MOLDOVA STATE UNIVERSITY
LAW FACULTY
DOCTORAL SCHOOL OF LEGAL SCIENCES

As Manuscript

CZU: 343.222:343.346.8(478)(043)

STRÎMBEANU ALEXANDRU

CRIMINAL LIABILITY FOR ILLEGAL ACCESS TO COMPUTERIZED INFORMATION

Specialty554.01 – Criminal Law and Criminal Enforcement Law

Summary of the Doctor of Law thesis

CHIȘINĂU, 2023

The Thesis has been developed within the Doctoral School of Legal Sciences,
Moldova State University

PhD Assessment Committee:

The President of the PhD Assessment Committee: STATI Vitalie, Doctor of Law, University Professor, MSU
PhD Supervisor: BRÎNZA Serghei, Habilitated Doctor of Law, University Professor, MSU
Official reviewers:

1. GRECU Raisa, Habilitated Doctor of Law, Assistant Professor, Faculty of Law, "Constantin Stere" University of European Political and Economic Studies
2. CERNOMOREȚ Sergiu, Doctor of Law, Assistant Professor, Faculty of Security Sciences, State University of Physical Education and Sports
3. COPEȚCHI Stanislav, Doctor of Law, Assistant Professor, MSU

Secretary of the PhD Assessment Committee: MIHAILOV Tatiana, Doctor of Law, University Lector, MSU

The defense will take place on June, 23 2023, time 10.00, in the meeting of the Doctoral Committee of the Doctoral School of Legal Sciences of the State University of Moldova, in room 119, block II of the State University of Moldova (municipality of Chisinau, str. Mihail Kogălniceanu, 67).

The doctoral thesis and the summary can be consulted at the USM Library, on the website of ANACEC and on the website of the Faculty of Law of the State University of Moldova (http://drept.usm.md).

The summary was sent to May, 19 2023.

PhD Supervisor:
Brînza Serghei, Habilitated Doctor
of Law, University Professor
Moldova State University _____

Author:
Strîmbeanu Alexandru _____

Secretary of the PhD Assessment Committee:
Mihailov Tatiana, Doctor of Law,
University Lector
Moldova State University _____

CONTENT

CONCEPTUAL GUIDELINES OF THE RESEARCH

Topicality of theme. The criminalization of illegal access to computerized information in the criminal law of the Republic of Moldova was determined by the appearance in the 80's of the last century in local society of relations regarding access to computerized information. The emergence of these relationships marked the transition in our country from a post-industrial society to an information society. After the development of these relations, it was found that the existence of extra-penal regulations regarding access to computerized information is not sufficient for the development and safe conduct of social relations regarding authorized or permitted access to computerized information. Computerized information has rapidly attained the status of a resource of increasing significance. Under these conditions, the need arose to ensure authorized or permitted access to computerized information through appropriate protection measures against illegalities characterized by an increased social danger. Consequently, only in 2002, in the Criminal Code of the Republic of Moldova from 1961 (hereafter – CrC RM from 1961)[1], art. 176[1]"Illegal (unsanctioned) access to computerized information". Later, in the Criminal Code in force of the Republic of Moldova[2] (hereinafter – CrC RM), illegal access to computerized information was criminalized in article 259. The interpretation and application over two decades of art. 259 CrC RM has demonstrated that it is largely not adapted to current social challenges and, therefore, does not allow the effective defense of social relations regarding authorized or permitted access to computerized information. Therefore, the deep analysis of the problems related to the interpretation and application of this article, as well as the proposal of solutions aimed at contributing to the effective functioning of the mechanism for preventing and combating illegal access to computerized information, becomes urgent.

The theme's inclusion in international concerns. With the advent of the first computer, the computer environment became a vulnerable part of the international security system. The transition from a post-industrial society to an information society has resulted in the globalization and transnationalization of computerized information. Such information can be meaningful both for a single individual and for the state and society as a whole. As a result, computer crimes in general and illegal access to computer information in particular affect security not only at the national level, but also at the international level. Due to this fact, international cooperation in the field of preventing and combating these crimes becomes particularly important.

According to para. (2) art. 6 of Law no. 1069 of 22.06.2000 regarding informatics (hereinafter - Law no. 1069/2000), "for the Republic of Moldova, international relations in the field of informatics are regulated by international conventions and agreements to which it is a party. [...]".[3]In this context, the Convention of the Council of Europe on computer crime, adopted in Budapest on 23.11.2001[4](hereinafter – the Budapest Convention) is included, which was ratified by Law no. 6 of 02.02.2009 for the ratification of the Council of Europe Convention on computer crime.[5]According to art. 2 of this act, "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, the access to

---

[1] Codul penal al Republicii Moldova: nr. 41 din 24.03.1961. În: *Veştile Sovietului Suprem al R.S.S. Moldoveneşti*,1961, nr. 10, 41.

[2] Codul penal al Republicii Moldova: nr. 985 din 18.04.2002. În: *Monitorul Oficial al Republicii Moldova*, 2002, nr.128-129, 1012.

[3] Legea cu privire la informatică: nr. 1069 din 22.06.2000. În: *Monitorul Oficial al Republicii Moldova*, 2001, nr. 73-74, 547.

[4]*Convention on Cybercrime*. [citat 06.03.2022] Disponibil: https://rm.coe.int/1680081561

[5] Legea pentru ratificarea Convenţiei Consiliului Europei privind criminalitatea informatică: nr. 6 din 02.02.2009. În: *Monitorul Oficial al Republicii Moldova*, 2009, nr. 37-40, 104.

the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.”.[6]

In the same context, we are talking about Directive 2013/40/EU of the European Parliament and of the Council of 12.08.2013 on attacks against information systems and replacing Framework Decision 2005/222/JHA of the Council (hereinafter – Directive 2013/40/ EU). In the preamble of this directive it is mentioned, among other things: “it is necessary to adopt a common approach to the constitutive elements of crimes, criminalizing as common law crimes the illegal access to an IT system [...]. Member States should provide for penalties for attacks against computer systems. Those sanctions should be effective, proportionate and dissuasive and should include imprisonment and/or a fine.”[7] In accordance with art. 3 of Directive 2013/40/EU, “illegal access to information systems Member States shall take the necessary measures to ensure that the intentional and unauthorized access to an information system or part of it is criminalized when it is committed in violation of a measure of security, at least when it is not a minor case”.[8]Of course, such provisions must be viewed through the lens of Government Decision no. 1171 of 28.11.2018 for the approval of the Regulation on the harmonization of the legislation of the Republic of Moldova with the legislation of the EU. According to point 2 of this decision, “the harmonization of the legislation of the Republic of Moldova with the legislation of the EU is a continuous process, the aim of which is the integration into the internal legal order of the EU legislation, in accordance with the commitments assumed by the Republic of Moldova in the framework of the bilateral agreements concluded with the EU, of the Government's action plans, as well as with the legislative programs of the Parliament”[9].

According to paragraph (2) art. 6 of Law no. 1069/2000, “[...] in case the international conventions and agreements contain other rules than those provided by the legislation of the Republic of Moldova regarding IT, the provisions of the international conventions and agreements shall apply”.[10]However, none of the norms of international law, which contain the recommendation to criminalize illegal access to computer information, are directly applicable. The Moldovan legislator “adapted” these norms in a not quite successful manner, a fact demonstrated by the mediocre quality of art. 259 CrC RM. Consequently, in the process of perfecting art. 259 CrC RM, one of the main benchmarks should be the letter and spirit of the international regulations regarding the prohibition of illegal access to computerized information.

The framing of the theme in national and regional concerns. We initiated the scientific approach based on the materials on the topic of the thesis, dedicated to the criminal law aspects of the offenses provided for in art. 259 CrC RM, which were published by:S. Bacinschi; A. Barbăneagră; A. Borodac; M. Botnarenco; S. Brînza; S. Copețchi; S. Crijanovschi; L. Dumneanu; M. Gheorghiță; A. Ghimpu; L. Gîrla; R. Gojan; S. Grișciuc-Bucica; D. Gurev; N. Lazareva; A. Pareniuc; A. Smochină; V. Soltan; Iu. Stan; V. Stati, etc. (Republic of Moldova); Gh. Alecu; V. Coman; S. Corlățeanu; A. Crăciunescu; V. Dobrin; M. Dobrinoiu; A.T. Drăgan; M. Dunea; C. Duvac; G. Florescu, V. Florescu;

---

[6]*Convention on Cybercrime*. [citat 06.03.2022] Disponibil: https://rm.coe.int/1680081561

[7]*Directiva 2013/40/UE a Parlamentului European și a Consiliului din 12.08.2013 privind atacurile împotriva sistemelor informatice și de înlocuire a Deciziei-cadru 2005/222/JAI a Consiliului.*[citat 18.12.2020] Disponibil: https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32013L0040&from=en

[8] Ibidem.

[9] Hotărârea Guvernului pentru aprobarea Regulamentului privind armonizarea legislației Republicii Moldova cu legislația Uniunii Europene: nr. 1171 din 28.11.2018. În: *Monitorul Oficial al Republicii Moldova*, 2018, nr. 499-503, 1314.

[10] Legea cu privire la informatică: nr. 1069 din 22.06.2000. În: *Monitorul Oficial al Republicii Moldova*, 2001, nr. 73-74, 547.

M. Gorunescu; A.V. Iugan; L.C. Kövesi; C. Manea; C. Marin; T. Medeanu; A.C. Moise; C. Moțoc; N. Niță; R.A. Nestor; F.-V. Onofrei; Z. Sadâc; P. Tamas-Erno; O. Vară; G. Zlati, etc. (Romania); P.P. Andrușko; D.S. Azarov; S.Ia. Burda; M.V. Karcevski; N.S. Kozak; Iu.V. Oriol; D.O. Ricika; N.A. Rozenfeld; A.Ia. Skiba; T.I. Sozanski; A.V. Zaghika, etc. (Ukraine); T.A. Abramean; O.Ia. Baev; I.R. Beghișev; A.M. Doronin; M.Iu. Dvoreţki; M.A. Efremova; R.R. Gaifutdinov; A.A. Grebenkov; O.S. Guzeeva; Z.I. Hisamova; L.V. Ivanova; D.G. Malâșenko; V.A. Meșcereakov; G.P. Novosiolov; O.S. Ozerova; A.N. Popov; E.A. Russkevici; O.M. Safonov; M.V. Staricikov; V.G. Stepanov-Eghianț; A.V. Susloparov; A.E. Șarkov; A.V. Șulga; T.L. Tropina; M.A. Zubova, etc. (The Russian Federation); N.F. Ahramenka; O.I. Bahur; L.I. Gasan; A.I. Lukașov; O.G. Nikitenko; N.A. Sivițkaia; N.A. Șved; Iu.N. Tanana, etc. (Republic of Belarus); A.B. Bekmagambetov; I.Ș. Borceașvili; A.M. Galiaskarova; A.T. Ismagulova; V.P. Revin; V.V. Revina, etc. (Republic of Kazakhstan); I.B.O. Agaev; G.S.O. Kurbanov, etc. (Republic of Azerbaijan), etc.

Placing the theme in an inter- and transdisciplinary context. We initiated the scientific approach with the support also of the materials on the topic of the thesis, published by the authors of some works in the field of constitutional law, criminal procedural law, informational law, IT law, national security law, civil law, intellectual property law, criminology, forensics, computer science, etc.:R. Abrihan; T. Anghel; L. Băjenaru; N. Chirpat; O. Cerbu; N.-G. Drăgulănescu; I.-T. Gigi; C. Hlopeatnicov; Gh.Iu. Ioniță; G.-I. Luncan; R.-L. Lupșa; A. Munteanu; R.N. Popescu; Iu. Rusu; D. Savu; V. Sîli; I. Soroceanu; C.O. Șofran; A.-M. Tîrziu; M. Tomescu; V. Țurcanu; I.R. Urs; I. Vasiu; L. Vasiu; M.A. Dubko; V.O. Kaleatin; A.D. Kos; Iu.V. Logvinov; V.N. Loktiuhin; V. Krâlov; S.G. Spirina; V.V. Strigunov, etc.

The purpose of the research is to thoroughly investigate the constituent elements and aggravating circumstances of the crimes provided for in art. 259 CrC RM, to highlight the vulnerabilities that characterize the interpretation and application of this article, as well as to propose solutions intended to contribute to the improvement of the mechanism of counteracting by criminal means illegal access to computerized information.

Research objectives: investigation of doctrinal views regarding liability for the crimes provided for in art. 259 CrC RM; the use of the potential, available in national regulations regarding access to computerized information, in the process of interpreting this article; identifying the degree of compatibility between art. 259 CrC RM and the regulations of international origin regarding the prohibition of illegal access to computerized information; studying the positive experience of other states in terms of preventing and combating illegal access to computerized information through criminal means; the establishment of social values defended against the crimes provided for in art. 259 CrC RM; revealing the characteristics of the material or immaterial object of the crimes provided for in this article; examination of the distinguishing features that characterize the victim of the crimes provided for in art. 259 CrC RM; establishing the structure and content of the prejudicial act provided for by this article; revealing the prejudicial consequences and the causal link in the case of the crimes provided for in art. 259 CrC RM; discussing the subjective side and the subject of the offenses provided for in this article; analysis of the circumstances that aggravate the liability for the crimes provided for in art. 259 CrC RM; the delimitation of crimes, provided for in art. 259 CrC RM, of other crimes; investigating the vulnerabilities that characterize the practice of applying art. 259 CrC RM, followed by the formulation of solutions; analysis of the shortcomings of a technical-legislative nature from which the provision of art. 259 CrC RM, followed by the formulation of proposals for *lege ferenda*.

The research hypothesis is based on the assumption that: by criminalizing the facts gathered under the marginal name of illegal access to computerized information, the legislator seeks to

establish a reasonable balance between the right of some people to freely access computerized information and the right of other people not to allows illegal access to such information; the offenses provided for in art. 259 CrC RMhave two objects, but they are not complex crimes; in the case of the crimes provided for in art. 259CrC RM, the main immaterial object is computerized information. In the case of the same crimes, the computer information destroyed, damaged, modified, blocked or copied constitutes the secondary intangible object; the computers, the computer system or the computer network, whose operation has been disrupted, form the secondary material object; the position in relation to the structure of the objective side of the crimes, provided for in art. 259 CrC RM, must be differentiated according to the normative modalities of the adjacent action within the prejudicial act; due to the unsuccessful structure of the objective side of the crimes provided for in art. 259 CrC RM, there is no possibility of effective criminal defense of social relations regarding authorized or permitted access to computerized information; it is opportune to increase liability in the case of committing crimes, provided for in art. 259 CrC RM, either on an IT system that is an integral part of the critical infrastructure, or regarding sensitive information regarding the protection of critical infrastructures.

Synthesis of research methodology and justification of chosen research methods. The research undertaken is based on the study of the specialized doctrine, the national criminal and extra-criminal legislation, the norms of international law, the EU regulations, the jurisprudence of the Constitutional Court of the Republic of Moldova and the Constitutional Court of Romania, the practice of the courts of the Republic of Moldova and from Romania.

In order to achieve the purpose and objectives revealed above, the logical (rational) method, the historical method, the systemic analysis method and the comparative method were applied.

Thus, all three postures - exegetical, dogmatic, critical - in which the study of art. 259 CrC RM, involves the use of the following categories and laws of logic: definition; specification and generalization; division and classification; differentiation and integration; analysis and synthesis; the demonstration; argumentation; reasoning, etc.

From a historical perspective, art. was researched. 176^1 "Illegal (unsanctioned) access to computerized information" from the CrC RMfrom 1961. From the same perspective, the amendments and additions that art. 259 CrC RMhas supported them over time.

The systemic analysis method was applied because art. 259 CrC RMconstitutes a part of an integral normative system whose structural elements are closely related to each other. Starting from these premises, it can be stated that, in the normative system of the Republic of Moldova, the regulations regarding access to computerized information form a system. The reference character (blanket) of the provisions of art. 259 CrC RMindicates that it can only be interpreted and applied if it is viewed through the lens of extra-criminal regulations regarding access to computerized information. Or, certain notions from art. 259 CrC RMare defined in such regulations.

The criminal framework in Georgia, Greece, the Grand Duchy of Luxembourg, the Kingdom of Belgium, the Kingdom of Denmark, the Kingdom of Spain, the Kingdom of Sweden, the Kingdom of the Netherlands (Netherlands), the Republic of Armenia, the Republic of Austria served as a reference point for the comparative law analysis. , the Republic of Belarus, the Republic of Bulgaria, the Czech Republic, the Republic of Cyprus, the Republic of Croatia, the Republic of Estonia, the Federal Republic of Germany, the Republic of Finland, the French Republic, the Republic of Italy, the Republic of Latvia, the Republic of Lithuania, the Republic of Malta, the Republic of Poland, the Portuguese Republic, the Slovak Republic, Republic of Slovenia, Kingdom of Spain, Romania, Ukraine, Hungary, etc.

CONTENT OF THE THESIS

The thesis consists of three chapters. Each chapter ends with a summary section (conclusions) of the issues addressed and the results obtained.

In Chapter 1 – *Doctrinal and normative approaches regarding criminal liability for illegal access to computerized information* – the conducted investigations focused on: scientific materials regarding criminal liability for illegal access to computerized information, published in the Republic of Moldova and abroad; the social and legal conditioning of the criminalization of illegal access to computerized information; systemic coherence between art. 259 CrC RMand the complementary provisions of the national legislation; comparative law analysis of regulations regarding illegal access to computer information.

These investigations are necessary to establish the doctrinal and normative foundation of the theoretical concept of solving the problem of liability for the crimes provided for in art. 259 CrC RM. Among the objectives of the present research are: the investigation of the doctrinal views regarding the liability for the crimes provided for in art. 259 CrC RM; the use of the potential, available in national regulations regarding access to computerized information, in the process of interpreting this article; identifying the degree of compatibility between art. 259 CrC RMand the regulations of international origin regarding the prohibition of illegal access to computerized information; studying the positive experience of other states in terms of preventing and combating illegal access to computerized information through criminal means. The achievement of these objectives is the condition for the achievement of the purpose of this thesis in the part that refers to the thorough investigation of the constituent elements and the aggravating circumstances of the crimes provided for in art. 259 CrC RM, as well as highlighting the vulnerabilities that characterize the interpretation and application of this article.

Thus, for example, in 2003 a research was published[11]in which the author of the commentary to art. 259 CrC RMis *M. Gheorghiță*.

From the point of view of the author in question, the generic legal object of the offenses provided for in art. 259 CrC RMconstitutes "all relations related to public security regarding the production, use, dissemination of the protection of information and informational resources, information processing systems with the application of ECM (electronic computing machines)".[12]Examining the special legal object, M. Gheorghiță believes that it consists of "social relations that appear in the process of collecting, processing, keeping and presenting computerized information and informational resources".[13]Although he uses the phrase "immediate object of the crime", the author in question has in mind the material object of the crime, mentioning "computer technology, i.e. various types of electronic computing machines, computing equipment (printers, scanners, analyzers, explorers, etc.), as well as different means of telecommunications, with the help of which the computing technique is connected to the information networks (network adapters, modems, etc.)".[14]

In the context of the analysis of the objective side of the offenses provided for in art. 259 CrC RM, M. Gheorghiță claims that "if the illegal access to computerized information is a procedure for committing another crime, the act committed must be classified as a crime".[15]Also, the given author records: "The composition of the offense is material. The offense is considered consummated starting

[11] BARBĂNEAGRĂ, Alexei et al. *Codul penal al Republicii Moldova. Comentariu* / Sub red. lui Alexei BARBĂNEAGRĂ. Chișinău: Arc, 2003. 836 p. ISBN 9975-61-291-1.
[12]Ibidem, p. 568.
[13]Ibidem, p. 568.
[14]Ibidem, p. 568.
[15]Ibidem, p. 569.

with the presence of at least one of the consequences listed in the law: destruction, blocking, modification or copying of information, violation of the operation of ECM, ECM systems or their networks".[16]

Characterizing the subjective side of crimes of illegal access to computerized information, M. Gheorghiță establishes that this "manifests itself through direct or indirect intent. [...] The causes and purposes of crime can be diverse: greed; revenge; envy; hooliganism; "sporting" interest; the desire to damage the competitor's business reputation, etc.".[17]

Finally, in relation to the subject of the offenses provided for in art. 259 CrC RM, M. Gheorghiță is of the opinion that he "is the natural person responsible for the committed acts, who has reached the age of 16. If the illegal access to computerized information was committed by the representative of the legal entity in its interests, the liability is borne by the immediate executor and the legal entity".[18]

The next work is authored by *A. Borodac* and dates from 2004.[19]

As a result of the discussion of the legal object of the crimes of illegal access to computerized information, the given author concludes that "the generic group object of crimes in the field of computer science is the social relations that protect computerized information security. The immediate basic object of these crimes is the social relations that protect the right of the holder of computerized information regarding its inviolability and the correct exploitation of the computerized system".[20]

The analysis of the objective side of the crimes in question allows A. Borodac to talk about three signs of it. However, the given author highlights only two such signs: "1) illegal access to computerized information; 2) destroying, damaging, blocking or copying information, or disrupting the operation of computers, systems or computer networks".[21]It is not clear what role A. Borodac attributes to the signs listed above: component parts of the prejudicial act; the prejudicial act and the prejudicial consequences?

Next, the respective author defines several notions that are used in art. 259 CrC RM: "illegal access to computerized information"; "information"; "computers"; "material information carriers"; "information system"; "computer network"; etc.

In the plan of examining the subjective constitutive elements of crimes of illegal access to computerized information, A. Borodac shows that "the subjective side of the crime is characterized by both direct and indirect intent. The subject of the crime can be any responsible natural person who has reached the age of 16, as well as a legal person".[22]

The following work dates from 2005, with *A. Barbăneagra* as co-author[23], which makes the comment on art. 259 CrC RM.

In the process of identifying the fundamental social value damaged by committing the crimes provided for in this article, A. Barbăneagra points out that "the generic object of the crime is

[16]Ibidem, p. 569.
[17]Ibidem, p. 570.
[18]Ibidem, p. 569.
[19] BORODAC, Alexandru. *Manual de drept penal. Partea specială*. Chişinău: Tipografia Centrală, 2004. 622 p. ISBN 9975-9788-7-8.
[20]Ibidem, p. 362.
[21]Ibidem, p. 364.
[22]Ibidem, p. 366.
[23] BARBĂNEAGRĂ, Alexei et al. *Codul penal comentat şi adnotat*. Chişinău: Cartier, 2005. 656 p. ISBN 9975-29-338-X.

constituted by the social relations aimed at information security".[24]In order to make the interpretation of the provisions of art. 259 CrC RM, the respective author defines the notions of "computerized information", "illegal access to computerized information", "computerized system" etc.

From the perspective of para. (1) art. 25 CrC RM, in conjunction with art. 259 CrC RM, A. Barbăneagra claims that "the crime is considered consummated from the moment one of the actions listed in the provisions of the law took place".[25]Having a different opinion from the one expressed by M. Gheorghiță and A. Borodac, A, Barbăneagra believes that, in the case of the crimes provided for in art. 259 CrC RM, the subjective side "is achieved by direct intention".[26]This opinion stems from the reporting by A. Barbăneagra of the crimes analyzed in the category of formal crimes.

This author thus reveals the characteristics of the subject of crimes of illegal access to computerized information: "The subject of the crime can be any natural person, responsible, who has reached the age of 16. The subject of the given crime can also be a legal person".[27]

A research co-authored by *V. Stati* dates from 2005.*[28]*

Among other things, this author states that "the generic legal object of the crimes in Chapter XI "Crimes in the field of information technology and telecommunications" of the special part of the Criminal Code is represented by social relations in the field of information technology and telecommunications".[29]This opinion is consistent with Law no. 254 of 09.07.2004 for the amendment and completion of the Telecommunications Law no. 520-XIII of July 7, 1995 and of the Criminal Code of the Republic of Moldova.[30]According to the given law, the title of Chapter XI of the special part of the Criminal Code was changed from "Crimes in the field of information technology" to "Crimes in the field of information technology and telecommunications". Developing the idea, V. Stati claims that "two types of crimes provided for in Chapter XI of the special part of the Criminal Code can be distinguished: a) crimes in the field of IT (provided in art. 259, 260, 261 of CrC RM); b) crimes in the field of telecommunications (provided in art. 261^1CrC RM)".[31]

Regarding the special legal object of the crimes provided for in art. 259 CrC RM, the respective author mentions that this "is a complex legal object. Thus, the main legal object is represented by social relations regarding legal access to computerized information. The secondary legal object is formed by the social relations related to the legal intervention in the information system. The material or, as the case may be, immaterial object of the crime in question is made up of: computerized information; computers; computer system; it network".[32]

In the context of examining the object of crimes of illegal access to computerized information, V. Stati sees the special quality of the participant in social relations protected by art. 259 CrC RM: "The victim of the crime of illegal access to computerized information is the owner or possessor of resources and informational systems, of technologies and means of ensuring them, i.e.: the natural person, the legal person or the state that fully or partially exercises the right of possession , use and

[24]Ibidem, p. 434.
[25]Ibidem, p. 435.
[26]Ibidem, p. 435.
[27]Ibidem, p. 435.
[28] BRÎNZA, Serghei et al. *Drept penal. Partea specială.* Chișinău: Cartier, 2005. 804 p. ISBN 9975-79-324-X.
[29]Ibidem, p. 493.
[30] Legea pentru modificarea și completarea Legii telecomunicațiilor nr. 520-XIII din 7 iulie 1995 și a Codului penal al Republicii Moldova: nr. 254 din 09.07.2004. În: *Monitorul Oficial al Republicii Moldova*, 2004, nr. 189-192, 848.
[31]BRÎNZA, Serghei et al. *Drept penal. Partea specială.* Chișinău: Cartier, 2005, p. 494. 804 p. ISBN 9975-79-324-X.
[32]Ibidem, p. 495.

disposition of resources and information systems, technologies and means of ensuring them. Also, the user of computerized information can appear as a victim".[33]

Also, the point of view regarding the structure and content of the objective side of the crimes analyzed deserves attention: "The objective side of the crime from art. 259 CrC RMincludes: a) the prejudicial act consisting in the main action of illegal access to computerized information, accompanied by the adjacent action of destroying, damaging, modifying, blocking or copying the information, of disrupting the functioning of computers, the system or the computer network ; b) harmful consequences expressed in the form of destruction, damage, modification, blocking or copying of information, disruption of the functioning of computers, the system or the computer network; c) the causal connection between the prejudicial act and the prejudicial consequences".[34]From this opinion it is clear that the crimes of illegal access to computerized information are crimes with a material component, and the prejudicial consequences constitute the mandatory secondary sign of the objective side of these crimes.

In the exegesis dedicated to the key notion that characterizes the prejudicial act provided for in art. 259 CrC RM, V. Stati states: ""Access" means using the resources of an IT system, i.e. giving instructions to an IT system, communicating with/through an IT system, storing information or finding it in an IT system. Access includes entering another computer system, connected through public telecommunications networks or another computer system from the same computer network, regardless of the communication method. The access must be illegal, that is, it must be carried out by violating regulatory security measures, with the intention of obtaining computerized information that constitutes a personal secret or a state secret, or other confidential information, the collection or dissemination of which may harm public interests or rights and the legally protected interests of natural or legal persons".[35]In the same vein, the aforementioned author distinguishes "illegal access" within the meaning of art. 259 CrC RMof other facts: "The following are not considered illegal access: 1) authorized access by the owner or possessor of resources and information systems, technologies and the means of ensuring them, for testing or protecting the information system; 2) access by public authorities in the context of criminal prosecution or the performance of operative investigative measures, in accordance with the law; 3) access to the usual and legitimate activities of design of information systems, current operating practices of information systems or legal commercial practices; 4) access to information about oneself".[36]

Concluding the examination of the objective side of the crimes analyzed, V. Stati evokes: "The crime provided for in art. 259 CrC RMis a material one. It is considered consumed from the moment of the occurrence of harmful consequences in the form of destruction, damage, modification, blocking or copying of computerized information or disruption of the functioning of computers, the system or the computer network".[37]

resenting the characteristics of the subjective side of the crimes provided for in art. 259 CrC RM, V. Stati states: "The subjective side of the crime in question is characterized by direct or indirect intent. The reasons for the offense may consist of: "sporting" interest, hooligan intentions, revenge, material interest etc.".[38]Regarding the last constituent element of the crimes examined, V. Stati's point of view mentions: "The subject of the crime is: 1) the natural person responsible, who at the

[33]Ibidem, p. 496.
[34]Ibidem, p. 496.
[35]Ibidem, p. 496.
[36]Ibidem, p. 497.
[37]Ibidem, p. 497.
[38]Ibidem, p. 497.

time of committing the crime reached the age of 16; 2) the legal person carrying out entrepreneurial activity".[39]This special quality of the legal person - subject of the crime is determined by the provision of para. (4) art. 21 CrC RM: "The legal person carrying out entrepreneurial activity is criminally liable for the crimes committed, provided for in art. 140^1, 165, 185^1-185^3, 205, 206, 208^1, 215-217^3, 218, 221, 223-246^1, 248-251, 254, 257, 259-261, 362^1". This provision had such a content until the entry into force of Law no. 277 of 18.12.2008 for the amendment and completion of the Criminal Code of the Republic of Moldova.[40]With the entry into force of this law, the provision from para. (4) art. 21 CrC RMacquired another content: "Legal persons, with the exception of public authorities, are criminally liable for crimes for the commission of which a sanction is provided for legal persons in the special part of this code." Only from this moment can we talk about the legal person (with the exception of the public authority) as the subject of crimes of illegal access to computerized information.

V. State concludes the analysis of the crimes provided for in art. 259 CrC RM with the examination of the aggravated version provided for in para. (2) of this article, which involves committing these crimes: a) repeatedly; b) by two or more people; c) with the violation of the protection system; d) with connection to telecommunications channels; e) with the use of special technical means.

In 2010, the work was published, the co-authors of which are L. *Gîrla and Iu.Tabarcea.*[41]

The generic legal object of the crimes of illegal access to computer information is described as follows by the co-authors in question: "social relations that ensure the security of the production, preservation, use, distribution or protection of computer information, computer systems, information resources and telecommunications services".[42]Characterizing the special legal object of the respective crimes, L. Gîrla and Iu. Tabarcea points out that it forms: "the social relations that ensure the legal order of access to computerized information. The secondary legal object is public relations that ensure the legality of access to computer systems".[43]The originality of this point of view is confirmed by the examination of the secondary legal object of the crimes provided for in art. 259 CrC RM.

In the context of examining the object of these crimes, the two co-authors also state: "The material object of the crime provided for in art. 259 CrC RMrepresents: computerized information; the computer; computer system, computer network. [...] The victim of this crime can be the owner or possessor of information resources or computer systems, technologies or the means of ensuring them, i.e. the natural person, the legal person or the state that fully or partially exercises the right to own, to use or dispose of informational resources or IT systems, technologies or the means of securing them. Also, the victim of the crime can be the user of the computerized information".[44]

The structure and content of the objective side of crimes of illegal access to computerized information are described by L. Gîrla and Iu. Tabarcea in a manner that does not differ from that presented by V. Stati in the work mentioned above, of which he is the co-author. In the same vein, the reflections of L. Gîrla and Iu. Tabarcea regarding the illegality of access within the meaning of art. 259 CrC RM. The same co-authors define the terms "destruction of computer information",

[39]Ibidem, p. 497.
[40] Legea pentru modificarea și completarea Codului penal al Republicii Moldova: nr. 277 din 18.12.2008. În: *Monitorul Oficial al Republicii Moldova*, 2009, nr. 41-44, 120.
[41] ГЫРЛА, Л.Г., ТАБАРЧА, Ю.М. *Уголовное право Республики Молдова. Часть Особенная. Том 2*. Кишинэу: Cartdidact, 2010. 592 с. ISBN 978-9975-4158-2-8.
[42]Ibidem, p. 8.
[43]Ibidem, p. 13.
[44]Ibidem, p. 14, 15.

"damage to computer information", "modification of computer information", "blocking of computer information", "copying of computer information" and "disruption of the functioning of computers, computer system or computer network", which are used in art. 259 CrC RM. L. Gîrla and Iu. Tabarcea considers the offenses provided for in this article to be material, thus describing the moment of their consummation: "the moment of destruction, damage, modification, blocking or copying of computerized information, of disrupting the functioning of computers, the system or the computer network".[45]

Regarding the subjective side of the crimes analyzed, the two co-authors express the point of view that is the majority in the local criminal doctrine: direct or indirect intention; the reason embodied in: material interest; personal interest; unfair competition, etc. Characterizing the subject of the crimes provided for in art. 259 CrC RM, L. Gîrla and Iu. Tabarcea describes not only the general conditions that he must fulfill, but also his special quality: "the person who does not have the right of access to computerized information, to the computer system or to the computer network, established by law or by contract; the person who exceeds the limits of the permission to access them; the person who has not obtained the permission of a person who is authorized to use, administer or control the computer system, conduct scientific research or perform other types of operations in the computer system".[46]The analysis, carried out by L. Gîrla and Iu. Tabarcea, concludes with the detailed examination of the aggravating circumstances recorded in para. (2) art. 259 CrC RM.

In 2011, the work of *S. Brînza and V. Stati*was published.[47]

Taking into account the completion of the Criminal Code with art. 260^1-260^6, operated by Law no. 278/2008 and conditioned by the international commitments of the Republic of Moldova, these authors mention: "Taking into account the provisions of the Council of Europe Convention on computer crime, we can distinguish the following three types of crimes examined: 1) crimes against the confidentiality and integrity of data and computer systems (provided in art. 259, 260, 260^1-260^4, 261 CrC RM); 2) IT crimes in the strict sense (provided in art. 260^5 and 260^6 CrC RM); 3) crimes in the field of telecommunications (provided in art. 261^1CrC RM)".[48]

It shows interest and the relationship between the crimes provided for in art. 259 CrC RM, on the one hand, and the crimes specified in art. 178, 260^1-260^3 CrC RM, on the other hand, examined by S. Brînza and V. Stati. The authors in question conclude that the crimes provided for in art. 259 CrC RMare material crimes, since they are considered consumed "from the moment of the production of damages in large proportions".[49]

In the context of the analysis of the subject of crimes of illegal access to computerized information, S. Brînza and V. Stati state that "only the person who is not authorized under the law or a contract, who exceeds the limits of the authorization or does not have the permission of the competent person to use, to administer or control a computer system or carry out scientific research or perform any other operation in a computer system, may be the subject of the offense specified in art. 259 CrC RM".[50]

In relation to the aggravation specified in letter g) para. (2) art. 259 CrC RM, the same authors claim: "It is considered that not any computerized information is accessed, but a computerized

[45]Ibidem, p. 19.
[46]Ibidem, p. 19-20.
[47] BRÎNZA, Serghei, STATI, Vitalie. *Drept penal. Partea specială. Vol. II*. Chișinău: Tipografia Centrală, 2011. 1324 p. ISBN 978-9975-53-028-7.
[48]Ibidem, p. 258.
[49]Ibidem, p. 269.
[50]Ibidem, p. 269.

information protected by law. It is considered: information about mental disorders, about the request for psychiatric assistance and treatment in a psychiatric institution, as well as other information about the person's state of mental health; information about addressing the person in specialized institutions in relation to the realization of his rights to reproduction and the protection of reproductive health or about the measures taken and the state of his reproductive health; [...] etc. If there is illegal access to computerized information protected by law, about the personal life that constitutes the personal or family secret of another person, the contest between the offense provided for in letter g) paragraph (2) art. 259 CrC RM and one of the crimes specified in para. (1) or (1^1) art. 177 CrC RM".[51]

In 2019, the work of *S. Copeţchi* appears.[52]

First of all, attention is drawn to the opinion of this author regarding the tangents of other crimes with the crimes of illegal access to computer information: "In order to be damaged the social relations that are organically derived from the confidentiality, integrity and availability of computer data, it is enough that the perpetrator has accessed illegal such computer data. The realization of some additional actions (secondary with an alternative character) should not count for inclusion according to art. 259 CrC RM, but for the individualization of the punishment or, possibly, for the inclusion of those committed in the pattern of another criminal norm. Precisely for these reasons, we believe that the Moldovan legislator should review his position when constructing the content of the incriminating norm listed in art. 259 CrC RM, by adopting good practices in the matter. In this sense, the legislative models from the criminal legislation of Georgia, Bulgaria and Romania seem to be eloquent, being in perfect harmony with the one derived from the text of the Budapest Convention".[53]

S. Copeţchi has a clear position regarding the structure of the objective side of the examined crimes: "Prejudicial consequence, as well as the causal link between the act and the harmful consequence, are mandatory signs of the composition of the offense specified in art. 259 CrC RM. More precisely, in order to be in the presence of the crime in the form of a consummated fact, it is necessary that the prejudicial action has caused damages in large proportions to the owner or possessor of the computerized information, the computer or the computer system. [...] It should be noted that according to a Draft Law for the amendment and completion of some legislative acts, which has been on the table of the Parliament of the Republic of Moldova since 2016[54], the ferenda law proposal is submitted to exclude the prejudicial consequence in the form of damages in large proportions from the text of paragraph (1) art. 259 CrC RM, following that it appears as an aggravating circumstance under letter h) paragraph (2) art. 259 CrC RM. We support the advanced legislative proposal. It is unclear, however, the reason for the procrastination of the actual transposition of the said legislative initiative".[55]

---

[51]Ibidem, p. 270-271.

[52] COPEŢCHI, Stanislav. Infracţiunile informatice potrivit legii penale moldave: studiu de drept comparat şi propuneri *de lege ferenda*. În: *Realităţi şi perspective ale învăţământului juridic naţional. Culegerea materialelor ştiinţifice elaborate în baza comunicărilor de la Conferinţa ştiinţifică naţională cu participare internaţională, organizată cu ocazia a 60 de ani de la înfiinţarea Facultăţii de Drept (USM, 01-02 octombrie 2019, Chişinău). Vol. II*. Chișinău: CEP USM, 2020, pp. 29-40. ISBN 978-9975-149-88-4.

[53]Ibidem.

[54]*Proiectul legii pentru modificarea şi completarea unor acte legislative (Legea privind Serviciul de Informaţii şi Securitate al RM – art.7; Codul penal – art. 178, 208^1, 259 ş.a.)*. [citat 30.08.2020] Disponibil: www.parlament.md/ProcesulLegislativ/Proiectedeactelegislative/tabid/61/LegislativId/3183/language/ro-RO/Default.aspx+&cd=3&hl=ro&ct=clnk&gl=at

[55]COPEŢCHI, Stanislav. Infracţiunile informatice potrivit legii penale moldave: studiu de drept comparat şi propuneri *de lege ferenda*. În: *Realităţi şi perspective ale învăţământului juridic naţional. Culegerea materialelor ştiinţifice elaborate în baza comunicărilor de la Conferinţa ştiinţifică naţională cu participare internaţională, organizată cu ocazia a 60 de ani de la înfiinţarea Facultăţii de Drept (USM, 01-02 octombrie 2019, Chişinău). Vol. II*. Chișinău: CEP USM, 2020, pp. 29-40. ISBN 978-9975-149-88-4.

We are finalizing the examination of scientific materials on criminal liability for illegal access to computerized information, published in the Republic of Moldova, with the work developed by *L. Dumneanu and D. Gurev*.[56]

The object of this work is the analysis of all crimes in the computer field, including the crimes provided for in art. 259 CrC RM. Apart from the constitutive elements and the aggravating circumstances of these crimes, the authors focus on aspects of interest for the criminal law analysis of crimes in the IT field: defining concepts regarding information technologies; the computer and the calculation system; computer networks and the Internet; information security; the evolution of international and transnational regulations regarding IT crimes; the evolution of national regulations regarding IT crimes; the concept of IT crimes; types of IT crimes; the characteristic features of computer crimes, etc.

