Preventing computer crime by knowing the legal regulations that ensure the protection of computer systems

Professor **Elena-Ana IANCU**[1]
Lecturer **Enache TUȘA**[2]
PhD. **Nicolaie IANCU**[3]
Associate professor **Eduard SIMION**[4]
Associate professor **Adrian-Cristian MOISE**[5]

Abstract

Our intention in this study is to emphasise a few aspects relating to the need to support cyber education and to preventive goals, by informing people about the strategies in place at Union and/or national level, which reflect current realities, in relation to which each person, active entities and, last but not least, the authorities will have to act so as to identify early on any possible risks. We have also aimed to identify legislation that criminalises acts of cyber fraud, in which respect we have referred to certain articles in the criminal codes of several European countries. We consider that cyber education and legal education, regardless of the social level one belongs to, the social roles one takes on at a given time, and/or of age, are essential to setting the foundations for a cyber security culture.

Keywords: *education, cyber space, cyber security, law, criminal offence.*

JEL Classification: *K14, K24*

DOI: 10.24818/TBJ/2023/13/3.03

1. Introduction

In a context where digitization is an objective taken on by the European Union, all countries cooperate to achieve common cyber security at EU level. In view of ensuring an open, safe cyber space, that would increase trust in the entities implementing the necessary technology, which, on the one hand, is unknown or little known to citizens, and on the other hand, can be used by people aiming to obtain illegal/unlawful pecuniary or non-pecuniary benefits, advantages or dominant positions in various fields of activity, control in regional or world areas, we turn our

[1] Elena-Ana Iancu - "Aurel Vlaicu" University of Arad, Academy of Legal Sciences from Romania, https://orcid.org/0000-0002-5921-2222, elenaanaiancu@gmail.com.
[2] Enache Tușa - Ovidius University of Constanța, Romania, https://orcid.org/0000-0003-4703-1763, enachetusa@gmail.com.
[3] Nicolaie Iancu - Brigadier General (r), President of SARA Law Research Center, Oradea, Romania, https://orcid.org/0000-0002-0892-6823, niancu2009@yahoo.com.
[4] Eduard Simion - University of Oradea, Romania, https://orcid.org/0000-0003-0801-7272, eduard.simion@gmail.com.
[5] Adrian-Cristian Moise - "Spiru Haret" University, Faculty of Juridical, Economic and Administrative Sciences, Craiova, Romania, https://orcid.org/0000-0001-8755-0563, adriancristian.moise@gmail.com.

attention to the educational field, including cyber education, which cannot be separated from specific legal education in this age of digitization, especially in the larger context of sustainable development of a country.

Cyber security at the level of the European Union cannot be achieved without protecting the social values that complement the concept of security, therefore, a thorough knowledge of legal norms (rules) that criminalise acts which endanger such values or generate consequences through the harm resulting from actions and/or inactions, that may be quantified as clear, certain, well-defined damages, or which create preconditioning situations, of danger, is necessary in order to anticipate delinquent behaviours that have a negative impact on the social values existing in the cyber space.

The socio-economic challenges of modern society necessarily involve the existence of well-trained human resources that are able to effectively manage the various tasks related to the job held, but also to handle the evolution (revolution) of computer science in an efficient manner[6].

Romania's National Sustainable Development Strategy 2030 has been approved in Romania (through Government Decision no. 877/2018), in which 17 goals were formulated and undertaken. In the context of the current study, we make reference to: goal 16 *"Peace, justice and strong institutions"* which includes social capital and public safety as a specific goal[7], and goal 17 *"Partnerships for the goals"*, which includes national safety and international partnerships. Thus, we propose an interdisciplinary study by which to emphasise the importance of the existence of legal rules protecting cyber security and safety, the need to disseminate the information and data that every individual should be aware of, in order to understand the legal or illegal nature of their conduct. We also wish to highlight the need for ongoing training of specialists with professional skills pertaining to other fields, as well as the need for every citizen to become familiar with the measures to be adopted and implemented so as to increase their safety in the online environment or during offline periods.

The feeling of tranquility and trust conferred by state institutions to the population in relation to the the implementation of measures for the preservation of public order and peace, of the safety of communities and goods, as part of the "public safety" concept, should be reflected at both a macrosocial and a microsocial level[8].

Thus, each individual will be ready to support communities/social micro-groups in the process of development, of ensuring peace in society, of increasing the degree of trust in state institutions, of contributing to the safety of the social microgroups in which they live/are active, even by ensuring specialised support within their own family.

---

[6] Daniela-Cristina Creț (2021), *Defending family law values via criminal law norms,* in „Agora International Journal of Juridical Sciences", Vol. 15, No. 2, 2021, p. 17, DOI: https://doi.org/10.15837/aijjs.v15i2.4654.

[7] Elena-Ana Iancu (2019)**,** *The Contribution of Forensic Science to Establishing the Truth in Criminal Proceedings* in „Athens Journal of Law", Volume 5, Issue 4, 2019- pp. 1-2, DOI: https://doi.org/10.30958/ajl.5-4-6.

[8] Daniela-Cristina Creț (2021), *op. cit.*, p.17.

Familiarity, knowledge and comprehension of the cyber space are essential to the processes of cyber crime prevention and combating, irrespective of the hypotheses we refer to, generated by the mixed use of cyber space and/or of the classical environment, in which perpetrators carry out certain material acts that make up the objective side of the criminal offence, or where the cyber space is the only space in which the entire illegal activity is carried out.

Even if, apparently, certain categories of criminal offences might seem impossible to commit by means of technology or of a computer (information) system, in light of the possible regulatory approach, however, in fact, the concrete methods of committing crimes are very diverse, as wrongdoers use interconnected technology both in the stage of preparing the moment when they will take action, and at the time of coomitting the deed and/or thereafter.

Also, in the case of criminal participation, the people involved use existing technical means in the process of search for/identification of new potential victims, to secure an alibi for themselves, to detect the technology used by state authorities to ensure the security of interconnected infrastructures, or to ensure the surveillance/monitoring of certain areas.

Therefore, an increased interest in educational institutions, in the direction of preventive education in the field of order, safety and/or security, and implicitly, of cyber security, will contribute to an increase in the level of public safety and/or national security, which will be so necessary in the future, including by assigning research themes with a pronounced preventive focus, which themes are part of the subject sheets aimed at developing transversal skills, as well as by assigning research themes within doctoral (PhD) or postdoctoral studies.

As a result, in reference to the prevention and/or combating of criminal offences or to personal identification, it is necessary to place emphasis on biometrics, which involves interconnected systems that are able to take over, process, verify or establish identity, as well as store the characteristics of a person.

Law no. 51/1991[9] *on the national security of Romania*, republished, defines the concept of "national security of Romania" as "a state of social, economic and political legality, equilibrium and stability that is necessary for the existence and development of the Romanian national state – a sovereign, unitary, independent and indivisible state, to the maintenance of legal order as well as of the climate for the unhampered exercise of the fundamental rights, freedoms and duties of the citizens, in accordance with the democratic principles and rules provided by the Constitution".

