ACROSS
www.across-journal.com
ISSN 2602-1463
Vol. 7 (5) 2023 Cross-border Laws and Regulations

https://doi.org/10.5281/zenodo.8037276

REFLECTIONS ON INFORMATIC CRIME IN THE REPUBLIC OF MOLDOVA

Andrei NASTAS
"Dunarea de Jos" University of Galati, Romania
Institute of Legal, Political and Sociological Research

Sergiu CERNOMOREȚ
State University of Physical Education and Sports, Chisinau, Republic of Moldova
Institute of Legal, Political, and Sociological Research
"Dunarea de Jos" University of Galati, Romania

Anatolie FAIGHER
"Alecu Russo" State University of Balti, Republic of Moldova

Abstract
The evolution of the socio-economic sphere inevitably generates changes in the criminal phenomenon, in this sense, the Republic of Moldova is not an exception. In recent years, there has been a growing spread of cybercrime. In addition, a number of crimes involve the increasing use of information technology in crime.

The examination of the concept and features of cybercrime and of the incriminating juridical-criminal means destined to fight this phenomenon, represents an urgent necessity, of a special topicality.

The latent character and the complexity of the IT operations determine the connection of the legal and organizational-institutional basis, destined to the social control of the IT crimes. In this sense, we propose the examination of cybercrime in terms of the specific legislative and organizational-institutional of the Republic of Moldova.

Keywords: computer science, access, computer fruit, computer forgery, information, computer security

INTRODUCTION

Virtual space has become an integral and indispensable part of world society and economy. The context in which, in the Republic of Moldova, crime, as a whole, is correlated with cyberspace, which is manifested by the increasing use of information

ISSN 2602-1463
Vol. 7 (5) 2023 Cross-border Laws and Regulations

technology or for committing crimes.

The context in which according to the Decision of the Parliament of the Republic of Moldova no. 257 of 22.11.2018, computer fraud, computer attacks, electronic payment fraud, and child pornography on the global Internet are types of crimes that require specialized investigations, proper training and equipment of law enforcement agencies. Cybercrime is a criminal phenomenon that in turn fuels many risks and crises in cyberspace, and the prevention and combating of cybercrime must be a major concern of all actors involved, especially at the institutional level, where the responsibility for development is concentrated. and the implementation of coherent policies in the field.[1]

We do not subscribe to the opinion expressed by S. Purici, that the legislation of the states of the world is constantly changing due to the accelerated development of information technology, and international cooperation is faced with a continuous challenge produced by the increase of transnational cybercrime. We note the combined effort of states to harmonize their legislation in order to combat the phenomenon in question, but the results are only satisfactory and it will not be possible to talk about eradicating the phenomenon.[2]

METHODOLOGY

The complex nature of cybercrime has led to the need to use a set of ideas, theories, general and special methods of a cognitive nature, especially: comparative, historical, systemic, statistical, and logical (method of deduction, induction, analysis, synthesis, etc.). Also, starting from the latent nature of cybercrime, but also the lack of a uniform judicial practice in the Republic of Moldova, we proceeded to examine the statistical data, complaints, denunciations and findings regarding the commission of cybercrimes, activity reports and reports of the prosecuting authorities. of the Ministry of Internal Affairs of the Republic of Moldova during the years 2017-2021, served as a source for identifying the main ways of committing cybercrime. Legislative provisions, statistical data, criminal policies have been filtered through the doctrinal opinions of the authors of scientific papers in the field.