In the context of the analysis of the object of the offenses provided for in art. 259 CrC RM, draws attention to the following point of view: "The material (immaterial) object of the offense provided for in para. (1) art. 259 CrC RM can be expressed in several variants, having an alternative character: computerized information; computers; computer system; IT network".[57]This opinion is useful in order to establish in more detail the content of the material or immaterial object of the offenses provided for in art. 259 CrC RM. In the context of examining the problem related to the plurality of victims of the crimes provided in art. 259 CrC RM, L. Dumneanu and D. Gurev state: "The identification of one or more victims (with different qualities) in a single crime is not excluded".[58]We will develop this idea infra to conclude that the crime has only one victim where the same person is both the owner, other possessor or user of the illegally accessed computer information, and the owner or other possessor of the information destroyed, damaged, altered, blocked or copied, or of the computer, computer system or computer network, whose operation has been disrupted. In other cases, the owner, other possessor or user of the illegally accessed computer information may be someone other than the owner or other possessor of the computer, computer system or computer network, whose operation has been disrupted. Only in these latter cases, we can talk about the presence of the main victim and the secondary victim.

In another vein, from the point of view of the social and legal conditioning of the criminalization of illegal access to computerized information, it is justified to make the following statements: 1) the factors that determine the need to attribute criminal wrongdoing to illegal access to computerized information are of a social nature-legal and socio-economic: intensifying the exchange of information between natural persons, legal persons and states; the penetration of information technologies in all areas of human activity; massive use of satellite communications, computers and computer networks, etc.; 2) the need to criminalize illegal access to computerized information was conditioned by the prohibition or restriction of access to such information for certain persons. This prohibition or restriction, defied by the perpetrator, causes him to enter the computer system, in violation of the protection system, to call information that the perpetrator was not authorized to access; 3) not the computerized form of the information, but the prohibited or restricted nature of its access conditions the need to criminalize the facts provided for in art. 259 CrC RM.

From the perspective of systemic coherence between art. 259 CrC RMand the complementary provisions of the national legislation, it is justified to state the following: 1) the provisions of art. 259 CrC RMforms interconnections with the extra-penal regulations regarding access to computerized

[56] DUMNEANU, Ludmila, GUREV, Dorina. *Infracțiuni în domeniul informatic: Note de curs*. Chișinău: CEP USM. 261 p. ISBN 978-9975-158-29-9.
[57]Ibidem, p. 89.
[58]Ibidem, p. 92-93.

information. This is explained by the reference character (blanket) of the provisions of art. 259 CrC RM. This article can only be interpreted and applied if viewed through the lens of extra-criminal regulations on access to computerized information; 2) the extra-criminal legal framework in the IT field is deficient. However, in the respective laws (Law no. 1069/2000, Law no. 467/2003 and Law no. 20/2009) the definitions of some important concepts are missing ("computer network", "protection system", "telecommunications channels", etc.) used in art. 259 CrC RM, which negatively influences the clarity and predictability of this article.

Under the aspect of the comparative law analysis of the regulations regarding illegal access to computerized information, it is justified to make the following statements: 1) as a synthesis of the conceptions regarding the generic legal object of crimes similar in essence to those provided for in art. 259 CrC RM, provided by the criminal laws of the majority of EU member states, Georgia and Ukraine, it can be said that the owner of the social value protected by these laws is different: the owner of the computerized information, regardless of whether he is a natural person or a legal person; the natural person, whose freedom or privacy has been violated; the state, whose security was threatened; 2) in accordance with most of the articles that essentially correspond to art. 259 CrC RM, which are part of the criminal laws of the EU member states, Georgia and Ukraine, only the computer system and/or computer data represent the material or immaterial object of the respective crimes; 3) in the case of most of the analyzed foreign criminal laws, the actions, which in art. 259 CrC RM have the role of main action and adjacent action, they are criminalized as distinct crimes in different paragraphs of the same article, in different articles of the same division of the criminal law or even in different articles of distinct divisions of the criminal law.

In Chapter 2 – *Criminal law analysis of the crimes provided for in art. 259 CrC RM* – the investigations carried out focused on: the object of the crimes provided in art. 259 CrC RM (the legal object, the tangible (intangible) object and their victim); the objective side of the offenses provided for in art. 259 CrC RM(the prejudicial act, the moment of consummation and the prejudicial consequences in their case; attempt and preparation in the case of the offenses provided in art. 259 CrC RM; causal connection in their case); the subjective side of the crimes provided in art. 259 CrC RM (the guilt manifested in their case; the reason, purpose and emotions in the case of the crimes provided in art. 259 CrC RM); the subject of the crimes provided in art. 259 CrC RM(the general conditions that this subject fulfills; the special quality of the subject of the offenses provided in art. 259 CrC RM); the aggravating circumstances of the offenses provided for in art. 259 CrC RM(under the broad law aspect (the commission of these crimes: by two or more persons; with the violation of protection systems; with the connection to telecommunications channels; with the use of special technical means; with the illegal use of the computer, system or network information systems, for the purpose of committing one of the crimes provided for in paragraph (1), in articles 260^{1}-260^{3}, 260^{5} and 260^{6}CrC RM; with regard to information protected by law); under the ferenda law aspect (the opportunity to aggravate the liability in the event of the commission of the crime) either on an IT system that is an integral part of the critical infrastructure, or regarding sensitive information regarding the protection of critical infrastructures)).

These investigations take shape in the application of the materials and methods that are necessary in the context of the criminal law analysis of the crimes provided for in art. 259 CrC RM. Among the objectives of the present research are: the establishment of social values defended against the crimes provided for in art. 259 CrC RM; revealing the characteristics of the material or immaterial object of the crimes provided for in this article; examination of the distinguishing features that characterize the victim of the crimes provided for in art. 259 CrC RM; establishing the structure and content of the prejudicial act provided for by this article; revealing the prejudicial consequences and the causal link

in the case of the crimes provided for in art. 259 CrC RM; discussing the subjective side and the subject of the offenses provided for in this article; analysis of the circumstances that aggravate the liability for the crimes provided for in art. 259 CrC RM; the delimitation of crimes, provided for in art. 259 CrC RM, of other crimes; investigating the vulnerabilities that characterize the practice of applying art. 259 CrC RM, followed by the formulation of solutions; analysis of the shortcomings of a technical-legislative nature from which the provision of art. 259 CrC RM, followed by the formulation of legal ferenda recommendations. The achievement of these objectives is the condition for the overall achievement of the purpose of this thesis.

Thus, for example, considering the title of Chapter XI of the special part of the Criminal Code of the Republic of Moldova, S. Brînza, V. Stati[59] and A.T. Drăgan[60] believes that the generic legal object of the crimes provided for in this chapter is represented by social relations in the field of IT and telecommunications. We note that informatics and telecommunications represent the pair of fundamental social values, which are protected against the crimes provided for in Chapter XI of the special part of the Criminal Code of the Republic of Moldova.

Under to the *de lege ferenda* perspective, it is justified to state that the phrase "crimes in the field of information technologies", as well as the phrase "cybercrimes", are not suitable to designate the group of crimes provided for in Chapter XI of the special part of the Criminal Code of the Republic of Moldova. The title of Chapter XI of the special part of the Criminal Code demonstrates the lack of congruence between the provisions of the domestic criminal law and the provisions of the Budapest Convention.

The offenses provided for in art. 259 CrC RM, they are biobiectual crimes, but they are not complex crimes. The main legal object of the offenses provided in art. 259 CrC RMforms the social relations regarding authorized or permitted access to computerized information. This object is the same for both crimes specified in art. 259 CrC RM. The adjacent action, described in art. 259 CrC RM, affects the secondary legal object of the crimes provided for in this article. Concretely, we are of the opinion that: the destruction or damage of computerized information affects its integrity; modifying the computerized information affects its authenticity; blocking computerized information affects its availability; copying the computerized information affects its irreproducibility; disrupting the operation of computers, the system or the computer network affects their functionality.

The offenses provided for in art. 259 CrC RM, have an immaterial main object that consists of illegally accessed computer information. At the same time, destroyed, damaged, modified, blocked or copied computer information forms the secondary immaterial object of these crimes. The computers, the computer system or the computer network, whose operation has been disrupted, form the secondary material object of the crimes provided in art. 259 CrC RM.

To the extent that they ensure through the execution of a program the automatic processing of computer data, smart TVs, Playstation consoles, Xbox, smart mobile phones, printers, faxes, scanners or other such devices are computer systems. Because it ensures the automatic processing of computer data by executing a program, the ATM and the POS type terminal represent computer

[59] BRÎNZA, Serghei et al. *Drept penal. Partea specială*. Chișinău: Cartier, 2005, p. 493. 804 p. ISBN 9975-79-324-X; STATI, Vitalie. Răspunderea penală pentru infracţiunile în domeniul informaticii şi telecomunicaţiilor. În: Analele Ştiinţifice ale Universităţii de Stat din Moldova. Seria „Ştiinţe socioumanistice". Vol. 1. Chişinău: CEP USM, 2005, pp. 387-394. ISSN 1811-2668; BRÎNZA, Serghei, STATI, Vitalie. *Drept penal. Partea specială. Vol. II*. Chișinău: Tipografia Centrală, 2011, p. 254. 1324 p. ISBN 978-9975-53-028-7; BRÎNZA, Serghei, STATI, Vitalie. *Tratat de drept penal. Partea specială. Vol. II*. Chișinău: Tipografia Centrală, 2015, p. 342. 1300 p. ISBN 978-9975-53-470-3.

[60] DRĂGAN, Alin Teodorus. *Frauda informatică: analiza juridico-penală a infracțiunii*: tz. de doct. în drept. Chișinău, 2017, p. 119. 179 p.

systems; 5) to the extent that it ensures the automatic processing of computer data through the execution of a program, the payment card represents a computer system. Such a hypothesis is attested when the payment card is inserted into the ATM, thus forming a tandem with this computer system.

In art. 259 CrC RM criminalizes not simply illegal access to computerized information, but illegal access to computerized information accompanied by the destruction, damage, modification, blocking or copying of information, by disrupting the functioning of computers, the system or the computer network, if, as a result, large / particularly large amounts of damage occurred.

Regardless of the factual modality under which the access to a computer system appears, we must establish whether this access had a continuity, so that we can talk about the access to the computerized information in that system. Only in such a case can we talk about access to computerized information in the sense of art. 259 CrC RM. Regardless of the factual way in which the access to a computer, to a material support of information or to a computer network appears - we must establish whether this access had a continuity, so that we can talk about the access to the computerized information from that computer, from that material support of information or from that computer network. In the absence of such continuity, we cannot talk about access to computerized information within the meaning of art. 259 CrC RM.

It is not justified to retain the ideal contest between one of the crimes, provided for in art. 259 CrC RM, and one of the crimes provided for in art. 260^2 or 260^3 CrC RM. The same destruction, damage, modification, blocking or copying of information or disruption of the functioning of computers, the system or the computer network must not be qualified on the basis of two articles.

The deletion or elimination of computerized information cannot represent examples arising from the notion of "destruction of computerized information", used in art. 259 CrC RM. The notion of "destruction of computerized information", used in art. 259 CrC RM, can only be represented by the destruction or damage of the computer, the material information support, the computer system or the computer network, which has the effect of destroying the computerized information that was in that computer, on that material information support, in that computer system or in that computer network. Under these conditions, art. 259 CrC RM must be applied together with art. 197 CrC RM or with art. 104 CrC RM. The notion of "damage to computerized information", used in art. 259 CrC RM, can only be represented by the damage to the computer, to the material support of information, to the computer system or to the computer network, which has the effect of damaging the computerized information that was in that computer, on that material support of information, in that system computer or in that computer network. In such circumstances, art. 259 CrC RM must be applied together with art. 197 CrC RM or with art. 104 CrC RM.

In art. 259 CrC RM, by "copying computerized information" we mean the logical copying of computerized information (which involves the use of a computer program), not its physical copying (for example: manual reproduction; reproduction by photographing the text or image on computer screen etc.). Reproduction in the human brain by memorization of information seen, heard or otherwise perceived does not form the content of the notion "copying computer information", used in art. 259 CrC RM. The essential condition for attesting the copying of computerized information, as a normative method of the adjacent action within the prejudicial act provided for in art. 259 CrC RM, is that the copied computerized information is stored in another computer, on another material information medium, in another computer system or in another computer network, than the one on which the computerized information was kept original. It is possible that: a) two or more people have access to the same computer, to the same physical information medium, to the same IT system or to the same IT network; b) at the same time, to restrict access for one or some of these persons to a part of such a computer, material support of information or computer system or such computer network.

In such a situation, to apply art. 259 CrC RM, the copied computerized information must be stored in that part of the computer, of the physical information medium, of the computer system or of the computer network, to which the victim does not have access. The copying of computerized information, if it does not cause damage in large or particularly large proportions and if it is not preceded by illegal access to that information, can represent the preparation of the crimes that involve the disclosure of certain information (for example, the preparation of the crimes provided in art. 204, para. (1) art. 315, art. 316, 337, 344 etc. CrC RM). In such cases, it is not necessary to apply art. 259 CrC RM.

It is not appropriate as in art. 259 CrC RM, there should be a special provision in which the liability for the attempted crimes provided for in this article would be established. Unlike the attempt to commit a crime, the preparation of a crime does not require the start of the execution of the prejudicial act. In the case of the crimes provided in art. 259 CrC RM, this means that, for reasons independent of the will of the perpetrator, the execution of the main action of illegal access to computerized information does not begin.

