CYBERSECURITY AND CYBERCRIME: CHALLENGES OF AN INVISIBLE SPACE

Lecturer **Felicia BEJAN**[1]

Abstract

The cyberspace is the new environment where a significant part of our social interconnections take place. To say that the future belongs to virtual space it's not a figure of speech at all. Consequently, the modern security concept includes a cybersecurity dimension. The cyberspace comes into our lives with a lot of advantages, but also with numerous vulnerabilities. The policy makers and the legislative systems around the world reacted with a sufficient delay to the rapid developments in the cyberspace, and still the reality online is one step ahead of the society's reaction. Similarly, to the relationships performed in the physical space, the relationships taking place in the cyberspace have to be organized through legal rules with the goal of ensuring a safe juridical life for each participant to this virtual legal circuit. The transition from traditional laws to ones addressed to virtual space is challenging for all the actors involved in this process, from international community, states, experts, legislators, administrative authorities and judicial institutions to corporations and individuals. The main threat is represented by cybercrimes. The cybersecurity and the law behind it, together with all the regulations having as goal to prohibit and sanction the criminal behaviour committed in the cyberspace are strongly interrelated. The aim of our study is to analyse the legal regime of preventing and combating cybercrime and the legal aspects of cybersecurity, to examine the level of protection ensured through current laws and to propose improvements to the existing legislative framework.

Keywords: *cybersecurity, cybercrime, the Network and Information Security (NIS) Directive digital age, law.*

JEL Classification: K10

1. Introduction

The cyberspace is the new dimension in which we live and carry out our activities. Consequently, an important part of our social relationships takes place in this environment. Obviously, the law must follow this new reality, as the legal relationships are social relations regulated through legal rules and a part of our juridical life moved to online.

The adaptation is a major challenge for the international community as well for each state, for their legislative, administrative and juridical authorities[2]. Important steps have already been taken, but there is much more to be done in order to achieve the cybersecurity imperatives, in the benefit of our rights.

As a matter of growing need, cyber law is becoming highly significant in the international and Romanian legal framework, a strong legal basis is an essential necessity to continuingly prevent and combat the illegal act in domain and to protect us, as a society and as individuals, as well.

2. Cybercrime: international and national legal regime

The need for a proper legislation to establish an efficient framework and to enforce control over the issue of cybercrimes was of particular concern for all the public and private players involved or affected by this phenomenon.

Hence, the importance and the emergency for legal protection of life in the cyberspace has forced international actors to adopt the first significant international treaty in the field, "necessary to deter action directed against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data by providing for the

[1] Felicia Bejan – Faculty for Political Sciences, University of Bucharest, Romania**,** felicia.bejan@unibuc.ro.

[2] See Cristina Elena Popa Tache, *Administrative Review and Reform Movements from the Perspective of International Investment Law*, in Julien Cazala, Velimir Zivkovic (editors), *Administrative Law and Public Administration in the Global Social System, (Contributions to the 3rd International Conference. Contemporary Challenges in Administrative Law from an Interdisciplinary Perspective, October 9, 2020)*, ADJURIS – International Academic Publisher, 2020, pp. 212- 217.

criminalisation of such conduct"[3], the Council of Europe's Budapest Convention on Cybercrime[4].

Under the Chapter II, Section 1 concerning the measures to be adopted at the national level[5], the Cybercrime Convention states that the offences to be criminalised through the domestic substantive criminal law by the parties of the international treaty are:

- the offences against the confidentiality, integrity and availability of computer data and systems**,** specifically illegal access, illegal interception, data interference, system interference, misuse of devices;
- computer-related offences, namely computer-related forgery, computer-related fraud;
- content-related offences and the offences related to child pornography;
- offences related to infringements of copyright and related rights.[6]

As a *sine qua non* condition for efficiently preventing, investigating, combating and sanctioning of the cybercrimes at the national and international level, the Budapest treaty emphasizes the need for mutual assistance and cooperation between states in the sphere of criminal offences in the cyberspace The provisions of the Chapter III on International Cooperation especially provides the principles governing the cooperation between the parties, respectively the general principles relating to international co-operation, of the principles relating to extradition and of the principles relating to mutual assistance. [7]

Recently, the Cybercrime Convention Committee has undertaken a results-oriented monitoring report, "The Budapest Convention on Cybercrime:benefits and impact in practice". The report's conclusions were optimistic as regards the positive impact of the treaty on the domestic legislation, the achieving of networks of practitioners able to cooperate efficiently, the improvement of the collaboration with public and private entities and the extending of the international cooperation.[8]

Romania signed the Cybercrime Convention in 2001 and, as a party to the convention, implemented it into the Romanian legislative system before its ratification in 2004, through the Title III entitled Prevention and combating cybercrime of the Law 161/2003[9], regulating "the prevention and fighting of cyber-crime, by specific measures to prevent, discover and sanction the infringements through the computer systems, providing the observance of the human rights and the protection of personal data".[10]

Thus, by the provisions of the said title[11], the Romanian criminal substantive law prohibited and penalized:

- the offences against the confidentiality and integrity of data and computer systems;
- computer-related offence and
- child pornography through computer systems.