The concept of cyber security includes the notion of connected infrastructure assets, such as connected computing devices, personnel, infrastructure, applications, digital services[10], telecommunication systems and data in the digital environment that may belong to government, private organizations, and citizens. The protected

[9] Published in the Official Journal 190 of 18 March 2014, https://legislatie.just.ro/Public/Detalii Document/1517, accessed on 07.06.2022.

[10] Guide to Developing a National Cybersecurity Strategy Strategic Engagement in Cybersecurity, 2nd edition 2021, https://ncsguide. org/the-guide/introduction/.

values are the availability, integrity and confidentiality of interconnected infrastructures.

The constant efforts of countries to increase the level of domestic cyber security are obvious in this age, when the latter cannot be separated from European and world cyber security. As of 2018, Romania has put into practice the NIS Directive[11], to which Law no. 362/2018 *on ensuring a high common level of security of networks and computer (information) systems*[12] makes reference.

As of 2022, at the level of the European Union, the Network Information and Security Directive (NIS 2)[13] will be applicable, which will replace the Network and Information Systems Security Directive (NIS) and which will be the reference for the creation of the European Cyber Crisis Liaison Organisation Network[14].

Limited knowledge of technology, in the field of media[15], combined with the emergence of platforms, and inherently, the intensification of current activities in the virtual space will remain challenges for the entities that manage technologies, as well as for their users, the behaviour of the latter having an impact on the dynamics of the criminal phenomenon.

Several procedures are used in the conceptualization of legal rules[16] (norms), which provide the quality standard in the process of regulation of future human conducts, aimed at protecting the general safety of earthlings, implicitly by identifying the best content of the norm, the expression of the legislator's thinking in relation to the already existing and unregulated social behaviours, to the tendencies of the phenomenon being analysed from an interdisciplinary perspective, as well as to the educational, technological and social realities that generate diverse behaviours through the use of computer systems.

2. Defence of social values through Romanian criminal law rules

In the Criminal Code of Romania (*Law no. 286/2009*), in Article (Art.) 181, with the marginal name "Computer Systems and Digital Data", the meaning given by the legislator to the two associated notions is indicated, with a remark that the legislator's way of thinking shows the need to approach the two in a cumulative manner. A first prerequisite for a device or assembly of devices to be considered as *computer system*, pursuant to paragraph (1) of Art. 181, is that they should be

[11] https://eur-lex.europa.eu/legal-content/RO/TXT/HTML/?uri=CELEX:32016L1148&from=RO, accessed on 07.06.2022.

[12] https://legislatie.just.ro/Public/DetaliiDocument/209670, accessed on 07.06.2022.

[13] Network and Information Security Directive-NIS, adopted on 10 November 2022, published in the Official Journal.

[14] https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf, p. 12, accessed on 5.12. 2022.

[15] Molly K. Land and Jay D. Aronson, *Human Rights and Technology: New Challenges for Justice and Accountability* in „Annual Review of Law and Social Science", 2020, 16:1, 223-240, https://www.annualreviews.org/doi/pdf/10.1146/annurev-lawsocsci-0602 20-081955, accessed on 20.12.2022.

[16] Iulia Boghirnea, *The Creation of the General Legal Norm*, „Annales Universitatis Apulensis, Series Jurisprudentia", no. 11/ 2008, pp. 28-38, https://journals.uab.ro/index.php/auaj/.

"interconnected" or "in an operational relation" (with one another). The second prerequisite is related to the functions of the device or assembly of devices, in the sense that at least one device or assembly of devices must ensure the automated processing of data, by means of *software.*

The facts, information or concepts which are represented in a form that may lead to the processing thereof in a computer system are considered to be *digital data* (*Law no. 286/2009, Art. 181, par. 2*).

We also note that, in the Criminal Procedure Code (Law no. 135/2010), in Art. 138 par. 4, the Romanian legislator defines the notion of computer system in a similar manner to the content of Art. 181, par. 2 of Law no. 286/2009, and the notion of digital data is taken from the same Article (paragraph 2), with a mention that it operates a distinction, by additional text, with regard to software, in the sense that the processing is carried out by a program which is "able to determine the performance of a function by a computer system" (*Law no. 135/2010, Art. 138 par. 5*).

In Romanian legislation, there are legal norms which state the meaning of cyber crime, such as Decision no. 217 of 2013, which, in point 3, indicates the abstract meaning of the notion as being "the acts provided by the criminal law or other laws with criminal provisions which are committed by using a cyber infrastructure".

By going through the Criminal Code of Romania (Law no. 286/2009), we find several Articles placed by the Romanian legislator in different chapters, with titles referring to the social value that is mainly protected by each of them. Thus, under Title VII, with the marginal name "Offences Against Public Security", a whole chapter, namely Chapter VI, with the marginal name "Offences Against the Security and Integrity of Computer Systems and Digital Data", is reserved to the protection of computer systems and data, within the meaning of which the legal object consists in the social relations regarding the safety and integrity thereof.

Similarly, in the Criminal Code, we highlight the criminal offence provided for in Article 374, with the marginal name "Child Pornography", placed by the legislator under Title VIII, with the marginal name "Offences That Harm Social Relationships", par. 2, which is the aggravated form of the offence, the means expressly provided for the carrying out of the material element in order to achieve the outcome being the "computer system or other means of data storage". Paragraph 3 of the same Article contains essential requirements related to the material element, namely that the accessing of child pornography material should occur "unlawfully" and through computer systems or other means of electronic communication.

Title IX, with the marginal name "Election Offences", includes Art. 391, with the marginal name "Counterfeiting Documents and Voting Records", which, in its aggravated form indicated in par. 3, provides as alternative regulatory methods of committing the crime, either the introduction in use, or the use of flawed computer software that leads to at least one of the consequences expressly provided by the legislator. These consequences refer to the alteration of the specific voting procedure in three stages, namely: the initiation/preparation stage, in which pre-voting

registrations are made, the centralization stage, in which the results obtained in the polling stations are summed up, or the stage of seats' distribution, in which the seats are distributed. In the case of the assimilated form of the offence, indicated in par. 4 in connection with par. 3, the alteration of the national computer system, by the action of introducing non-compliant data, information or procedures, which lead to the falsification of the results in the final stage of determining the results of the elections, is punished.