Prejudicial consequences, provided for in art. 259 CrC RM, must be causally related to the adjacent action of destruction, damage or modification of information, or of disruption of the functioning of computers, the system or the computer network, not to the main action of illegal access to computerized information. The main action of illegal access to computerized information cannot, by itself, represent the cause of the harmful consequences provided for in art. 259 CrC RM.

The quasi-unanimous position in the specialized literature is that the offenses provided for in art. 259 CrC RM, can be committed with direct intent or with indirect intent.[61]We support this position.

The special quality of the subject of the crimes, provided for in art. 259 CrC RM, can be easily established by reference to the phrase "of a person who is not authorized under the law or a contract, exceeds the limits of authorization or does not have the permission of the competent person to use, administer or control an IT system or to carry out scientific research or to perform any other operation in a computer system", which is used in art. 259 CrC RM. It follows that the person who accesses the computerized information is not liable under art. 259 CrC RM in any of the following cases: a) it is authorized under the law or a contract; b) does not exceed the authorization limits; c) has the permission, from the competent natural or legal person, according to the law, to grant it, to use, administer or control an IT system or to carry out scientific research or to perform any other operation in an IT system.

Art. 259 CrC RMprovides for liability for two crimes which are provided for in para. (1) and lit. h) paragraph (2) art. 259 CrC RM. At lit. b)-g) and g^1) para. (2) art. 259 CrC RM, the aggravating circumstances of the crimes brought together under the marginal name of illegal access to computerized information are specified.

---

[61] BRÎNZA, Serghei, STATI, Vitalie. *Tratat de drept penal. Partea specială. Vol. II*. Chișinău: Tipografia Centrală, 2015, p. 355. 1300 p. ISBN 978-9975-53-470-3; BARBĂNEAGRĂ, Alexei et al. *Codul penal al Republicii Moldova. Comentariu (Adnotat cu jurisprudenţa CEDO şi a instanţelor naţionale)*. Chişinău: Sarmis, 2009, p. 568. 860 p. ISBN 978-9975-105-20-0;BARBĂNEAGRĂ, Alexei et al. *Codul penal al Republicii Moldova. Comentariu* / Sub red. lui Alexei BARBĂNEAGRĂ. Chişinău: Arc, 2003, p. 570. 836 p. ISBN 9975-61-291-1; BORODAC, Alexandru. *Manual de drept penal. Partea specială*. Chişinău: Tipografia Centrală, 2004, p. 366. 622 p. ISBN 9975-9788-7-8; ГЫРЛА, Л.Г., ТАБАРЧА, Ю.М. *Уголовное право Республики Молдова. Часть Особенная. Том 2*. Кишинэу: Cartdidact, 2010, с. 19. 592 с. ISBN 978-9975-4158-2-8; ЛАЗАРЕВА, Наталья. Уголовно-правовая характеристика преступлений в области информатики и электросвязи. În: *Revista ştiinţifică a USM „Studia Universitatis". Seria „Ştiinţe sociale"*, 2007, nr. 6, pp. 133-141. ISSN 1857-2081; SOLTAN, Veaceslav. Infracțiunile informatice (art. 259-261^1 Cod penal). În: *Procuratura Republicii Moldova. Buletin informativ*, 2010, nr. 15, pp. 38-43. [citat 11.07.2022] Disponibil: http://procuratura.md/file/BULETIN%20VIRTUAL%2015.pdf

Chapter 3 – *The results obtained from the criminal law analysis of the crimes provided for in art. 259* CrC RM– is focused on the personal contributions of the author, including the original results obtained by the author.

The results, obtained following the criminal law analysis of the offenses provided in art. 259 CrC RM, are grouped as follows: the results obtained from the criminal law analysis of the object of these crimes; the results obtained following the criminal law analysis of the objective side of the offenses provided in art. 259 CrC RM; the results obtained from the criminal law analysis of the subjective side of these crimes; the results obtained following the criminal law analysis of the subject of the offenses provided in art. 259 CrC RM; the results obtained following the criminal law analysis of the aggravating circumstances of these crimes.

The investigations, carried out in Chapter 3, represent the effect and balance of the application in Chapter 2 of the thesis of the materials and methods that are necessary in the context of the criminal law analysis of the crimes provided for in art. 259 CrC RM. Naturally, these investigations follow the same research objectives, which are expected to be carried out in Chapter 2 of the thesis. The achievement of such objectives is the condition for the overall achievement of the purpose of this thesis.

Thus, for example, in the context of the analysis of the legal object of the crimes provided for in art. 259 CrC RM, we have the basis to state: 1) social relations regarding the security of computer data and electronic communications present sufficient significance from an axiological point of view, so that they are subject to criminal defense; 2) it is not admissible to confuse the notions of "information security" and "computer (cyber) security".

In the context of examining the material (immaterial) object of the crimes provided for in art. 259 CrC RM, it is justified to make the following statements: 1) in the sense of art. 259 CrC RM, computerized information is information intended for processing on a computer, fixed on a medium that can be read by a computer or transmitted in an environment that makes it possible to interact within a computer system or a computer network; 2) computer data must be regarded as information represented in a form suitable for carrying out operations through computer means with the possible involvement of a person; 3) computer programs, computer data, procedures, processes of use, personnel and users cannot represent parts of a computer system; 4) not any entity, which can be used as a support (means) for storing computer data, can cumulate the function of ensuring by executing a program the automatic processing of computer data. Only in the case of the cumulation of the two functions, the respective entity constitutes an IT system; 5) the computer system represents the interconnected data processing node for the purpose of data transport, while the set of such nodes constitutes the computer network; 6) the notion of information system should not be confused with the notion of computer system within the meaning of art. 259 CrC RM. The relationship between the notions of "computer system" and "information system" is a "part-whole" relationship.

In the context of the analysis of the objective side of the offenses provided for in art. 259 CrC RM, we have the basis to state: 1) by "access to computerized information" within the meaning of art. 259 CrC RM must be understood: obtaining the possibility to resort to computerized information, in order to benefit from its useful qualities; 2) in the case of crimes provided in art. 259 CrC RM, access to computerized information implies a logical, not physical, interaction with such information. Logical interaction with computerized information is expressed in the fact that the perpetrator uses a computer program or several computer programs that ensure the processing of that information; 3) the act of illegal intrusion into the computer, into the material support of information, into the computer system or into the computer network, in which or on which the said information is located,

must be seen as a pre-condition, not as a stage in the process of committing illegal access to computerized information. Therefore, the illegal intrusion into the computer, into the material support of information, into the computer system or into the computer network, in which or on which the computerized information is located, must be qualified as preparation, not as an attempt, if, for reasons independent of the perpetrator's will, there is no illegal access to that information; 4) the use and/or disposal of the computerized information is the purpose of the action to access the computerized information, a purpose that goes beyond the scope of this action; 5) the crime, provided in art. 260^{1}CrC RM, can be conceived only in the case of a transmission of computer data (including an electronic emission). In the case of the crimes provided in art. 259 CrC RM, computerized information from computers, from material information carriers, from the computer system or network, is illegally accessed, not computerized information transmitted between computers, between material information carriers, between computer systems or between computer networks; 6) access to computerized information is illegal, if it is carried out: a) without authorization under the law or a contract; b) exceeding the authorization limits; c) without the permission of the competent person to use, administer or control an IT system or to conduct scientific research or perform any other operation in an IT system, etc.

In the context of examining the subjective constitutive elements of the crimes provided for in art. 259 CrC RM, it is justified to make the following statements: 1) the crimes, provided for in art. 259 CrC RM, are committed with direct or indirect intent; 2) only art. 260^{6}CrC RM if the illegal access to computerized information is followed by the introduction, modification or deletion of computer data, the restriction of access to this data or the prevention in any way of the operation of a computer system, in order to obtain a material benefit for oneself or for another, if these actions caused large or particularly large damages; 3) in accordance with letter d) paragraph (1) art. 76 CrC RM, the commission of the act by a person with reduced responsibility is considered a mitigating circumstance that is taken into account when determining the penalty. Precisely in this position, the state of affect can be taken into account when individualizing the punishment that is applied for the offenses provided in art. 259 CrC RM; 4) subjects of the crimes, provided in art. 259 CrC RM, can be the persons who have the right of access to a computer, to a material support of information, to a computer system or to a computer network. Such persons must not have the right of access to the computerized information from the computer, from the material support of information, from the computer system or from the computer network to which they have legal access; 5) subjects of the crimes, provided in art. 259 CrC RM, may also be the persons who do not have a right of access to a computer, to a material support of information, to a computer system or to a computer network. Of course, such persons also have no right of access to the computerized information; 6) the crimes provided in art. 259 CrC RM have not only a special subject. They have a special composition.

Finally, in the context of the analysis of the aggravating circumstances of the crimes provided for in art. 259 CrC RM, we have the basis to state: 1) in the case of the commission of one of the crimes provided for in this article by an organized criminal group or by a criminal organization, letter b) para. (2) art. 259 CrC RM; 2) through protection systems, within the meaning of letter c) para. (2) art. 259 CrC RM, means the procedures, devices or specialized computer programs with the help of which access to computerized information is restricted or prohibited for certain categories of users; 3) in the sense of lit. c) para. (2) art. 259 CrC RM, by “protection” we mean the protection against illegal access to computerized information, not the protection against illegal access to: a) the computer, material information carrier, computer system or network, which contain computerized information that can be accessed illegally; b) the room, other place for storage or the home where the computer, material information support, system or computer network, which contain the

computerized information that can be accessed illegally, is located; 4) the provision from letter d) para. (2) art. 259 CrC RM is applicable, if the notion of "computer network" intersects with the notion of "electronic communications network". On the contrary, if the notion of "computer network" does not intersect with the notion of "electronic communications network", then art. 259 CrC RM (except letter d) para. (2)), etc.

CONCLUSIONS AND RECOMMENDATIONS

The results, which we obtained in the present thesis, consist of the following: 1) the doctrinal views regarding the liability for the crimes provided for in art. 259 CrC RM; 2) the potential provided by the national regulations regarding access to computerized information was used in the process of interpreting this article; 3) the degree of compatibility between art. 259 CrC RMand the regulations of international origin regarding the prohibition of illegal access to computerized information; 4) the positive experience of other states was studied in terms of preventing and combating illegal access to computerized information through criminal means; 5) the social values defended against the crimes provided for in art. 259 CrC RM; 6) the characteristics of the material or immaterial object of the crimes provided for by this article have been revealed; 7) the distinguishing features that characterize the victim of the crimes provided for in art. 259 CrC RM; 8) the structure and content of the prejudicial act provided for by this article have been established; 9) the prejudicial consequences and the causal link were revealed in the case of the crimes provided for in art. 259 CrC RM; 10) the subjective side and the subject of the crimes provided for by this article were discussed; 11) the circumstances that aggravate the liability for the offenses provided for in art. 259 CrC RM; 12) the delimitation of the offenses provided for in art. 259 CrC RM, of other crimes; 13) the vulnerabilities that characterize the practice of applying art. 259 CrC RM, following the formulation of solutions; 14) the shortcomings of a technical-legislative nature suffered from the provision of art. 259 CrC RM, following the formulation f of proposals for *lege ferenda*.

The important scientific problem, solved after obtaining the described results, is expressed in the substantiation of the concept of interpretation of art. 259 CrC RMand the qualification of crimes based on this article without violating the principle of legality, this substantiation having the effect of identifying errors in the application of art. 259 CrC RMand the defects that characterize the provision of this article, thus creating the theoretical basis necessary to perfect the practice of applying art. 259 CrC RMand to improve the quality of this article.

I. Conclusions:

The important scientific problem was demonstrated by the ***conclusions*** developed based on the research hypothesis, as follows:

1.By criminalizing the acts brought together under the marginal name of illegal access to computerized information, the legislator seeks to establish a reasonable balance between the right of some people to freely access computerized information and the right of other people not to allow illegal access to such information. The right to information is a right provided by art. 34 of the Constitution. The right to freely access computer information is only one version of this constitutional right. From para. (2) art. 54 of the Constitution shows that the right to information can be restricted. It is important that this restriction: a) be provided by law; b) to correspond to the unanimously recognized norms of international law; c) to be necessary in the interests of national security, territorial integrity, economic well-being of the country, public order, for the purpose of preventing mass disturbances and crimes, protecting the rights, freedoms and dignity of other

persons, preventing the disclosure of confidential information or guaranteeing the authority and impartiality of justice. The restriction of the right to freely access computerized information, provided by art. 259 CrC RM, fulfills these three conditions. This restriction is based on the law and aims to protect the legitimate interest of a person, society or the state. This results from the description of the subject of the crime, which is made in para. (1) art. 259 CrC RM: "a person who is not authorized under the law or a contract, exceeds the limits of the authorization or does not have the permission of the competent person to use, administer or control an IT system or carry out scientific research or perform any other operation in – an IT system" (see: *Chapter 3, Subchapter 3.1*).