RESULTS

The provisions of the Council of Europe Convention on Cybercrime[3] were ratified by the Republic of Moldova on February 2, 2009.[4]

ISSN 2602-1463
Vol. 7 (5) 2023 Cross-border Laws and Regulations

With reference to the legal framework of the Republic of Moldova, we mention that the adoption of the Criminal Code of the Republic of Moldova (2002) established the legal basis of criminal liability for cybercrime. Which along the way assessed significantly, correlated with social realities, dictated by the need to ensure legal and criminal protection of social values and relations. Thus, the legislative headquarters of the facts for which criminal liability is established in the IT sphere is within the chapter. XI Criminal Code of the Republic of Moldova, entitled - "Computer Crimes and other crimes in the Field of Telecommunications". With direct reference to cybercrimes, they are entitled as follows:

- Article 259 of the Criminal Code of the Republic of Moldova - Illegal access to computerized information;
- Article 260 Criminal Code of the Republic of Moldova - Illegal production, import, marketing or provision of technical means or program products;
- Article 2601 of the Criminal Code of the Republic of Moldova - Illegal interception of a computer data transmission;
- Article 2602 of the Criminal Code of the Republic of Moldova - Alteration of the integrity of computer data kept in a computer system;
- Article 2603 of the Criminal Code of the Republic of Moldova - Disruption of the functioning of the information system;
- Article 2604 Criminal Code of the Republic of Moldova - Illegal production, import, marketing or provision of passwords, access codes or similar data;
- Article 2605 of the Criminal Code of the Republic of Moldova - False information technology;
- Article 2606 Criminal Code of the Republic of Moldova - Computer fraud;
- Article 261 Criminal Code of the Republic of Moldova - Violation of security rules of the information system.

Although criminal liability is expressly prescribed by the above list, we consider that it cannot be considered as exhaustive. The reason is simple - cybercrime is not limited to cybercrime. In this regard, a number of criminal components of the Criminal Code of the Republic of Moldova contain signs that allow the use of virtual space for committing crimes. In the context in which, at the present stage, there is no unanimously accepted definition of the notion of “cybercrime”, the attempts to define it are multiple, which is due to the complexity and magnitude of the phenomenon. The national extra-criminal legal framework itself does not contain a definition of cybercrime - Law no. 20 of 03.02.2009, regarding the prevention and fight against cybercrime,[5] establishing only the institutional principles and the vectors of activity

ISSN 2602-1463
Vol. 7 (5) 2023 Cross-border Laws and Regulations

in this respect. The definition of the term cybercrime has been the basis of many round tables, seminars, conferences, organized at European and global levels, as its fight is both a national and an international issue.

The concept of information security of the Republic of Moldova, approved by Law no. 299/2017[5], represents the basic document for the elaboration of the Information Security Strategy of the Republic of Moldova for the years 2019–2024 and the policy document that integrates the central fields and associated with the information space, which provides notions, defines the principles of organization at state, society and individual level. as well as details the legal, technical-organizational, economic and counter-information methods for ensuring the information security of the Republic of Moldova. Obviously, we cannot equate the notions of computer security with information security.

In defining the concept of information security of the Republic of Moldova, the legislator also referred to cybercrime, as follows - "the concept of information security of the Republic of Moldova, is determined by the need to protect the interests of the state, society and person, vital and important objectives strategy for national security, the need to ensure the protection of information attributed to state secrecy, as well as the need to prevent and combat cybercrime ".

The lack of the concept of cybercrime is not an exclusive and unique problem, or from a legal point of view, the interpretation of criminal and extra-criminal signs encounters major divergences, both in criminal doctrine and in judicial practice. Which imposes the need to systematize and standardize the doctrine and judicial practice of the Republic of Moldova.

Following the analysis of national legislation in the field of preventing and combating cybercrime, a number of barriers and regulatory gaps at the national level were found, including:

1) in the Criminal Code of the Republic of Moldova no. 985/2002, namely:

a) Article 178 CpRM, "Violation of the right to secrecy of correspondence", does not provide for criminal liability for acts committed in respect of electronic correspondence (messaging), as the notion of "postal items", according to the Postal Communications Law no. 36/2016, provides only the physical goods sent and received;

ISSN 2602-1463
Vol. 7 (5) 2023 Cross-border Laws and Regulations

b) Article 2081 of the Code on Child Pornography does not criminalize knowingly gaining access to child pornography through information and communication technologies, although this is enshrined in the Council of Europe Convention for the Protection of Children against Sexual Exploitation and Abuse sexual harassment, concluded in Lanzarote on October 25, 2007, and ratified by Law no. 263/2011;
c) most of the offenses provided for in Chapter XI of the special part of the Code, "Computer offenses and offenses in the field of telecommunications", have a material composition and are consumed only when causing a large amount of damage;

2) in the Code of Criminal Procedure of the Republic of Moldova no. 122/2003, namely:

(a) the procedure of the "computer search" provided for in the Council of Europe Convention on Cybercrime, adopted in Budapest on 23 November 2001, is not regulated;
b) the special measure of computer data interception investigations is missing;
c) the legal framework does not allow the performance of special investigative measures necessary for the documentation of computer crimes;

d) no restriction on access to the web pages, including those hosted by the provider, containing information that endangers the life, health and normal development of children, information promoting war or terrorism, urges hatred or national, racial or religious discrimination, hostility or violence ".[6]

Cybercrime in the sense of criminal law does not identify with the same concept in the criminological sense, the latter being broader in content. In essence, the concept of cybercrime, in our opinion, should include all the crimes in which the purpose, methods, means or place of the crime are, as the case may be: information itself, virtual environment, computer system/network or technologies. informational.

From the point of view of criminology, the concept of cybercrime involves placing emphasis in particular on the legitimacy and trends of the phenomenon of cybercrime. Among this, we mention: the rise of cybercrime in the context of economic crime (the former is the means of committing an economic crime), against the background of the decrease in the number of economic crimes (although their magnitude is not directly proportional to the damage caused). The confirmation of the statements can serve the so-called case of "Theft of the Billion in the Republic of Moldova", some elements of which were established by the Kroll report. At the same time, there is a trend

ISSN 2602-1463
Vol. 7 (5) 2023 Cross-border Laws and Regulations

diametrically opposed to the one exposed - the lack of specialization of perpetrators in the field of information technology and the orientation of "criminal attention" to individuals, individuals, as victims of cybercrime (eloquent example, in this sense, would serve situations the case of crooks who present themselves in virtual space as representatives of banks, which serve victims and obtain pin-codes from bank accounts, break them).

Cybercrime is characterized by a high degree of latency. This is due to the differentiation and confidentiality (encryption) of information (drawings, graphics, videos, images, sounds, etc.). In this regard, it is worth listing the methods and techniques used to facilitate the commission of cybercrime:

1) means of anonymisation (which hide technical data identifying the user), wireless access points with unrestricted (open) access to the global Internet in public places;
2) the use of complex asymmetric algorithms for encrypting critical information when extorting financial means through information technologies;
3) the use of decentralized electronic payment systems based on crypto-algorithms (cryptocurrency);
4) networks for direct data exchange between users, which does not leave certain traces of activity in the content of the history recorded in the computer system or in the logs held by service providers;

5) the use of web hosting by criminals;
6) small service providers do not ensure a minimum level of cyber security of their own network and often do not keep track of service users, nor do they record metadata regarding access to the Internet;
7) fixed Internet services provided on the territory of the Republic of Moldova which is not effectively controlled by the constitutional authorities ”.[7]

Examining the judicial practice and starting from the reasons for committing cybercrime, we could divide their perpetrators into the following groups:

• the perpetrators of the crime acting out of interest / mobile material (committing computer crimes aims at the acquisition of other people's property, most often - financial resources from the electronic or bank accounts of the victims); An eloquent example from the judicial practice of the Republic of Moldova would be the criminal case in which CK, by prior agreement and with another person, a citizen of the Republic of Bulgaria and the defendants DV and DM, acting as a member of the

ISSN 2602-1463
Vol. 7 (5) 2023 Cross-border Laws and Regulations

organized criminal group, being on the territory of the Republic of Moldova, being in possession of the technical means designed and adapted, of “skimmer” type, when copying information from bank cards, which was previously illegally imported into the Republic of Moldova on July 11, 2014 in order to commit the offenses provided by art. art. 237, 259 CP RM, not being authorized under the law, pursuing the purpose of collecting information from bank cards for later use in the manufacture of bank cards with which they were to be stolen, financial sources, having a well-structured plan, between 13-15 July 2014, they illegally installed the technical means of “skimmer” type on the ATM no. 1, which belongs to BC “Energbank” SA, located at address x, illegally accessed the information on the bank cards of 158 users, which they copied, on a device for storing information.[8]