Of course, Title I of the Special Part, with the marginal name "Offences Against the Person", in Chapter VI, with the marginal name "Offences Against Individual Freedom", contains crimes that may be concretely committed through the use of computer systems, such as: threats (Art. 206), blackmail (Art. 207), harassment (Art. 208), sexual intercourse with a minor (Art. 220), offences that used to be committed through classic methods before the large-scale use of computers and technology. Taking into account the number of people who use technical means capable of being interconnected through the applications used by the owners of these types of mobile goods, we also notice a change in the behaviour of the perpetrators during the preparation, the commission of the acts provided for by the criminal law/criminal offences such as threat, blackmail, harassment. In the same sense, we make reference to the special law with criminal provisions, "Law 217/2003 on preventing and combating domestic violence"[17], in which cyber violence is defined in Art. 4, letter h), as a manner of manifesting domestic violence. Thus, we retain, from the abstract content of this Article, that the legislator provides as a regulatory method of crime commission *"the abusive use of information and communication technology"*, by means such as: computers, telephones with the ability to connect to cyberspace platforms, or other devices that use telecommunications. In order to qualify as cyber violence, we note, in the legal text, the legislator's requirements, namely, that the use should be abusive and that the purpose expressly provided for, in the sense of retaining the direct intention qualified by purpose, should be "to embarrass, humiliate, frighten, threaten, silence the victim".

In Title II of the Criminal Code of Romania. The Special Part, with the marginal name "Offences Against Property", Chapter IV includes crimes falling under the marginal name "Frauds Committed Using Computer Systems and Electronic Payment Methods".

The criminal offence with the marginal name *"Computer Fraud"* is provided for in Art. 249 and can be committed, according to sentence (thesis) I, through specific actions of computer data manipulation by at least one of the following methods: computer data entry; computer data transmission; computer data alteration; computer data deletion. It may be an action or an inaction, the latter occurring, according to sentence II, when the perpetrator "restricts access to computer data" or, alternatively, when he hinders the operation of a computer system. The specific form of guilt for this type of crime is direct intention, the purpose being expressly provided by the legislator, namely to obtain a benefit. With

[17] Republished in the Official Journal no. 948 of 15 October 2020.

reference to the essential requirements, we note that the legislator stipulates in the criminalising rule that damage should result from the action and/or inaction. We also note the express provision that the material benefit foreseen and pursued by committing the act can be a benefit for the perpetrator and/or another person.

In the same chapter, we find the offence of *"Making Fraudulent Financial Operations"* in three versions, namely: the simple version in paragraph 1, the assimilated version in paragraph 2, and the mitigated version in paragraph 3. Thus, in the typical form of the crime, the material element is achieved through specific actions that materialise in the cash withdrawal operation, according to sentence I, or by "loading or unloading an electronic money instrument". Also, according to sentence II, the material element is achieved by actions of "transfer of funds, monetary value or virtual currency", while retaining the essential requirement that the actions should be carried out without the consent of the owner. Thus, we also note that, through the regulatory methods of committing the crime, the behaviour of the perpetrator is sanctioned, irrespective of whether or not the payment instrument is cashless or whether the identification data allowing its use have been used.

In the assimilated version provided for in paragraph 2, the material element can be achieved through any specific action that results in one of the operations provided for in paragraph 1, but we retain as a regulatory method the requirement that the use should be unauthorized or that the identification data used for authentication should be fictitious. The legal rule, through its abstract content, in paragraph 3, provides for a sanction against the perpetrator who transmits the identification data to another person in order to carry out at least one operation provided for in paragraph 1 and paragraph 2, with the essential requirement that the transmission should be unauthorized.

In Art. 250^1, with the marginal name *"Illegal Operations with Cashless Payment Instruments"*, we retain, in terms of the material element, the inaction of possessing an illegally appropriated cashless payment instrument, by committing one of the acts provided for in "Art. 228, Art. 229, Art. 233-236, Art. 238, Art. 239, Art. 243, Art. 244 and Art. 295", in the case of paragraph 1. In paragraph 2, the acquisition of a cashless payment instrument obtained by committing one of the acts referred to in paragraph 1 is punished. We note, both in paragraph 3 and in paragraph 4, that the material element which can be achieved through action and/or followed by inaction, involves several alternative methods. Thus, paragraph 3 criminalises the manufacture, possession, transmission of computer data, equipment, hardware or software necessary for the appropriation of a cashless payment instrument, whereas paragraph 4 criminalises the acquisition of means necessary for the appropriation of a cashless payment instrument. We note, in these paragraphs, on the one hand, the similar form of guilt, direct intention, qualified by purpose, in the sense that the purpose expressly required by the legislator, "to serve for the appropriation of a cashless payment instrument" must be proven, and on the other hand, the reference to the same facts provided for by the legislator, as mentioned in paragraph 1.

The Romanian legislator also criminalised, through Art. 251 with the marginal title *"Acceptance of Financial Operations Carried Out Fraudulently"*, the

facts by which a person accepts cash withdrawal operations, including monetary value or virtual currency. In the case of this Article, it is essential that the active subject should be aware that the premise action or inaction occurs by using a forged payment instrument (paragraph 1) or by using it without the owner's consent (paragraph 1). Likewise, the use of unauthorized identification data or the use of fictitious data in the procedures provided for in paragraph 1 will be sanctioned according to paragraph 2, the assimilated version.

With reference to the punishment provided by the legislator in the case of the offences provided for in this chapter, we highlight the fact that the penalty is imprisonment with a special minimum limit of 2 years and a special maximum limit of 7 years, with the exception of the mitigated version provided for in Art. 250[18], paragraph 3 and Art. 251[19], paragraph 1, paragraph 2, in which the special minimum limit is one year and the maximum special limit is 5 years.

We also highlight the fact that the Romanian legislator indicates, in Art. 180[20], the meaning of the terms "cashless payment instrument" in paragraph 1, "electronic payment instrument" in paragraph 2, "electronic money" in paragraph 3, and "virtual currency" in paragraph 4.

The Romanian legislator in the Art. 180 of the Romanian Criminal Code defines the following terms, in accordance with the provisions of Directive (EU) 2019/713[21] of the European Parliament and of the Council of 17 April 2019 on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA.

The non-cash payment instrument, contained in the Art. 180 (1) of the Romanian Criminal Code represents "a device, an object or a record, protected, respectively protected, material or immaterial, respectively material or immaterial, or a combination thereof, other, respectively other than a currency with circulation value and which alone, respectively alone or together with a procedure or set of procedures, allows the holder or user to transfer money or monetary value, including by electronic currency or virtual currency".

According to the Art. 180 (2) of the Romanian Criminal Code, the electronic payment instrument means "an instrument that allows cash withdrawals, loading and unloading of an electronic money instrument, as well as fund transfers, other than those ordered and executed by financial institutions".

The paragraph 3 of the Art. 180 of the Romanian Criminal Code defines the notion of electronic currency, which means "the monetary value stored electronically, including magnetically, representing a claim on the issuer, issued

[18] The criminal offence of *"Making Fraudulent Financial Operations"* committed through the regulatory method of unauthorized transmission of identification data to another person in order to carry out the operations provided for in paragraph 1.

[19] The criminal offence of *"Acceptance of Financial Operations Carried Out Fraudulently"*.

[20] The article was amended by at. 1 point 1 of Law no. 207/2021, published in the Official Journal no. 720 of 22 July 2021.