2. The offenses provided in art. 259 CrC RM, they are biobiectual crimes, but they are not complex crimes. The offenses provided for in art. 259 CrC RM, are biobiectual. The structure of the prejudicial act provided by this article tells us about this. Thus, the prejudicial act analyzed includes two components: a) the main action of illegal access to computerized information; b) the adjacent action of destruction, damage, modification, blocking or copying of information or of disrupting the functioning of computers, the system or the computer network. The main legal object of the offenses provided for in art. 259 CrC RMforms the social relations regarding authorized or permitted access to computerized information. This object is the same for both crimes specified in art. 259 CrC RM. The secondary legal object of the offenses provided for in art. 259 CrC RMconstitutes the social relations regarding the integrity, authenticity, availability or irreproducibility of computerized information or the functionality of computers, the system or the computer network, protected against the causing of: a) damages in large proportions (in the case of the offense provided for in paragraph (1)); b) damages in particularly large proportions (in the case of the offense provided for in letter h) para. (2)). In the case of the crimes provided for in art. 259 CrC RM, neither the main action nor the adjacent action represent crimes of their own kind. In the special part of the Criminal Code of the Republic of Moldova, there are no rules in which either the illegal access to computerized information, or the destruction, damage, modification, blocking or copying of information or the disruption of the functioning of computers, the system or the computer network, would be criminalized separately. So, the offenses provided for in art. 259 CrC RM, they are biobiectual crimes, but they are not complex crimes. (see: *Chapter 2, Subchapter 2.1; Chapter 3, Subchapter 3.1*).

3. In the case of the crimes provided in art. 259 CrC RM, the main immaterial object is computerized information. In the case of the same crimes, the computer information destroyed, damaged, modified, blocked or copied constitutes the secondary intangible object; the computers, the computer system or the computer network, whose operation has been disrupted, form the secondary material object. The phrase "illegal access to computerized information" from the provision of art. 259 CrC RM indicates a violation of the established order of access to information from computers, from material information supports, from the computer system or from the computer network. Such a violation makes it difficult or even impossible to carry out social relations between the subjects who use, administer or control an IT system, who carry out scientific research or who perform any other operation in an IT system. Considering this aspect, it would appear that the crimes, provided for in art. 259 CrC RM, have an immaterial object (which consists of computerized information), not a material object. However, we cannot ignore another phrase from the provision of art. 259 CrC RM –"if it is accompanied by the destruction, damage, modification, blocking or copying of information, by the disruption of the functioning of computers, the system or the computer network". This phrase refers to the adjacent action and is relevant (like the phrase "illegal access to computerized information") in order to establish the entities through

which the special legal object of the crimes provided for in art. 259 CrC RM. From the phrase "if it is accompanied by the destruction, damage, modification, blocking or copying of information, by disrupting the functioning of computers, the system or the computer network" it follows that – apart from the illegally accessed computer information (which is the main immaterial object of the examined crimes) – the entities, through which the special legal object of the crimes provided for in art. 259 CrC RM, are represented by: a) destroyed, damaged, modified, blocked or copied computerized information (which forms the secondary immaterial object of the offenses provided for in art. 259 CrC RM); b) the computers, the computer system or the computer network, whose operation has been deregulated (which forms the secondary material object of these crimes) (see: *Chapter 3, Subchapter 3.1*).

4.The position in relation to the structure of the objective side of the crimes, provided for in art. 259 CrC RM, must be differentiated according to the normative modalities of the adjacent action within the prejudicial act. Taking into account the specifics of the offenses provided in art. 259 CrC RM, we appreciate that, only in cases of destruction, damage or modification of information, or disruption of the functioning of computers, the system or the computer network, verbum regens covers both the prejudicial act and the prejudicial consequences. Or, in the presence of these four normative modalities, certain metamorphoses occur at the level of the material or immaterial object of the offenses provided in art. 259 CrC RM. That is why, in these four cases, the result, necessary for the consummation of the crime, consists, first of all, in the destruction, damage or modification of the information, or in the disruption of the functioning of the computers, the system or the computer network. Secondly, such a result is expressed in damages in large proportions. At a glance in corpore, in the analyzed cases, the prejudicial consequences consist in the destruction, damage or modification of information, or the disruption of the functioning of computers, the system or the computer network, which takes the form of damages in large proportions. As a consequence, the objective side of the crimes provided for in art. 259 CrC RM has, in its first version, the following structure: a) the prejudicial act which consists of the main action of illegal access to computerized information, followed by the adjacent action of destroying, damaging or modifying the information, or of disrupting the functioning of computers, of the computer system or network; b) the harmful consequences, namely – the destruction, damage or modification of information, or the disruption of the functioning of computers, the system or the computer network, which take the form of damages in large proportions (in the case of the offense provided for in paragraph (1)) or damages in particularly large proportions (in the case of the offense provided for in letter h) para. (2)); c) the causal link between the prejudicial act and the prejudicial consequences. In another version, the objective side of the crimes provided for in art. 259 CrC RM has the following structure: a) the prejudicial act which consists of the main action of illegal access to computerized information, followed by the adjacent action of blocking or copying the information; b) prejudicial consequences, namely – damages in large proportions (in the case of the offense provided for in paragraph (1)) or damages in particularly large proportions (in the case of the offense provided for in letter h) para. (2)); c) the causal link between the prejudicial act and the prejudicial consequences (see: *Chapter 3, Subchapter 3.2*).

5. Due to the unsuccessful structure of the objective side of the offenses provided in art. 259 CrC RM, there is no possibility of effective criminal defense of social relations regarding authorized or permitted access to computerized information. In art. 259 CrC RM criminalizes not simply illegal access to computerized information, but illegal access to computerized information accompanied by the destruction, damage, modification, blocking or copying of information, by disrupting the functioning of computers, the system or the computer network, if, as a result , large /

particularly large amounts of damage occurred. Only in some cases, illegal access to computerized information per se can form the content of criminal or contraventional acts (for example, of the acts provided in art. 327, 335 or 370 CrC RM or in art. 312 CrC RM). In the other cases, if the perpetrator's intention is limited to making illegal access to computerized information, and this intention is realized, then there is no basis for applying art. 259 CrC RM. In this case, the objective side of the crime is missing in its entirety, which is why we talk about the lack of the crime component. The need to review the current structure of the objective side of crimes, provided for in art. 259 CrC RM, is determined not only by this state of affairs. Another argument consists in the presence of art. 260^2 and 260^3CrC RM, which makes unnecessary the presence in art. 259 CrC RM of the phrase that refers to the adjacent action within the prejudicial act provided for in art. 259 CrC RM: "if it is accompanied by the destruction, damage, modification, blocking or copying of information, by the disruption of the functioning of computers, the system or the computer network". (see: *Chapter 2, Subchapter 2.2; Chapter 3, Subchapter 3.2*).

6. It is opportune to increase liability in the case of committing crimes, provided for in art. 259 CrC RM, either on an IT system that is an integral part of the critical infrastructure, or regarding sensitive information regarding the protection of critical infrastructures. Analysis of art. 259 CrC RM demonstrates that this article is not adjusted to current social requirements, as social relations that appear and develop in connection with: a) computer systems that are integral parts of the critical infrastructure lack criminal defense; b) sensitive IT data regarding the protection of critical infrastructures. The urgent need for such a supplement is dictated by the war of aggression waged by the Russian Federation against Ukraine (which has collateral effects on the Republic of Moldova), as well as by the hybrid war waged by the Russian Federation, among others, against the Republic of Moldova. Also, the need to fill that gap is suggested in Council Decision (CFSP) 2019/797 of 17.05.2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States. All this confirms that it is opportune to complete Chapter XIII of the general part of the Criminal Code of the Republic of Moldova with two articles in which the notions of "critical infrastructure" and "sensitive IT data regarding the protection of critical infrastructures" would be defined. These definitions will be modeled on the definitions of the same notions in Directive 2008/114/EC, of course, with the appropriate adjustments. Apart from this, it is appropriate to increase the liability for the crimes provided for in art. 259 CrC RM, if they are committed either on an IT system that is an integral part of the critical infrastructure, or on sensitive IT data regarding the protection of critical infrastructures (see: *Chapter 2, Subchapter 2.5; Chapter 3, Subchapter 3.5*).

Description of personal contributions emphasizing its theoretical significance and practical value. The personal contributions consist in the thorough and complex investigation of the constitutive elements and the aggravating circumstances of the crimes provided for in art. 259 CrC RM. Representing the basic / aggravated component of the respective crimes, these constitutive elements and aggravating circumstances constitute the legal basis of criminal liability based on art. 259 CrC RM.

Personal contributions may include: demonstrating the need to distinguish the notion of "information security" from the notion of "information (cyber) security", the notion of "information system" from the notion of "information system", the notion of "information system" from the notion of "information network", etc.; proposing definitions for each of the notions that refer to the material (immaterial) object of the offenses provided for in art. 259 CrC RM, taking into account the reference extra-criminal norms; arguing the need to distinguish two alternative versions of the objective side of the crimes provided for in art. 259 CrC RM, depending on the specifics of the normative modalities of the adjacent action; establishing the correlation between the crimes, provided

in art. 259 CrC RM, and other offenses provided for in Chapter XI of the special part of the Criminal Code of the Republic of Moldova; detailed characterization of the aggravating circumstances of the crimes provided for in art. 259 CrC RM, taking into account the reference extra-criminal norms, etc.

Regarding the previous doctrinal heritage, we find that there are not too many scientific studies dedicated to the criminal law analysis of the crimes provided in art. 259 CrC RM. The investigation by local criminal investigators of the constitutive elements and the aggravating circumstances of these crimes is characterized by insufficiency or by certain contradictions (namely, the aspects related to: the content of the generic legal object of the crimes provided for in art. 259 CrC RM; the structure of the special legal object of these crimes; the meaning of the notions "computerized information", "computer system", "computer network" and "computer"; the structure of the objective side of the crimes provided for in art. 259 CrC RM, etc.).

The legal and empirical basis of this study is: a) the provisions of art. 259 CrC RM; b) other rules from Chapter XI of the special part of the Criminal Code of the Republic of Moldova; c) certain rules from the general part and from the special part of the Criminal Code of the Republic of Moldova, necessary either for the systemic interpretation of art. 259 CrC RM, or the examination of the crimes provided for in this article through the lens of participation, the stages of the criminal activity or other such institutions; d) the provisions of the extra-criminal legislation that comply with art. 259 CrC RM and thus contributes to its interpretation; e) the practice of applying art. 259 CrC RM; f) the rules of the criminal laws of other states, which correspond to art. 259 CrC RM; g) the norms that constitute historical precedents in relation to art. 259 CrC RM. *The scientific basis* of the present study is represented by the works of local doctrinaires, as well as those of foreign doctrinaires.

The theoretical significance of the thesis resides in: a) resizing the criminal defense of social relations regarding authorized or permitted access to computerized information; b) the accumulation of ample theoretical and practical material indispensable for the development of current and complex directions of the investigation of crimes provided for in art. 259 CrC RM; c) detailed characterization of the constitutive elements and aggravating circumstances of the crimes provided for in art. 259 CrC RM; d) identifying the shortcomings that characterize the provision of art. 259 CrC RM and the practice of applying this provision.

The practical value of the thesis consists in the following: a) the interpretation from new perspectives of the provisions of art. 259 CrC RM contributes to the development of the scientific discussion regarding the establishment of the legal basis of criminal liability for the acts incriminated in this article; b) the analysis of comparative law and the historical analysis of the regulations regarding liability for illegal access to computerized information have a cognitive significance in order to perceive the legal and social essence of the crimes provided for in art. 259 CrC RM; c) interpretation of concepts, used in art. 259 CrC RM, is useful in terms of interpreting this article in accordance with the principle of legality and ensuring a uniform practice of applying art. 259 CrC RM, thus reducing the possibility of extensive unfavorable interpretation and application by analogy of art. 259 CrC RM; d) establishing defects, which characterizes the provision of art. 259 CrC RM, can be capitalized in the process of perfecting this provision, in order to increase the clarity and predictability of art. 259 CrC RM, in order to harmonize the provisions of this article with the provisions of the Budapest Convention and to adjust the provisions of art. 259 CrC RM to current social requirements.

Data on approval of results. The main conclusions of the thesis can be found in 19 scientific publications. The results, obtained in this study, were presented and approved at several national and international scientific forums, which took place in the period 2020-2022.

Indication of the limits of the obtained results, with the determination of the remaining unresolved issues. The limits of the obtained results are conditioned by: a) carrying out an analysis with predilection for criminal law of the offenses provided for in art. 259 CrC RM; b) the empirical analysis of the domestic judicial practice and that of Romania; c) systemic analysis of crimes, provided for in art. 259 CrC RM, taking into account the supplementary regulations from the reference extra-criminal legislation. Since all the objectives of the thesis have been achieved, we cannot talk about problems left unsolved. Instead, future research directions related to the addressed topic can be drawn, which will be penciled *infra*.