Subsequently, the New Criminal Code[12] and the New Criminal Procedure Code[13] , entered into force 1 February 2014, have taken over substantive and procedural provisions in the field. Thus,

---

[3] Preamble of the Cybercrime Convention. p. 1.

[4] Adopted by the Committee of Ministers of the Council of Europe on 8 November 2001, opened for signature in Budapest, on 23 November 2001 and entered into force on 1 July 2004.

[5] Cybercrime Convention, Council of Europe, 2001, Budapest, p. 5-6.

[6] The classification of cybercrimes is not unitary. For example, according to the 2013 United Nations Office on Drugs and Crime, *Draft Comprehensive Study on Cybercrime*, cybercrimes can be: Acts against the confidentiality, integrity and availability of computer data or systems, Computer-related acts for personal or financial gain or harm, Computer content-related acts.

[7] Convention On Cybercrime, Council of Europe, 2001, Budapest, p. 12-13.

[8] *The Budapest Convention on Cybercrime:benefits and impact in practice*, Cybercrime Convention Committee, Council of Europe, 2020, p. 44.

[9] Published in the Romanian Official Monitor no. 279/2003. The Law 161/2003 is a normative act which is not dedicated to the regulation of cybercrimes. Also, Romania ratified the Additional Protocol concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems in 2009.

[10] Article 34 of the Law 161/2003.

[11] Article 42- 47, Article 48-50 and Article 51 of the Law 161/2003.To illustrate, the mentioned articles criminalized illegal access to a computer system; illegal interception of any transmission of computer data; illegal alteration, deletion or deterioration of computer data of the access restriction to such data; unauthorized data transfer from a computer system serious hindering, without right, of a computer system operation; input, alteration or deletion with without right, of the access to these data.

[12] Law 286/2009 in the New Criminal Code was enforced through Law 187/2012.

[13] Law 135/2010 on the New Criminal Procedure Code was enforced through the Law 255/2013.

the New Criminal Code integrated offenses against security and integrity of computer systems and data[14], the majority of those implemented initially by the Title III of the Law 161/2003. The most important crimes regulated by the New Criminal Code are:

- illegal access to a computer system;[15]
- illegal interception of computer data transmissions;[16]
- altering computer data integrity;[17]
- disruption of the operation of computer systems;[18]
- unauthorized transfer of computer data;[19]
- disruption of the functioning of computer systems;[20]
- illegal operations with devices or software;[21]
- computer data forgery;[22]
- computer fraud;[23]
- child pornography.[24]

Additionally, the New Criminal Procedure Code stipulates legal rules regulating methods of surveillance or investigation, such as wiretapping of communications or of any type of remote communication, accessing a computer system, video, audio or photo surveillance, tracking or tracing with the use of technical devices, obtaining data regarding the financial transactions of individuals, withholding, delivery or search of mail deliveries, use of undercover investigators and informants, authorized participation in specific activities, controlled delivery, obtaining traffic and location data processed by providers of public electronic communication networks or by providers of electronic communication services intended for the public.[25]

In our opinion, through the above mentioned normative acts, formally the Romanian legislator has entirely implemented the Budapest Convention.

We agree with the point of view expressed in the juridical literature that "the Romanian legal provisions are often vague and dispersed in a confusing way [...] that the effectiveness of existing legal measures needs to be reconsidered. There is a need to better describe, in an unambiguous manner, the elements of the prohibited conduct and take into account the recent years developments in computer technology and perpetration techniques [...] there is a clear need to update the legal framework according to the new shapes of cybercrime."[26]

Another aspect to be reviewed *de lege ferenda*, on our opinion, is the penalties regime which we consider to be not properly shaped, in the sense an increasing of the imprisonment period limits is required in order to achieve the preventing and combating role.

Also, regarding the implementation of the Cybercrime Treaty, there is to be observed that the offences related to infringements of copyright and related rights are not especially regulated neither by Law 161/2003, nor by New Criminal Code.

We are of the opinion that the reason why the national legislator did not particularly prohibit this type of behaviour through the Title III of the Law 161/2003 and, after that, did not incriminate in the Penal Code the copyright infringements similarly with the offences taken over form the Law

[14] For an analysis of the provisions regarding cybercrimes in the New Criminal Code, see Dobrinoiu Maxim, *Considerations on the Efficiency of the Romanian New Criminal Code in Combating Cybercrime*, CKS 2013, p 30-36. See also, Nadiia Shulzhenk. Snizhana Romashkin, *Internet fraud and transnational organized crime*, „Juridical Tribune-Tribuna Juridica", Volume 10, Issue 1, March 2020, p. 162-172.
[15] Article 360 of the New Criminal Code.
[16] Article 361 of the New Criminal Code.
[17] Article 362 of the New Criminal Code.
[18] Article 363 of the New Criminal Code.
[19] Article 364 of the New Criminal Code.
[20] Article 363 of the New Criminal Code.
[21] Article 365 of the New Criminal Code.
[22] