbednost podiže na kvalitetno viši nivo. Ona je posebno ugrožena različitim protivpravnim delatnostima zloupotrebe računarskih programa, podataka ili sistema.

Posebno opasan vid takve računarske zloupotrebe se javlja u obliku zlonamernog pravljenja, unošenja, distribucije ili širenja različitih vrsta računarskih virusa. Radi se o zlonamernim računarskim programima koji su napravljeni sa ciljem nanošenja štete računaru, računarskoj mreži ili računarskim podacima i koji se ubacuje u računar sa namerom ugrožavanja poverljivosti, celovitosti ili dostupnosti računarskih podataka, odnosno sa ciljem ometanja rada računara ili računarske mreže na druge načine. Krivično zakonodavstvo Srbije, kao i neka druga uporedna zakonodavstva predviđaju specifičnu

inkriminaciju pravljenja ili širenja računarskih virusa, o čijim elementima, karakteristikama, oblicima ispoljavanja i sadržini govori ovaj rad.

Ključne reči: *računarski program, računarski virus, zloupotreba, krivično delo, odgovornost*

REFERENCES

1. Bača, N., Ćosić, J. (2013). Prevencija računalnog kriminaliteta [Prevention of Computer Crime]. *Policija i sigurnost*, 22(1), str. 146-158.
2. Delić, N. (2021). *Krivično pravo. Posebni deo [Criminal law – Special part]*. Beograd: Pravni fakultet.
3. Đorđević, Đ. (2011). *Krivično pravo. Posebni deo [Criminal law – Special part]*. Beograd: Kriminalističko-policijska akademija.
4. Dragojlović J., Danojlić, M., (2015). *Krivično delo pravljenje i unošenje računarskih virusa kao oblik ugrožavanja računarskih sistema [The Criminal Offense of Creating and Inserting Computer Viruses as a Form of Threat to Computer Systems]*, In: Bejatović, M., (editor), Proceedings, **Adapting Legal Regulation to Current Trends in the Region**, Faculty of Law for Economy and Judiciary, Novi Sad, str. 639-648**.**
5. Dragojlović J., Krstinić D., (2015). Evropski standardi u borbi protiv visokotehnološkog kriminaliteta i njihova implementacija u zakonodavstvu Republike Srbije [European Standards in Combating High-Tech Crime and Their Implementation in the Legislation of the Republic of Serbia]. *Evropsko zakonodavstvo*, 14(51), str. 92-103.
6. Dragojlović, J. (2025). *Krivično pravo. Posebni deo [Criminal law – Special part]*. Novi Sad: Pravni fakultet za privredu i pravosuđe.
7. Dragojlović, J., (2023). Jurisdiction for criminal offenses of cybercrime – international and national standards. *Pravo teorija i praksa*, 40(1), str. 63-83.
8. Dragojlović, J., Koprivica A., (2023). *Osvrt na računarski kriminalitet u zakonodavstvu Republike Srbije [Overview of Computer Crime in the Legislation of the Republic of Serbia]*, In: Počuča, M., (editor), Proceedings, **Two Decades of Development in Legal Thought**, Faculty of Law for Economy and Judiciary, Novi Sad, str. 410-420.
9. Dulčić, K. (2007). Oblici štete od računalnih virusa i odgovornost za štetu [Types of Damage Caused by Computer Viruses and Liability for Such Damage]. *Zbornik Pravnog fakulteta Sveučilišta u Rijeci,* 28(1), str. 189-228.
10. Jovašević, D., Mitrović, Lj., Ikanović, I. (2017). *Krivično pravo Republike Srpske. Posebni deo* [Criminal Law of the Republika Srpska: Special Part]. Banja Luka: Univerzitet Apeiron.
11. Jovašević, D., Mitrović, Lj., Ikanović, V. (2021). *Komentar Krivičnog zakonika Republike Srpske* [Commentary on the Criminal Code of the Republika Srpska]. Banja Luka: Službeni glasnik.
12. Marković, I. (2012). Evropsko krivično pravo [European Criminal Law]. *Pravni život,* 61(12), str. 503-520.
13. Mrvić Petrović, N. (2005). *Krivično pravo [Criminal law]*, Beograd: Službeni glasnik.
14. Nikolovska, S. (2013). *Metodika na istražuvanje kompjuterski kriminalitet [Methodology for the Study of Computer Crime]*. Skopje: Fakultet za bezbednost.
15. Krivični zakonik Severne Makedonije [Criminal Code of the Republic of North Macedonia], *Služben vesnik* na Republika Makedonija, br. 37/96, 80/99, 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 i 132/2014, 160/2014, 199/2014, 196/2015, 226/2015, 169/2016, 97/2017, 170/2017, 248/2018, 36/2023 i 188/2023.
16. Krivični zakonik Republike Srpske [Criminal Code of the Republika Srpska], *Službeni glasnik Republike Srpske, br. 64/2017, 104/2018, 15/2021, 89/2021, 73/2023, 9/2024, 105/2024, 1472025, 19/2025 i 31/2025.*
17. Krivični zakonik [Criminal Code], *Službeni glasnik* RS, br. 85/2005, 88/2005, 107/2005, 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016, 35/2019 i 94/2024.
18. Krivični zakonik Crne Gore [Criminal Code of Montenegro], *Službeni list* Republike Crne Gore, br. 70/2003, 13/2004, 47/2006, 40/2008, 25/2010, 32/2011, 64/2011, 40/2013, 56/2013, 42/2015, 58/2015, 44/2017, 49/2018, 3/2020, 26/2021, 144/2021, 145/2021, 110/2023 i 123/2024.
19. Stojanović, Z., Delić, N. (2013). *Krivično pravo. Posebni deo [Criminal law special part]*. Beograd: Pravni fakultet.
20. Vojković, G., Štambuk Šunjić, M. (2006). Konvencija o kibernetičkom kriminalu i Kazneni zakon Republike Hrvatske [Convention on Cybercrime and the Criminal Code of the Republic of Croatia]. *Zbornik Pravnog fakulteta u Splitu*, 43(1), str.123-136.
21. Zirojević, M., Ivanović, Z. (2022). *Cyber law*. Beograd: Institut za uporedno pravo.
22. Zvrlevski, M., Andonova, S., Milošeski, V, (2014). Atanasov, R. (2021). *Priračnik za kompjuterski* criminal [Handbook on Computer Crime]. Skopje: OSCE.

CIP - Каталогизација у публикацији
Библиотеке Матице српске, Нови Сад

34:316.3”20”(082)

INTERNATIONAL Scientific Conference “Legal days - Prof. Slavko Carić” (22 ; 2025 ; Novi Sad)
XXII International Scientific Conference “Legal days - Prof. Slavko Carić”, “Law and Justice”, October 10th and 11th 2025 in Novi Sad : [proceedings] / [The Editor-in-Chief Milan Počuča]. - Novi Sad : The University of Business Academy, The Faculty of Law for Commerce and Judiciary, 2025 (Novi Sad : Feljton). - 614 str. : tabele, graf. prikazi ; 24 cm

Radovi na engl. jeziku. - Tiraž 100. - Str. 15: Introductiory remarks / Milan Počuča. - Napomene i bibliografske reference uz tekst. - Bibliografija uz svaki rad. - Rezime na srp. jeziku uz svaki rad.

ISBN 978-86-86121-84-4

a) Правна наука -- Савремено друштво -- 21. в. -- Зборници

COBISS.SR-ID 176461065