II. Recommendations:

1) completion of art. 6 CrC RM with paragraph (3) which would have the following provision: *"The act committed by imprudence constitutes a crime only when it is expressly provided for by the norm of the special part of this code"*;

2)exclusion of references to intention from all the rules of the special part of the Criminal Code of the Republic of Moldova, in which this form of guilt is mentioned;

3)completing Chapter XIII of the general part of the Criminal Code of the Republic of Moldova with the following articles:

"Article 134[25]. Computer data

Computer data means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program capable of determining the execution of a function by a computer system";

"Article 134[26]. Computer system

Computer system means the system defined as such in Law no. 20/2009 regarding the prevention and combating of computer crime";

"Article 134[27]. Security measures

Through security measures, in the sense of art. 259, it is understood the use of procedures, devices or specialized computer programs with the help of which access to computerized information is restricted or prohibited for certain categories of users";

"Article 134[28]. The person who illegally accesses computer data

The person who is in one of the following situations illegally accesses computer data:

a) is not authorized, under the law or a contract;

b) exceeds the authorization limits;

c) does not have the permission, from the competent natural or legal person, according to the law, to grant it, to use, administer or control an IT system or to carry out scientific research or to perform any other operation in an IT system";

"Article 134[29]. Critical infrastructure

By critical infrastructure, in the sense of art. 259, means an element, a system or a component thereof, located on the territory of the Republic of Moldova, which is essential for the maintenance of vital societal functions, health, safety, security, social or economic well-being of individuals, and whose disruption or destruction would have a significant impact for the Republic of Moldova as a result of the inability to maintain the respective functions";

"Article 134[30]. Sensitive computer data regarding the protection of critical infrastructures

Through sensitive IT data regarding the protection of critical infrastructures, in the sense of art. 259, it is understood the computer data regarding a critical infrastructure that could be used, in case of disclosure, for the purpose of planning and carrying out actions that cause the disruption or destruction of critical infrastructure installations";

4)changing the title of Chapter XI of the special part of the Criminal Code from "*Computer crimes and crimes in the field of telecommunications*" to "*Crimes against the security of computer data and electronic communications*";

5)modification of the title and provision of art. 259 CrC RM, as follows:

"Article 259. Illegal access to computer data

(1) Illegal access to computer data by violating security measures [...]

(2) The same action performed:

b) by two or more people;

e) with the use of special technical means;

g) regarding computer data protected by law;

g[1]) for reasons of prejudice;

i) on an IT system that is an integral part of the critical infrastructure;

j) regarding sensitive IT data regarding the protection of critical infrastructures[...]";

6)supplementing the Criminal Code of the Republic of Moldova with a new article:

"Article 246[1]. Illegal access to computer data

Illegal access to computer data, if the act does not constitute a crime,

it is sanctioned with a fine from 30 to 60 conventional units applied to the natural person, with a fine from 120 to 180 conventional units applied to the legal person".

Suggestions regarding potential future research directions related to the topic addressed: 1) elaboration of a draft decision of the Plenary of the Supreme Court of Justice regarding the application in practice by the courts of art. 259 CrC RM; 2) in-depth analysis of some institutions of the general part of criminal law (stages of criminal activity, participation, causes that remove the criminal nature of the act, etc.) in the context of the application of art. 259 CrC RM; 3) elucidation of the criminological and criminal procedural connotations of the crimes provided for in art. CrC RM.

Proposals for the use of the results obtained in the socio-cultural and economic fields: in the process of legislative creation (in order to eliminate the shortcomings characterizing the provisions of art. 259 CrC RM, of increasing the degree of clarity and predictability of art. 259 CrC RM, of harmonizing this article with the provisions of the Budapest Convention and of adjusting art. 259 CrC RM to current social demands), in the educational process (in order to increase the level of knowledge and skills of students from law faculties in higher education institutions, of audiences and beneficiaries of continuous training within the National Institute of Justice) and in perspective scientific activity (for the purpose of developing the scientific discussion regarding liability for the crimes provided for in art. 259 CrC RM).

BIBLIOGRAPHY

1. BARBĂNEAGRĂ, Alexei et al. *Codul penal al Republicii Moldova. Comentariu (Adnotat cu jurisprudenţa CEDO şi a instanţelor naţionale)*. Chişinău: Sarmis, 2009. 860 p. ISBN 978-9975-105-20-0.
2. BARBĂNEAGRĂ, Alexei et al. *Codul penal al Republicii Moldova. Comentariu* / Sub red. lui Alexei BARBĂNEAGRĂ. Chişinău: Arc, 2003. 836 p. ISBN 9975-61-291-1.
3. BORODAC, Alexandru. *Manual de drept penal. Partea specială*. Chişinău: Tipografia Centrală, 2004. 622 p. ISBN 9975-9788-7-8.
4. BRÎNZA, Serghei et al. *Drept penal. Partea specială*. Chișinău: Cartier, 2005. 804 p. ISBN 9975-79-324-X.
5. BRÎNZA, Serghei, STATI, Vitalie. *Drept penal. Partea specială. Vol. II*. Chișinău: Tipografia Centrală, 2011. 1324 p. ISBN 978-9975-53-028-7.

6. BRÎNZA, Serghei, STATI, Vitalie. *Tratat de drept penal. Partea specială. Vol. II*. Chișinău: Tipografia Centrală, 2015. 1300 p. ISBN 978-9975-53-470-3.
7. Codul penal al Republicii Moldova: nr. 41 din 24.03.1961. În: *Veştile Sovietului Suprem al R.S.S. Moldoveneşti*, 1961, nr. 10, 41.
8. Codul penal al Republicii Moldova: nr. 985 din 18.04.2002. În: *Monitorul Oficial al Republicii Moldova*, 2002, nr. 128-129, 1012.
9. COPEȚCHI, Stanislav. Infracţiunile informatice potrivit legii penale moldave: studiu de drept comparat şi propuneri *de lege ferenda*. În: *Realități și perspective ale învățământului juridic național. Culegerea materialelor științifice elaborate în baza comunicărilor de la Conferinţa ştiinţifică naţională cu participare internaţională, organizată cu ocazia a 60 de ani de la înființarea Facultății de Drept (USM, 01-02 octombrie 2019, Chișinău). Vol. II*. Chișinău: CEP USM, 2020, pp. 29-40. ISBN 978-9975-149-88-4.
10. *Directiva 2013/40/UE a Parlamentului European și a Consiliului din 12.08.2013 privind atacurile împotriva sistemelor informatice și de înlocuire a Deciziei-cadru 2005/222/JAI a Consiliului*. [citat 18.12.2020] Disponibil: https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32013L0040&from=en
11. DRĂGAN, Alin Teodorus. *Frauda informatică: analiza juridico-penală a infracțiunii*: tz. de doct. în drept. Chișinău, 2017. 179 p.
12. DUMNEANU, Ludmila, GUREV, Dorina. *Infracţiuni în domeniul informatic: Note de curs*. Chișinău: CEP USM. 261 p. ISBN 978-9975-158-29-9.
13. Hotărârea Guvernului pentru aprobarea Regulamentului privind armonizarea legislației Republicii Moldova cu legislația Uniunii Europene: nr. 1171 din 28.11.2018. În: *Monitorul Oficial al Republicii Moldova*, 2018, nr. 499-503, 1314.
14. Legea cu privire la informatică: nr. 1069 din 22.06.2000. În: *Monitorul Oficial al Republicii Moldova*, 2001, nr. 73-74, 547.
15. Legea pentru modificarea şi completarea Legii telecomunicaţiilor nr. 520-XIII din 7 iulie 1995 şi a Codului penal al Republicii Moldova: nr. 254 din 09.07.2004. În: *Monitorul Oficial al Republicii Moldova*, 2004, nr. 189-192, 848.
16. Legea pentru ratificarea Convenţiei Consiliului Europei privind criminalitatea informatică: nr. 6 din 02.02.2009. În: *Monitorul Oficial al Republicii Moldova*, 2009, nr. 37-40, 104.
17. *Proiectul legii pentru modificarea și completarea unor acte legislative (Legea privind Serviciul de Informații și Securitate al RM – art. 7; Codul penal – art. 178, 208[1], 259 ș.a.)*. [citat 30.08.2020] Disponibil: www.parlament.md/ProcesulLegislativ/Proiectedeactelegislative/tabid/61/LegislativId/3183/language/ro-RO/Default.aspx+&cd=3&hl=ro&ct=clnk&gl=at
18. SOLTAN, Veaceslav. Infracțiunile informatice (art. 259-261[1] Cod penal). În: *Procuratura Republicii Moldova. Buletin informativ*, 2010, nr. 15, pp. 38-43. [citat 11.07.2022] Disponibil: http://procuratura.md/file/BULETIN%20VIRTUAL%2015.pdf
19. STATI, Vitalie. Răspunderea penală pentru infracţiunile în domeniul informaticii şi telecomunicaţiilor. În: Analele Ştiinţifice ale Universităţii de Stat din Moldova. Seria „Ştiinţe socioumanistice". Vol. 1. Chişinău: CEP USM, 2005, pp. 387-394. ISSN 1811-2668.
20. *Convention on Cybercrime*. [citat 06.03.2022] Disponibil: https://rm.coe.int/1680081561
21. ГЫРЛА, Л.Г., ТАБАРЧА, Ю.М. *Уголовное право Республики Молдова. Часть Особенная. Том 2*. Кишинэу: Cartdidact, 2010. 592 с. ISBN 978-9975-4158-2-8.

22. ЛАЗАРЕВА, Наталья. Уголовно-правовая характеристика преступлений в области информатики и электросвязи. În: *Revista ştiinţifică a USM „Studia Universitatis”. Seria „Ştiinţe sociale”*, 2007, nr. 6, pp. 133-141. ISSN 1857-2081.

LIST OF THE AUTHOR'S PUBLICATIONS ON THE THEME OF THE THESIS

A. Monograph

1. STRÎMBEANU, Alexandru. Răspunderea penală pentru accesul ilegal la informaţia computerizată: Monografie. Chişinău: Tipografia Centrală, 2023. 430 p. ISBN 978-5-88554-178-7.

B. Articole în reviste

2. BOTNARENCO, Mihaela, STRÎMBEANU, Alexandru. Sistemul informatic și rețeaua informatică: obiecte materiale ale infracțiunilor prevăzute la art.259 din Codul penal. În: Studia Universitatis Moldaviae, Seria „Ştiinţe Sociale”, 2022, nr. 8, pp. 77-90. ISSN 1814-3199.
3. BOTNARENCO, Mihaela, STRÎMBEANU, Alexandru. Victima infracțiunilor prevăzute la art. 259 din Codul penal. În: Studia Universitatis Moldaviae, Seria „Ştiinţe Sociale”, 2022, nr. 8, pp. 111-120. ISSN 1814-3199.
4. BRÎNZA, Serghei, STRÎMBEANU, Alexandru. Unele aspecte ale laturii obiective a infracțiunilor prevăzute la art. 259 din Codul penal. În: *Studia Universitatis Moldaviae, Seria „Ştiinţe Sociale”*, 2023, nr. 3, pp. 3-15. ISSN 1814-3199.
5. STRÎMBEANU, Alexandru. Accesul ilegal la informaţia computerizată: analiza comparativă a normelor din codurile penale ale Republicii Moldova și statelor membre ale Uniunii Europene. [citat 30.12.2022] Disponibil: În: *SSRN Electronic Journal*. ISSN 1556-5068. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4234979
6. STRÎMBEANU, Alexandru. Acțiunea adiacentă din cadrul infracțiunilor prevăzute la art. 259 din Codul penal. În: *Studia Universitatis Moldaviae, Seria „Ştiinţe Sociale”*, 2023, nr. 3, pp. 149-158. ISSN 1814-3199.
7. STRÎMBEANU, Alexandru. Caracterul ilegal al accesului la informaţia computerizată: condiţie de aplicare a art. 259 din Codul penal al Republicii Moldova. În: *Revista Institutului Naţional al Justiţiei*, 2023, nr. 1, pp. 9-13. ISSN 1857-2405.
8. STRÎMBEANU, Alexandru. Circumstanțele agravante ale infracțiunilor de acces ilegal la informația computerizată (art. 259 din Codul penal al Republicii Moldova). În: *SSRN Electronic Journal*. ISSN 1556-5068. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4331505
9. STRÎMBEANU, Alexandru. Condiționarea socială și juridică a incriminării accesului ilegal la informația computerizată. [citat 30.12.2022] Disponibil: În: *SSRN Electronic Journal*. ISSN 1556-5068. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4234976
10. STRÎMBEANU, Alexandru. Elementele constitutive subiective ale infracțiunilor de acces ilegal la informația computerizată (art. 259 din Codul penal al Republicii Moldova). [citat 30.12.2022] Disponibil: În: *SSRN Electronic Journal*. ISSN 1556-5068. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4313475
11. STRÎMBEANU, Alexandru. Materiale științifice referitoare la accesul ilegal la informaţia computerizată publicate în Republica Moldova. În: *Studia Universitatis Moldaviae, Seria „Ştiinţe Sociale”*, 2021, nr. 3, pp. 133-142. ISSN 1814-3199.