• the perpetrators of the crime acting for reasons of (self) confirmation (the desire to demonstrate to themselves or others their abilities/skills/knowledge in the field of information technology) An eloquent example of the judicial practice of the Republic of Moldova would serve the criminal case, according to which 2012-2018, ME, acting intentionally, initially carrying out the criminal activity on its own, subsequently, starting with 2015, by mutual agreement and by prior agreement with TA, starting with 2017, with CI and with TA, through computer systems connected to the global Internet network, using a series of usernames on the Internet, including: "JekaProf", "Procryptgroup", "karabulut", the accounts in the Jabber e-mail application - procryptgroup @ jabbim.pl, procryptgroup@exploit.im, ragnar78 @ exploit. im, encryption of "Smoke", "Aegis" and other files, being registered on online platforms (global Internet pages and forums) with limited access, specialized and intended for the exchange of information on illegal hacking activities ", Which involves the illegal activity of compromising the security of networks and computer systems with subsequent infiltration into other people's computers, including: https://forum.zloy.bz; https://forum.antichat.ru; https://forum.exploit.in, https://cryptor.biz, placing various advertisements on the mentioned platforms, offered services of production, marketing and making available, in any other form, illegally, the program products designed and adapted by ME and TA, for the purpose of committing by third parties, including from outside the Republic of Moldova, including persons not identified with the pseudonyms - "none_1" and "no-name", the offenses of illegal access to computer information, forgery and computer fraud, manifested, according to the notification of the Federal Bureau of Investigation (FBI) of the United States Department of Justice, by illegally accessing the bank accounts 3 of the companies based in the United States and stealing money from the given accounts.[9]

ISSN 2602-1463
Vol. 7 (5) 2023 Cross-border Laws and Regulations

• the perpetrators of the crime who act for reasons of jealousy, booling, envy or conflict, etc .; An example would be: J.A. committed the act of computer forgery, in the following circumstances, on July 26, 2015, in the time interval from 15.42 to 18.53, being at his home in t. X, being in conflicting relations with cet. P.P., as well as being opponents in the civil case no. Ch. Examined by the Buiucani District Court, Chisinau municipality, with the intention of violating the right to secrecy of correspondence, using computer systems with IP address: X, managed by the company "Moldtelecom" SA, assigned to the domicile of J.A. and with the IP address: X, managed by the company "Moldcell" SA, assigned to the computer system belonging to J.A. by unestablished methods and fraudulently obtaining the password, he accessed illegally and without the consent of P.P the mailboxes: X@gmail.com and X@yahoo.com, which belong to cet. PP, changed the access password to the respective mailboxes, thereby restricting the latter's access to the mailboxes, as well as illegally deleting the computer data kept by the latter, resulting in data untrue, actions taken to be used to examine the dispute civil between cet. P.P. and cet. J.A.[10]

• perpetrators of the crime who act for sexual reasons (dissemination, storage, sale of pornography, including child pornography) Example - N.E., in the period between 02.04.2019 - 03.11.2019, being at his home located in x, acting with the sole intention of downloading, viewing and holding photo / video images or other representations of one or more children engaged in explicit, real or simulated sexual activities, images or other representations of a child's sexual organs, lasciviously or obscenely using the "Lenovo S / N PF128VF2" laptop and the "Redmi Note 7" mobile phone with IMEI 1: z and IMEI 2: q, and the Internet with IP address: w, intended through the specialized program "BitTorrent", based on the principle of "peer-to-peer" copied, used and distributed -163 graphic and video files, 2 with child pornography content, which according to the database specialized in identifying victims of child pornography, Child abuse and sexual exploitation "ICSE" administered by the Interpol ICPO and the international police database "GRIDCOP" is child pornography;[11]