[21] Directive (EU) 2019/713 on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA was publiashed in the Official Journal of the European Union, L 123/18 of 10 May 2019, available on the website: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019L0713&from=RO, retrieved at 22 December 2022.

upon receipt of funds for the purpose of carrying out payment operations and which is accepted by a person, other than the electronic currency issuer".

We point out that, paragraph 4 of the Art. 180 from the Romanian Criminal Code refers to the notion of virtual currency, which means "a digital representation of value that is not issued or guaranteed by a central bank or public authority, is not necessarily linked to a legally established currency and does not hold the legal status of currency or money, but is accepted by physical or legal persons as a medium of exchange and can be transferred, stored and traded electronically".

According to the Art. 2 (a) from the Directive (EU) 2019/713 „a non-cash payment instrument represents a non-corporeal or corporeal protected device, object or record, or a combination thereof, other than legal tender, and which, alone or in conjunction with a procedure or a set of procedures, enables the holder or user to transfer money or monetary value, including through digital means of exchange".

Considering the above definitions, we believe that a clear distinction should be made between virtual currency and electronic currency.

A virtual currency is "an unregulated form of money in digital format, which is not issued or guaranteed by a central bank and which can be used as a means of payment". The virtual currency is a digital representation of value that can be traded through digital systems and functions as a medium of exchange, and/or as a unit of account, and/or as a store of value, but which does not have a legal status of means of payment. We emphasize that the virtual currency is not issued or guaranteed by any jurisdiction, performing its functions only with the consent of the community of users of this type of currency.

At the level of the European Union, according to the provisions of the Art. 2 point 2 of Directive 2009/110/EC[22] on the taking up, pursuit and prudential supervision of the business of electronic money institutions, amended by the Directive 2015/2366[23] of 25 November 2015 on payment services in the internal market, electronic money represents "electronically, including magnetically, stored monetary value as represented by a claim on the issuer which is issued on receipt of funds for the purpose of making payment transactions and which is accepted by a natural or legal person other than the electronic money issuer"

Virtual currencies can be classified into several categories. They can be convertible or non-convertible[24]. Convertible virtual currencies have an equivalent value in real currency and can be exchanged. We can mention, as an example, several

[22] Directive 2009/110/EC of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC, Official Journal of the European Union, 10.10.2009, L 267/7, available on the website: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009L0110&from=RO retrieved at 22 December 2022.

[23] Directive 2015/2366 of 25 November 2015 on payment services in the internal market, electronic money amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, Official Journal of the European Union, 23.12.2015, L 337/35, available on the website: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri= CELEX:32015L2366&from=RO retrieved at 22 December 2022.

[24] Moise, Adrian Cristian; Stancu, Emilian (2017). *Criminalistica. Elemente metodologice de investigare a infracțiunilor. Curs universitar* [Forensics. Methodological elements for the investigation of crimes. Academic course]. Bucharest: Universul Juridic, pp. 88-89.

convertible currencies: Bitcoin, Second Life Linden Dollars and WebMoney.

Non-convertible virtual currencies are intended for a specific domain in the virtual world, such as online gambling, known as Massively Multiplayer Online Role-Playing Games (MMORPGs), or Amazon.com. Some examples of non-convertible virtual currencies include: Project Entropia Dollars; Q Coins; World of Warcraft Gold.

Romanian legislation in the field of cybercrime, including computer fraud, adapted to the provisions of the Council of Europe Convention on cybercrime as well as to the provisions of other legal instruments at the level of the European Union, such as, for example, Directive (EU) 2019/713 on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA, and the Directive 2013/40/EU[25] of the Parliament European and Council of 12th of August 2013 regarding attacks against computer systems[26].

Before analyzing another terms in the field of computer crime, we must emphasize the fact that Romanian legislation has adapted to the provisions of cybercrime at the European Union level, first in terms of the terminology used.

Thus, in the content of the Art. 181 of the Romanian Criminal Code, the notions of computer system and computer data are defined. The computer system represents "any device or set of devices interconnected or in a functional relationship, one or more of which ensures the automatic processing of data, with the help of a computer program". Computer data is "any representation of facts, information or concepts in a form that can be processed by a computer system".

According to the Art. 35 para. (1) (d) from Law no. 161/2003[27] regarding some measures to ensure transparency in the exercise of public dignities, public functions and in the business environment, preventing and sanctioning corruption, this category also includes any computer program that can determine the performance of a function by a computer system[28].

In the Art. 35 para. (1) from Law no. 161/2003 the following terms are defined: information traffic data represents "any computer data related to a communication carried out through a computer system and produced by it, which represents part of the communication chain, indicating the origin, destination, route, time, date, size, volume and duration of communication, as well as the type of service

[25] Directive 2013/40/EU of the European Parliament and of the Council of August 12, 2013 on attacks against information systems and replacing Framework Decision 2005/222/JHA of the Council was published in the Official Journal of the European Union L 218/8 of 14th of August 2013, available on the website: https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32013L0040&from=RO, retrieved at 22 December 2022.

[26] Moise, Adrian Cristian (2020), *Dimensiunea criminologică a criminalității din cybespațiu* [*The Criminological Dimension of Cybercrime*], second edition, Bucharest: C.H. Beck, p. 190.

[27] Published in the Romanian Official Gazette no. 279/21.03.2003.

[28] Mirișan, Valentin; Cîrmaciu, Diana, (2019). *Fighting money laundering in Romania*, in Ákos Farkas, Gerhard Dannecker, Judit Jacsó (eds.), *Criminal law aspects of the protection of the financial interests of the European Union with particular emphasis on the national legislation on tax fraud, corruption, money laundering and criminal compliance with reference to cybercrime*. Wolters Kluwer, Budapest, pp. 387-398.

used for communication"; the service provider represents "any natural or legal person that offers users the opportunity to communicate through computer systems, or any other natural or legal person that processes or stores computer data for the aforementioned persons and for the users of the services offered by them".

In the content of the Article 2 of the Directive 2013/40/EU on attacks against information systems and replacing Framework Decision 2005/222/JHA several definitions are presented, such as, for example, the notions of IT system and IT data. The computer system is defined as "a device or group of interconnected or similar devices, one or more of which ensures, through a program, the automatic processing of computer data, as well as the computer data stored, processed, recovered or transmitted by this device or group of devices in order to exploit, use, protect and maintain them". Also, computer data refers to "a representation of facts, information or concepts in a form suitable for processing in a computer system, including a program that allows a computer system to perform a function".

The Romanian legislator criminalized in the Article 249 of the Romanian Criminal Code, as amended by the Art. 2 of the Law no. 207/2021 for the amendment and supplementing of the Romanian Criminal Code, the offence of computer fraud as the act of causing patrimonial damage to a person by entering, transmitting, modifying or deleting computer data, by restricting access to computer data or by preventing in any way the operation of a computer system, in order to obtain a material benefit for oneself or for another, is punishable by imprisonment from 2 to 7 years. We are of the opinion that the purpose of the Art. 249 is to criminalize any act of unlawful manipulation in the processing of data with the intention of carrying out an illegal transfer of property, due to the development of information and communications technology and the opportunities to commit crimes against patrimony have also increased.