12. STRÎMBEANU, Alexandru. Materialele științifice referitoare la accesul ilegal la informaţia computerizată publicate peste hotare. În: *Studia Universitatis Moldaviae, Seria „Ştiinţe Sociale”*, 2021, nr. 8, pp. 114-127. ISSN 1814-3199.
13. STRÎMBEANU, Alexandru. Noţiunea de acces la informaţia computerizată în accepţiunea art. 259 din Codul penal al Republicii Moldova. În: *Revista Institutului Naţional al Justiţiei*, 2022, nr. 3, pp. 16-22. ISSN 1857-2405.
14. STRÎMBEANU, Alexandru. Obiectul juridic generic al infracțiunilor de acces ilegal la informaţia computerizată (art. 259 din Codul penal al Republicii Moldova): aspectul *de lege lata*. Disponibil: În: *SSRN Electronic Journal*. ISSN 1556-5068. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4234980
15. STRÎMBEANU, Alexandru. Obiectul juridic generic al infracțiunilor de acces ilegal la informaţia computerizată (art. 259 din Codul penal al Republicii Moldova): aspectul *de lege ferenda*. Disponibil: În: *SSRN Electronic Journal*. ISSN 1556-5068. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4234982
16. STRÎMBEANU, Alexandru. Obiectul juridic special al infracțiunilor de acces ilegal la informaţia computerizată (art. 259 din Codul penal al Republicii Moldova): premise conceptuale. Disponibil: În: *SSRN Electronic Journal*. ISSN 1556-5068. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4313468
17. STRÎMBEANU, Alexandru. Obiectul juridic special al infracțiunilor de acces ilegal la informaţia computerizată (art. 259 din Codul penal al Republicii Moldova): reflecții, abordări și soluții. Disponibil: În: *SSRN Electronic Journal*. ISSN 1556-5068. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4313472

C. Articles in conference proceedings

18. STRÎMBEANU, A. Victima secundară a infracțiunilor prevăzute la art. 259 din Codul penal. În: *Conferința științifică națională cu participare internațională dedicată aniversării a 75-a a Universității de Stat din Moldova „Integrare prin cercetare și inovare” (10-11 noiembrie 2021)*. Chișinău: CEP USM, 2021, pp. 6-8. ISBN 978-9975-152-48-8.
19. STRÎMBEANU, Alexandru. Anumite aspecte ale obiectului material (imaterial) al infracțiunilor prevăzute la art. 259 CP RM. În: *Conferinţa ştiinţifică internaţională „Infracţiunea – Răspunderea penală – Pedeapsa. Drept şi Criminologie”, Ediţia a 2-a (24-25 martie 2022, Chişinău): Culegere de comunicări*. Chișinău: CEP USM, 2022, pp. 231-242. ISBN 978-9975-62-476-3.
20. STRÎMBEANU, Alexandru. Calculatorul – obiect material al infracțiunilor prevăzute la art. 259 din Codul penal. În: *Conferința științifică națională cu participare internațională „Integrare prin cercetare și inovare”, dedicată Zilei internaționale a Științei pentru pace și Dezvoltare (10-11 noiembrie 2022)*. Chișinău: CEP USM, 2022, pp. 69-71. ISBN 978-9975-152-48-8.
21. STRÎMBEANU, Alexandru. Coerența teleologică dintre art. 259 Cod penal și prevederile complementare din legislația națională. În: *Integrare prin cercetare și inovare. Științe juridice și economice. Vol. 1 (7-8 noiembrie 2020, Chișinău)*. Chișinău: CEP USM, 2020, pp. 13-16. ISBN 978-9975-152-48-8.

ADNOTARE

Strîmbeanu Alexandru, „Răspunderea penală pentru accesul ilegal la informația computerizată”. Teză de doctorat în drept. Școala Doctorală de Științe Juridice a Universității de Stat din Moldova. Chișinău, 2023

Structura tezei: introducere, trei capitole, concluzii și recomandări, bibliografie din 406 de titluri. Rezultatele obținute sunt publicate în 21 lucrări științifice.

Cuvintele-cheie: acces ilegal; informație computerizată; date informatice; sistem informatic; rețea informatică; calculator; sisteme de protecție.

Scopul lucrăriieste de a investiga temeinic elementele constitutive și circumstanțele agravante ale infracțiunilor prevăzute la art. 259 CP RM, de a evidenția vulnerabilitățile ce caracterizează interpretarea și aplicarea acestui articol, precum și de a propune soluții menite să contribuie la perfecționarea mecanismului de contracarare prin mijloace penale a accesului ilegal la informaţia computerizată.

Obiectivele cercetării: investigarea viziunilor doctrinare cu privire la răspunderea pentru infracțiunile prevăzute la art. 259 CP RM; utilizarea potențialului, de care dispun reglementările naționale cu privire la accesul la informaţia computerizată, în procesul de interpretare a acestui articol; identificarea gradului de compatibilitate dintre art. 259 CP RM și reglementările de sorginte internațională privind interzicerea accesului ilegal la informaţia computerizată,etc.

Noutatea şi originalitatea ştiinţifică a tezei rezidă în aceea că a fost realizată o analiză temeinică, sub aspect juridico-penal, a faptelor incriminate în art. 259 CP RM. Noutatea ştiinţifică a rezultatelor cercetării constă, de asemenea, în învederarea unor concepţii controversate atestate în doctrina de specialitate, în examinarea acestora şi în expunerea propriei viziuni argumentate. Pe acest fundament au fost punctate concluzii şi recomandări necesare pentru îmbunătățirea calității art. 259 CP RM și a cadrului normativ adiacent.

Rezultatele obținute care contribuie la soluționarea unei probleme ştiinţifice importante: fundamentarea concepției de interpretare a art. 259 CP RM și de calificare a infracțiunilor în baza acestui articol fără a fi încălcat principiul legalității, această fundamentare având ca efect identificarea erorilor de aplicare a art. 259 CP RM și a defectelor ce caracterizează dispoziția acestui articol, astfel fiind creată baza teoretică necesară pentru a perfecționa practica de aplicare a art. 259 CP RM și pentru a îmbunătăți calitatea acestui articol.

Semnificația teoretică a tezei: a) redimensionarea apărării penale a relaţiilor sociale cu privire la accesul autorizat sau permis la informaţia computerizată; b) acumularea unui amplu material teoretic şi practic indispensabil pentru dezvoltarea unor direcţii actuale şi complexe ale investigării infracţiunilor prevăzute la art. 259 CP RM; c) caracterizarea detaliată a elementelor constitutive și a circumstanțelor agravante ale infracțiunilor prevăzute la art. 259 CP RM; d) identificarea neajunsurilor de care suferă dispoziția art. 259 CP RM și practica de aplicare a acestei dispoziții.

Valoarea aplicativă a tezei: a) interpretarea din perspective noi a prevederilor art. 259 CP RM contribuie la dezvoltarea discuţiei ştiinţifice privind stabilirea temeiului juridic al răspunderii penale pentru faptele incriminate în acest articol; b) analiza de drept comparat și analiza istorică a reglementărilor privind răspunderea pentru accesul ilegal la informația computerizată comportă o semnificaţie cognitivă în vederea percepерii esenței juridice şi sociale a infracţiunilor prevăzute la art. 259 CP RM, etc.

Implementarea rezultatelor ştiinţifice: în procesul de creaţie legislativă (în scopul înlăturării neajunsurilor ce caracterizează dispoziția art. 259 CP RM), în procesul educaţional (în scopul de sporire a nivelului de cunoștințe și deprinderi ale studenţilor de la facultăţile de drept din instituţiile de învăţământ superior, a audienţilor și beneficiarilor de instruire continuă din cadrul INJ) şi în activitatea ştiinţifică de perspectivă.

АННОТАЦИЯ

Стрымбяну Александру, «Уголовная ответственность за несанкционированный доступ к компьютерной информации». Диссертация на соискание научной степени доктора права. Докторальная школа юридических наук Государственного университета Молдовы. Кишинэу, 2023

Структура диссертации: введение, три главы, выводы и рекомендации, библиография из 406 названий. Достигнутые результаты опубликованы в 21 научных работах.

Ключевые слова: несанкционированный доступ; компьютерная информация; компьютерные данные; информационная система; компьютерная сеть; компьютер; системы защиты.

Цель работы: углубленное исследование состава и отягчающих обстоятельств преступлений, предусмотренных ст. 259 УК РМ, выделение уязвимостей, характеризующих толкование и применение данной статьи, а также предложение решений, необходимых в плане совершенствования механизма противодействия уголовно-правовыми средствами несанкционированному доступу к компьютерной информации.

Задачи исследования: изыскание доктринальных взглядов на ответственность за преступления, предусмотренные ст. 259 УК РМ; использование в процессе толкования данной статьи потенциала внутриправовых норм, регламентирующих доступ к компьютерной информации и др.

Научная новизна и оригинальность результатов исследования выражаются впроведении тщательного уголовно-правового анализа преступлений, предусмотренных ст. 259 УК РМ. Научная новизна результатов исследования заключается также в изложении некоторых спорных доктринальных воззрений, в их рассмотрении и в предложении собственного аргументированного мнения. На этом основании делаются выводы и рекомендации, необходимые для улучшения качества ст. 259 УК РМ и смежной нормативной базы.

Полученные результаты, способствующие решению особо значимой научной проблемы, разрешенной в рамках проведенного диссертационного исследования состоят в обосновании концепции толкования ст. 259 УК РМ и квалификации преступлений по этой статье с соблюдением принципа законности, с целью выявления ошибок в применении ст. 259 УК РМ и недостатков, характеризующих диспозицию данной статьи, тем самым способствуя созданию теоретической базы, необходимой для совершенствования практики применения ст. 259 УК РМ и для улучшения качества данной статьи.

Теоретическая значимость: а) переосмысление концепции уголовно-правовой охраны общественных отношений по поводу санкционированного или разрешенного доступа к компьютерной информации; б) накопление обширного теоретического и практического материала, необходимого для разработки актуальных и комплексных направлений исследования преступлений, предусмотренных ст. 259 УК РМ; в) подробная характеристика состава и отягчающих обстоятельств преступлений, предусмотренных ст. 259 УК РМ и т.д.

Практическая применяемость исследования: а) толкование с новых позиций положений ст. 259 УК РМ способствует развитию научной дискуссии относительно установления правовых основ уголовной ответственности за деяния, предусмотренные данной статьей; б) сравнительно-правовой и исторический анализ норм об ответственности за несанкционированный доступ к компьютерной информации имеют познавательное значение для постижения правовой и социальной сущности преступлений, предусмотренных ст. 259 УК РМ и т.д.

Апробация результатов диссертационного исследования: в процессе законотворчества (в целях устранения недостатков ст. 259 УК РМ), в образовательном процессе (в целях повышения уровня знаний и навыков студентов юридических факультетов высших учебных заведений, слушателей и бенефициаров непрерывного образования в рамках НИЮ) и в перспективной научной деятельности.

ANNOTATION

Strimbeanu Alexandru, "Criminal liability for illegal access to computerized information". PhD in Law thesis. Doctoral School of Legal Sciences of the State University of Moldova. Chișinău, 2023

The structure of the thesis: introduction, three chapters, conclusions and recommendations, bibliography of 406 titles. The results achieved are published in 21 scientific papers.

Key-words: illegal access; computerized information; computer data; information system; computer network; computer; protection systems.

The purpose of the Ph.D. thesis is to thoroughly investigate the constituent elements and aggravating circumstances of the crimes provided by the art. 259 CrC RM, to highlight the vulnerabilities that characterize the interpretation and application of this article, as well as to propose solutions intended to contribute to the improvement of the mechanism of counteracting by criminal means illegal access to computerized information.

The objectives of investigation: investigating the doctrinal views regarding the liability for the crimes provided by the art. 259 CrC RM; the use of the potential, available in national regulations regarding access to computerized information, in the process of interpreting this article; identifying the degree of compatibility between art. 259 CrC RM and regulations of international origin regarding the prohibition of illegal access to computerized information, etc.

The scientific novelty and originality of the obtained results are expressed in a thorough criminal law analysis of crimes provided by the art. 259 CrC RM. The scientific novelty of the research results also consists in the examination of some controversial concepts attested in the specialized doctrine, in their examination and in the exposition of one's own reasoned vision. On this basis, conclusions and recommendations that are made are necessary to improve the quality of the art. 259 CrC RM and the related regulatory framework.

The obtained results which contribute solving of the foremost scientific problem: substantiation of the concept of interpretation of art. 259 CrC RM and the qualification of crimes in accordance with this article without violating the principle of legality, this substantiation having the effect of identifying errors in the application of art. 259 CrC RM and the defects that characterize the provision of this article, thus creating the theoretical basis necessary to perfect the practice of applying art. 259 CrC RM and to improve the quality of this article.

Theoretical importance: a) the resizing of the criminal defense of social relations regarding authorized or permitted access to computerized information; b) the accumulation of ample theoretical and practical material indispensable for the development of current and complex directions of the investigation of crimes provided by the art. 259 CrC RM; c) detailed characterization of the constitutive elements and aggravating circumstances of the crimes provided by the art. 259 CrC RM; d) identifying the shortcomings that characterize the provision of art. 259 CrC RM and the practice of applying this provision.

Practical value of the research paper: a) the interpretation from new perspectives of the provisions of art. 259 CrC RM contributes to the development of the scientific discussion regarding the establishment of the legal basis of criminal liability for the acts incriminated in this article; b) the analysis of comparative law and the historical analysis of the regulations regarding liability for illegal access to computerized information have a cognitive significance in order to perceive the legal and social essence of the crimes provided for in art. 259 CrC RM, etc.

Implementation of the scientific results: in the process of legislative creation (in order to remove the shortcomings that characterize the provision of art. 259 of the Criminal Code of the Republic of Moldova), in the educational process (in order to increase the level of knowledge and skills of students from law faculties in higher education institutions, of the audients and beneficiaries of continuous training from the NIJ) and in perspective scientific activity.

STRÎMBEANU ALEXANDRU

CRIMINAL LIABILITY FOR ILLEGAL ACCESS TO COMPUTERIZED INFORMATION

Specialty 554.01 – Criminal law and criminal enforcement

Summary of the doctoral thesis in law

Approved for printing: data
Offset paper. Offset printing.
Printing sheets: …

Paper size: 60x84 1/16
Circulation … ex…
Orders no. ….

Editorial-Polygraphic Center of the State University of Moldova
mun. Chisinau, str. Alexei Mateevici, 60, MD 2019