The complaints and denunciations examined indicate the fact that the activity of victimological prevention of cybercrime is focused on the following prohibitions, related to the rules of computer security, among which we mention:

• Copying and accessing computer products/programs from untrue sources of the Internet; examination, the opening of failures, including by e-mail, from unknown, dubious persons;
• Communication through social networks with strangers, who in reality may be

ISSN 2602-1463
Vol. 7 (5) 2023 Cross-border Laws and Regulations

crooks, recruits of sectarian/terrorist organizations
• Placing information on communication platforms / personal pages of information on identity data, lifestyle, income, occupation, business trips, etc .;
• Transmission online, to third parties of personal identity data (Name, surname, patronymic, year of birth, identity number, etc.) or bank data/accounts, passwords, from various pretexts;
• Carrying out internet-banking transactions, without confirming the correct address of the personal office or in the situation of requests on standard procedures;
• Use simple passwords, which are either the phone number, the year of birth or other data, which can be easily deduced/guessed
For these reasons, the emphasis on law enforcement should be based on the findings set out in the literature - "many crimes occur today on social networks and data in the networks are a combination of text and images, so a hybrid method for crime detection is suggested "[12].

CONCLUSIONS

The Republic of Moldova has a legal basis for preventing and combating by legal means the forms of manifestation of cybercrime. The basic and direct task in its prevention is the prerogative of the state security bodies to maintain public order and criminal investigation. In this sense, we consider that the lack of a uniform judicial practice, but also of the reduced number of registered/discovered computer crimes represent deficiencies in the activity of the bodies meant to prevent and fight this type of crime. The solution would be to examine the experience and good practices of European Union countries in preventing and combating cybercrime

REFERENCES

1) Hotărîrea Parlamentului Republici Moldova nr. 257 din 22.11.2018, p**rivind aprobarea strategiei securității informaționale a Republicii Moldova pentru anii 2019–2024 și a Planului de acțiuni pentru implementarea acesteia.** Pct. 33 la Anexa nr. 1 https://www.legis.md/cautare/getResults?doc_id=111979&lang=ro
2) S. Purici. "*Bune practice internaionale cu privire la investigarea infracțiunilor informatice*", *Studia Universitatis Moldaviae*, 2015, nr. 3(83), pp. 162-166
3) https://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf
4) Legea **pentru ratificarea Convenţiei Consiliului Europei privind criminalitatea informatică,** nr. 06 din 02.02.2009, Monitorul Oficial al Republicii Moldova, 2009, nr.37-40
5) Legea privind prevevenirea și combaterea criminalității informatice, nr. 20 din 03.02.2009,

ISSN 2602-1463
Vol. 7 (5) 2023 Cross-border Laws and Regulations

https://www.legis.md/cautare/getResults?doc_id=124978&lang=ro#
6) Legea **privind aprobarea Concepţiei securităţii informaţionale a Republicii Moldova,** nr. 299/2017 https://www.legis.md/cautare/getResults?doc_id=105660&lang=ro
7) Project Tenor II Summary Report, 10.12.2017, prepared for The National Bank of Moldova, https://www.bnm.md/files/Kroll_%20Summary%20Report.pdf
8) Dosar penal nr. 1ra-87/2016, http://jurisprudenta.csj.md/search_col_penal.php?id=6000
9) Dosar penal nr. 1ra-1284/2020, http://jurisprudenta.csj.md/search_col_penal.php?id=16249
10) Dosar penal nr. 1ra-445/2019, http://jurisprudenta.csj.md/search_col_penal.php?id=13789
11) Dosar penal nr. 1ra-706/2021, http://jurisprudenta.csj.md/search_col_penal.php?id=19440
12) A. Karimi, S. Abbasabadei, J. A. Torkestani, F. Zarafshan, *"Cybercrime Detection Using Semi-Supervised Neural Network",* Computer Science Journal of Moldova, vol.29, no.2 (86), 2021 pp. 176 https://ibn.idsi.md/sites/default/files/imag_file/155-183.pdf