The action of entering computer data covers activities such as incorrect feeding of computer data into the computer, as well as manipulation of computer programs, and other acts affecting the integrity of computer data during data processing. We highlight that the criminal act that occurred must lead to economic losses[29].

The action of transmitting computer data covers all communications by electronic means, being covered all types of computer data transfers, whether by telephone, fax, or e-mail[30]. The action of transmitting computer data represents the novelty brought by the Law no. 207/2021.

The act of modifying computer data refers to the act of altering existing data, especially by installing destructive programs.

The action of deleting data means the action of removing data from the electronic storage devices.

---

[29] Savin, Andrej (2013). *EU Internet Law*. Cheltenham, Glos: Edward Elgar Publishing Limited, pp. 239-240.

[30] Shipley, Todd G.; Bowker, Art (2014). *Investigating Internet Crimes. An Introduction to Solving Crimes in Cyberspace*. Waltham, Massachusetts: Elsevier Inc., pp. 20-21.

The action of restricting access to this computer data involves the use of passwords or encryption keys for the content of this computer data.

The point 87 from the Explanatory Report of the Council of Europe Convention on Cybercrime[31] underlines that any form of interference with the operation of an IT system refers to the following activities, such as: tampering with hardware, activities that suppress a list of computer data printed by a printer, activities affecting the recording or flow of data or the order in which computer programmes operate.

We emphasize that the text of the crime of computer fraud contained in the Art. 249 of the Romanian Criminal Code, adapted to the provisions of the Art. 8, which refers to computer fraud, of the Council of Europe Convention on Cybercrime, the only normative modality that the text of the Art. 249 has in addition to the Art. 8 of the Convention is the modality of transmitting computer data.

3. Comparative presentation of the regulations of several countries in the European Union

In the Criminal Code of Greece, the legislator placed the criminal offence *"Computer Fraud"* in Chapter XXIV, with the marginal name "Offences Against Property", in Article 386A. The material element can be achieved through action and/or inaction capable of causing damage to another person, performing illegal activities that influence the digital (computer) data processing process. The regulatory methods of committing the act also result from the abstract content of the offence, such as those specific to the incorrect configuration of the electronic program, or the unauthorized use of data, or an unauthorized intervention on the computer system. We retain, in this case as well, the form of guilt as being the direct intention qualified by purpose, to acquire an undue pecuniary benefit. In Art. 13 of the Criminal Code, the legislator explains the terms "computer system" in letter h), and "digital data" in letter i).

In the Criminal Code of the Republic of Italy, Article 640-ter with the marginal name *"Computer Fraud"*, paragraph 1, we retain, as a material element of the misdemeanour, the illegal workmanship, regardless of the method used, which is able to influence the operation of a computer system through illegal intervention on the data or information or programs "contained in a computer system". The misdemeanour has an aggravated version, provided for in paragraph 2, sentence I, if the concrete method of committing it includes a circumstance to be found in Art. 640-bis at the misdemeanour of "Aggravated Fraud for the Achievement of Public Funds", and in sentence II, if the active subject is circumstantiated, by holding the capacity of "system operator". In the same sense, we highlight paragraph 3, where the version will be aggravated as a result of the fact that the actions and/or inactions meet the typical characteristics of theft or the digital identity data are used improperly. With reference to the punishment, we note that the legislator provided

[31] The Explanatory Report of the Convention of the Council of Europe on cybercrime point 87, available on the website: https://rm.coe. int/16800cce5b retrieved at 22 December 2022.

for cumulative punishments, namely, imprisonment and a fine. The special minimum limit is 6 months in the typical version, provided for in Art. 640-ter, par. 1, and the special maximum limit is 6 years, according to the provisions of Art. 640 par. 3, in the aggravated version. As regards the amount of the fine, it is a minimum of 51 euros in the typical version, and a maximum of 3000 euros according to Art. 640 par. 3, in the aggravated version.

In the same regulatory act, in Art. 640-quinquies, with the marginal name *"Computer Fraud of the Subject Certifying Electronic Signatures"*, the illegal action by which one does not meet the obligation provided by law in the procedure of issuing a qualified certificate, through which the electronic signature is certified, is criminalised. In this case, the active subject is circumstantiated by the capacity of operator who provides specific services in the electronic signature certification procedure. We also retain other constituent elements, such as: the form of guilt, the direct intention, qualified by purpose, in the first hypothesis, that of obtaining an undeserved benefit (regardless of whether it is for oneself or for another), and in the second hypothesis, causing harm/damages to others. In this case, the punishment is imprisonment for "up to three years, and a fine between 51 euros and 1,032 euros".

The criminal offence with the same marginal name "Computer Fraud" was placed by the German legislator in the Criminal Code of the Federal Republic of Germany in subsection 263a of section XII, with the marginal name "Deception and Abuse of Trust", to sanction according to paragraph 1, sentence I, the intentional conduct of a person who, through his/her action, influences the result of a data processing process. Alternative regulatory methods are stated in the abstract content, namely: incorrect configuration of the program, use of incorrect data, use of incomplete data. In sentence II, the fact of influencing the result of a data processing process takes place through the use of data, with the essential requirement related to the material element, that "the use should be unauthorized". From the analysis of the abstract content, thesis III emerges, in the hypothesis that the processing is influenced in any way. According to the legal rule, as it results from paragraph 2, in the case of committing the deed in its typical form (paragraph 1), the legal provisions will refer to subsection 263 par. 2-6, which provides attempts, and expressly states that they are punishable. We also note the provision in subsection 263 par. 3, which lays down particularly serious cases, and subsection 263 par. 5, which criminalises less serious cases. We also note the preventive nature of the legal rule in subsection 263a, aimed at punishing the person who prepares to commit an act provided for in the typical version, paragraph 1. The penalties provided for in the legal rule are different, depending on the version of the criminal offence. Thus, for the typical version (paragraph 1), the punishments are alternative, imprisonment of up to 5 years or a fine, while for the mitigated version provided for in paragraph 5, it is imprisonment of up to 3 years or a fine. In the case of a particularly serious case, the legislator provides only an imprisonment penalty, with a special minimum limit of 6 months and a special maximum limit of 10 years. By reference to subsection 263, par. 5, the penalty can have a special minimum limit of 1 year, or 6 months in less serious cases, and a special maximum limit of 10 years, or 5 years in less serious cases. If the existence of a deed provided for in subsection 263, par. 3, is proven

(preparation of a deed related to par.1, typical nature of the deed), and any of the situations provided for in subsection 149 par. 2, letter a), letter b) is retained, the person will not be punished. In order to retain any of the causes of non-punishment, one must refrain from committing the deed (act), either voluntarily or by voluntarily destroying/putting in a state of unusability the computer programs one owns in order to commit the deed provided for in paragraph 1. The cause of non-punishment will also apply if the perpetrator has tried to prevent the commission of the deed in a context where there is a danger that other people will continue the preparation of the deed or its commission, with the essential requirements that the actions that would lead to the avoidance of danger should be carried out voluntarily and seriously.

In the Criminal Code of the Republic of Estonia, in section 2 - "Offences Against Any Form of Property", in subsection 1 with the marginal name "Deception", the crime of "Computer Fraud" is placed in Art. 213, in two versions, the typical one (paragraph 1), and the aggravated one (paragraph 2). The material element of the objective side in the typical version can be achieved through at least one of the regulatory methods, as follows: the action of accessing computer programs or computer data; the action or/and inaction of modifying computer programs or computer data; deletion of computer programs or computer data; damage to computer programs or computer data; blocking of computer programs or computer data. We retain, as the form of guilt, direct intention, qualified by the purpose of obtaining pecuniary benefits. As for the active subject, we note that it is not circumstantiated in paragraph 1, whereas in paragraph 2, it is circumstantiated either by the fact that it committed, prior to the deed, another criminal offence among those expressly provided by the legislator in point, such as: theft, robbery, fraud, blackmail, embezzlement, or by another circumstance of the active subject, which results from point 2, namely that it has the capacity of an official, or from point 4, when the active subject is multiple, being made up of a group. The punishment provided by the law is, in paragraph 1, for the commission of the deed in the typical form, a fine or imprisonment of up to three years, and in the aggravated version, only the main punishment, of imprisonment from one to five years. The offence can also be committed by a legal entity, according to paragraph 3, in which case it is punishable only with a fine.

The computer fraud which refers to the Art. 8 of the Council of Europe Convention on cybercrime, is stipulated by the Article 323-3-1[32] of the French Criminal Code, in Title II Other crimes against property, Chapter III Crimes against automatic data processing systems, as well as in the Article 313-1 of Title I Fraudulent Loans, Chapter III Fraud and other similar crimes.

With regard to the United Kingdom of Great Britain cybercrime legislation, we remark that computer fraud offence is criminalized in the Articles 1-8 of the Fraud Act 2006[33].

[32] Le Service Public De La Diffusion Du Droit, French Criminal Code, Article 323-3-1, available on the website: http://www.legifrance. gouv.fr, retrieved on 22 December 2022.

[33] The Fraud Act 2006, available on the website: https://www.legislation.gov.uk/ukpga/2006/35/contents, retrieved on 22 December 2022.

According to the comparative law analysis thatwe presented, we noticed that all European countries have almost completely transposed the provisions of the Council of Europe Convention on computer crime into their domestic law. At the same time, we noted the existence of non-uniform criminal provisions and sanctions, which differ from one country to another.

4. The role of educational policies in the process of creating a cyber security culture

The goal of educational programs is to cause changes in terms of attitudes and behaviour, so that their capacities may evolve towards providing a beneficial environment for the social development of the child on multiple levels. According to social theory, each child has a unique development path, in relation to the parent, who has a set of unique characteristics and needs, dependent on the context in which he/she lives. The social context in which the child develops and forms his/her personality is dependent on external signals and other entities, such as the school with which the family interacts. To create an educationally effective set of skills, the most important element is the adjustment of content to the needs of those involved in the training process. The educational partnership should comprise: "the human resources of the education system, the students (pupils) included in the school units, the students' families, central and local governmental institutions, non-governmental organizations, religious institutions, economic operators, trade unions, local authorities"[34]. The focus should be on developing the school's partnership with the family.

The family environment is the first educational and socializing environment that the child knows, having an essential impact on his/her development as an individual. The child's bond with the family is extremely strong and indispensable. The family is the most suitable place for the beginning of the child's education and constitutes the first socializing component. It is here that the first socializing and educational level takes shape, the place where, having their parents as models and trainers, children begin to learn the lessons meant to prepare them for life. The influences of family education have long-term effects and are defining in the formation of a negative or positive general attitude.

4.1 The role of the teacher-parent-student "trio" in establishing the foundation for a cyber security culture

By stating the above, we bear in mind the concrete realities of the contemporary world, in which children are influenced by the virtual environment and cyber violence. Cyber-attacks and vulnerabilities related to the security of the online environment negatively influence a child's education and development. In the process of monitoring the cyber environment, an important role is played by the

[34] Rădulescu. E. Țârcă A. (2000), *Școala și comunitatea (School and the Community)*, Bucharest, Humanitas Publishing House, p. 40.

family, the school and the community. Thus, the "trio" consisting of teachers, parents, and the student could be the foundation on which to support early education in the process of building a culture of cyber security, which needs to be first consolidated and/or developed in parents and, subsequently, shared with the other members of the family.

The role of the family is important in a child's development from several points of view: physical, intellectual, emotional, and aesthetic. The main actors that help the child in perfecting his/her own education are the family and the school, to which we may add the community. Educational institutions, along with the family, have an impact, through the concrete conditions in which the educational process takes place, on the child's personality and evolution during the educational process. Various research studies have confirmed the elements mentioned in this introduction.

In Romania, the new national strategy[35] for the protection and promotion of children's rights over the period 2022-2027 has been approved.

A sociological study at national level, entitled "Child Abuse and Neglect" and carried out in 2018 by the "Save the Children" organization, shows the impact of aggressive behaviour on children and the effects of such behaviour[36]. Physical abuse may have physical, neurological consequences and may lead to illness, fractures, disabilities, even death. It also frequently leads to the development of aggressive behaviours, emotional and behavioural problems, and learning difficulties that diminish academic outcomes. Sustained emotional abuse, in particular, has long-term consequences on the child's development, mental health, behaviour and self-esteem. We may add to these forms of abuse the multitude of risks to be encountered in the virtual environment, which cultivate a feeling of insecurity.

Austrian theorist Alfred Adler was the first psychologist who presented the concept of anger as the opposite of the aggressive instinct and of an expression of violence. Thus, he stated that anger is a natural reaction of the body in situations of frustration and attack or violence. According to Adler, anger is not a biological reaction that occurs automatically and involuntarily. Anger is a phenomenon that has a cause and an effect. This hypothesis also creates a connection between anger and personality. The universal feeling of inferiority is manifested by certain people through anger, in order to show power. This situation begins in childhood, when one's life is dominated by helplessness and dependence. The overwhelming feeling of inferiority, maladjustment and insecurity created by the pressure exerted by the care-providing adult to achieve greater results than what the child is capable of achieving leads to the use of anger as a protective mechanism. Aggressive behaviour

[35] *National strategy for the protection and promotion of children's rights* "protected children, a safe Romania" 2022-2027, https://mfamilie.gov.ro/docs/20220506-PROIECT-HG-Anexa-nr.1.pdf, accessed on 19.12.2022.

[36] https://www.salvaticopiii.ro/sci-ro/files/a4/a4afa9be-8055-4320-b96b-ae9a0dda39fa.pdf, accessed on 17 December 2022.

is meant to intimidate the aggressor[37]. This is the context in which educational methods and policies aimed at familiarising adults with curricular areas and with the educational environment in which they have been introduced are carried out.

Researcher Karen Bierman, professor of psychology at Penn State University, together with her team, studied a group consisting of 350 preschoolers. Half of them followed a traditional curriculum. The other half underwent, in addition to the basic curriculum, educational programs regarding social and emotional aspects – known as REDI. The results were published in the November 2018 issue of the journal *Child Development*, and show that 70% of the children who followed the REDI program showed less disruptive behaviour, as compared to 56% of the children in a class with an ordinary curriculum. 12% of students undergoing the REDI program had difficulty concentrating on the work tasks, as compared to 21% of the regular students. As for the level of vocabulary development, 20% of students in the REDI program class showed outstanding results in national competitions, while only 15% of the students in the traditional program class achieved the same. What we may learn from the presentation of this research is that educational and prevention methods can also work in terms of limiting and preventing cyber attacks.

4.2 Educational policy for the hygiene of the cyber space

A smooth school-family relationship is a prerequisite for children to achieve optimal academic outcomes. When this relationship does not work, the educational process may turn out to be unsuccessful and the cooperation between the school and the family may suffer on various levels, as reflected in the school activity[38]. The barriers and difficulties that occur in this mechanism of cooperation between the family and the school stand in the way of an optimal development of relations between the two factors, thus influencing negatively the children's learning process. Among the factors that hinder the school-family relationship we may mention: *the subjectivity of the parents, the low educational level of some families, their own conception about education*. However, the threats that the online environment poses for children are well known, especially by means of the applications pertaining to the Android system, with which smartphones are equipped. There are studies regarding the harmful impact that mobile phone apps have on children's education.

For the past more than three decades, people have been interested in the digital component and in ways to integrate it in the educational environment. Research carried out in the United States over a period of 12 years by the representatives of the SRI International company, in the United States, has dismantled many of the classic views regarding digital education. The 93-page study was drawn up for the United States Department of Education and it demonstrates

[37] Allan, R. (2006), *Getting control of your anger*, New York, The McGraw-Hill Companies, p. 32.

[38] Povey J., Campbell A., Willis L.-D., Haynes M., Western M., Bennett S., Antrobus E., Pedde C. (2016), *Engaging Parents in Schools and Building Parent-School Partnerships: The Role of School and Parent Organisation Leadership*, „International Journal of Educational Research", Vol. 79, pp. 128-141.

that students who have been educated in the online environment have a higher success rate, as compared to those who have been educated in the classic-traditional environment. One of the team coordinators, quoted by Claudia Butaru[39], states that the report took into account a number of comparative studies regarding online education and traditional education (in the classroom) over the period 1996-2008. Some of the studies refer to education from nursery (kindergarten) to the twelfth grade, but most of them were carried out in colleges or in adult continuing education programs of various types, from medical training to in the military field. The report also states that online interaction must be protected and secured against cyber attacks. The analysis conducted for the United States Department of Education showed that, on average, students who took some or all of their courses online achieved a 59% pass rate on tests, as compared to the average pass rate of classroom students, which was 50%. It is a modest, but statistically significant, difference.

"The essential significance of the study lies in the fact that it demonstrates the role of online education today, not only that it is better in the absence of other options, but that it actually tends to be better than conventional instruction", said Barbara Means, coordinator of the study and educational psychologist within the SRI International company, in the United States of America. This does not mean that we will give up traditional classrooms, auditoriums and libraries. But the report does suggest that online education could expand greatly in the next years, as new options and coordinates regarding its importance develop. A few years ago, online education was little more than an electronic version of traditional correspondence courses. The situation has changed substantially with the emergence of video applications on the Internet, instant messaging and work tools in the internet and intranet networks.

The greatest growth in the near future, according to Phillip R. Regier's predictions, will be in the field continuing education programs. Currently, in the state of Arizona, there are several educational platforms available to students enrolled in continuing education programs, both for courses requiring physical attendance and online courses. Regier estimates that in three to five years this number could triple, the growth occurring almost entirely in online programs. Phillip Regier also believes that online education will continue to have an influence on the transformation of university campuses. Education systems, universities, as well as many schools that provide educational services from nursery/kindergarten to 12th grade, now use platforms and infrastructure for online education on a large scale, such as Blackboard or the open-source system Moodle. But these are mainly used for displaying topics, reading lists or timetables, as well as for organizing debates and forums dedicated to education. Regier believes that things will evolve quite quickly, being accelerated by the increased use of social networking technology. Students will increasingly help one another and learn from one another, according to the American researcher. For instance, in his opinion, the starting assumption will be that students know the basics of differential calculus, and the time spent in the classroom will be used to apply mathematics to real-world problems, perhaps to exploring the physics of climate change or identifying stock price trends in the stock market.

[39] Namely, Steve Lohr http://www.elearning.ro/educatia-online-intrece-educatia-din-sala-de-clasa-conform-unui-studiu, accessed on 19.12.2022.

The authors emphasise the need for constant cyber education[40], so that, in addition to early education based on cyber education and a costant interest shown by the entities providing education, and implicitly, the professional skills obtained following the attendance by young people of study programs in various educational cycles, cyber education should be part of adult education and improve the way in which adults spend their free time or carry out social activities. At the same time, we highlight the concerns of authors[41] who have formulated questions for reflection in their studies, such as: how, what and how much would a student preparing in the field of cyber security need to learn and whether it is ethical to train a student who, in the future, could use their professional skills unethically[42]; however, preparing students by finding answers to unexpected events remains a training method in the process of improving practical skills.

5. Conclusions

The prevention of criminal offences that can be committed by means of computer systems depends on each of us, all the more so if we relate our actions and/or inactions to the social roles that each person has in society.

Some elements that would contribute to building a cyber security culture are the process of preparing a regulatory act, the time interval in which the regulatory act is given its final shape, as well as the legislator's approach, which regulates social behaviours, shows the meaning of certain phrases that should be explained in the public space in order to be known, understood and well delineated, especially when new situations emerge, generating new behaviours that are tacitly accepted, and as technology evolves, as strategies at the European Union and/or national level change, as various bodies are operationalized, that are designated at the level of the Union or the national authority in order to respond, investigate or identify potential risks.

The integration in the curricula of study disciplines that contribute to the acquisition of transversal skills, depending on the field in which the students are trained, would contribute to the consolidation of the cyber security culture, by including the discipline of cyber education in the initial, professional or post-university training programs, as well as by including some disciplines from the field of law in the curricula of study programs that train students in other fields than law.

---

[40] Martti Lehto, *Cyber security capacity building – cyber security education in Finnish universities* in „Proceedings of the 19th European Conference on Cyber Warfare and Security", ECCWS202, p. 225, https://www.researchgate.net/publication/342643043_Cyber_security_capacity_building_-cyber_security_education_in_Finnish_universities_Cyber_security_capacity_building_-cyber_security_education_in_Finnish_universities.

[41] Price, B.A.; Janicke, H.; Lallie, H.S.; Sinclair, J.E.; Joy, M.S. and Howley, R. (2014). *Pedagogic Challenges in Teaching Cyber Security – a UK perspective.* In: Venugopal, K.R. and Lingareddy, S.C (eds.), *ICC 2014 - Computer Networks and Security*, Elsevier, p. 612, https://oro.open.ac.uk/43610/, accessed on 19.12.2022.

[42] Ibid.

Bibliography

I. Books and articles

1. Allan, R. (2006), *Getting control of your anger*, New York, The McGraw-Hill Companies.
2. Daniela-Cristina Creț (2021), *Defending family law values via criminal law norms,* in „Agora International Journal of Juridical Sciences", Vol. 15, No. 2, 2021, DOI: https://doi.org/10.15837/aijjs.v15i2.4654.
3. Elena-Ana Iancu (2019)**,** *The Contribution of Forensic Science to Establishing the Truth in Criminal Proceedings* in „Athens Journal of Law", Volume 5, Issue 4, 2019-pp.1-2, DOI: https://doi.org/10.30958/ajl.5-4-6.
4. Iulia Boghirnea, *The Creation of the General Legal Norm*, „Annales Universitatis Apulensis, Series Jurisprudentia", no. 11/ 2008, pp. 28-38, https://journals.uab.ro/ index.php/auaj/.
5. Martti Lehto, *Cyber security capacity building – cyber security education in Finnish universities* in „Proceedings of the 19th European Conference on Cyber Warfare and Security", ECCWS202, https://www.researchgate.net/publication/342643043_Cyber _security_capacity_building_-cyber_security_education_in_Finnish_universities_Cy ber_security_capacity_building_-cyber_security_ education_in_Finnish_universities.
6. Mirișan, Valentin; Cîrmaciu, Diana, (2019). *Fighting money laundering in Romania*, in Ákos Farkas, Gerhard Dannecker, Judit Jacsó (eds.), *Criminal law aspects of the protection of the financial interests of the European Union with particular emphasis on the national legislation on tax fraud, corruption, money laundering and criminal compliance with reference to cybercrime*. Wolters Kluwer, Budapest, pp. 387-398.
7. Moise, Adrian Cristian (2020), *Dimensiunea criminologică a criminalității din cybespațiu* [*The Criminological Dimension of Cybercrime*], second edition, Bucharest: C.H. Beck.
8. Moise, Adrian Cristian; Stancu, Emilian (2017). *Criminalistica. Elemente metodologice de investigare a infracțiunilor. Curs universitar* [Forensics. Methodological elements for the investigation of crimes. Academic course]. Bucharest: Universul Juridic.
9. Molly K. Land and Jay D. Aronson, *Human Rights and Technology: New Challenges for Justice and Accountability* in „Annual Review of Law and Social Science", 2020, 16:1, 223-240, https://www.annual reviews.org/doi/pdf/10.1146/annurev-lawsocsci-0602 20-081955, accessed on 20.12.2022.
10. Povey J., Campbell A., Willis L.-D., Haynes M., Western M., Bennett S., Antrobus E., Pedde C. (2016), *Engaging Parents in Schools and Building Parent-School Partnerships: The Role of School and Parent Organisation Leadership*, „International Journal of Educational Research", Vol. 79, pp. 128-141.
11. Price, B.A.; Janicke, H.; Lallie, H.S.; Sinclair, J.E.; Joy, M.S. and Howley, R. (2014). Pedagogic Challenges in Teaching Cyber Security – a UK perspective. In: Venugopal, K.R. and Lingareddy, S.C (eds.), *ICC 2014 - Computer Networks and Security*, Elsevier, https://oro.open.ac.uk/43610/, accessed on 19.12.2022.
12. Rădulescu. E. Țârcă A. (2000), *Școala și comunitatea (School and the Community)*, Bucharest, Humanitas Publishing House.
13. Savin, Andrej (2013). *EU Internet Law*. Cheltenham, Glos: Edward Elgar Publishing Limited.
14. Shipley, Todd G.; Bowker, Art (2014). *Investigating Internet Crimes. An Introduction to Solving Crimes in Cyberspace*. Waltham, Massachusetts: Elsevier Inc.

II. Legislation

1. Law no. 51/1991, republished, on the national security of Romania, published in the Official Journal no. 190 of 18 March 2014.
2. Law no. 135/2010 Criminal Procedure Code, published in the Official Journal no. 486 of 15 July 2010, in force as of 1st February 2014.
3. Law no. 286/2009 Criminal Code, published in the Official Journal no. 510 of 24 July 2009, in force as of 1st February 2014.
4. Government Decision (H.G) no. 877/2018 on Romania's National Sustainable Development Strategy 2030, published in the Official Journal no. 985 of 21 November 2018.
5. Romania's Security Strategy for the period 2022-2027, published in the Official Journal no. 2 bis of 3 January 2022.
6. Government Decision (H.G) no. 217 of 15 May 2013 approving Romania's Cybersecurity Strategy and the National Action Plan for the Implementation of the National Cybersecurity System, published in the Official Journal no. 296 of 23 May 2013.
7. Directive (EU) 2019/713 on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA was publiashed in the Official Journal of the European Union, L 123/18 of 10 May 2019, available on the website: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019L0713&from=RO.
8. Directive 2009/110/EC of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC, Official Journal of the European Union, 10.10.2009, L 267/7, available on the website: https://eur-lex. europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009L0110&from=RO, retrieved at 22 December 2022.
9. Directive 2015/2366 of 25 November 2015 on payment services in the internal market, electronic money amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No. 1093/2010, and repealing Directive 2007/64/EC, Official Journal of the European Union, 23.12.2015, L 337/35, available on the website: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L2366&from=RO, retrieved at 22 December 2022.
10. Directive 2013/40/EU of the European Parliament and of the Council of August 12, 2013 on attacks against information systems and replacing Framework Decision 2005/222/JHA of the Council was published in the Official Journal of the European Union L 218/8 of 14th of August 2013, available on the website: https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32013L0040&from=RO, retrieved at 22 December 2022.
11. German Criminal Code, Section 263a, available on the website: http://www.gesetze-im-internet.de/englisch_ stgb/german_criminal_code.pdf, retrieved at 22 December 2022.
12. French Criminal Code, Article 323-3-1, available on the website: http://www.legifrance.gouv.fr, retrieved at 22 December 2022.
13. The Fraud Act 2006, available on the website: https://www.legislation.gov.uk/ukpga/2006/35/contents, retrieved at 22 December 2022.
14. The Romanian Criminal Code.
15. Law no. 207/2021 for the amendment and supplementing of the Romanian Criminal Code.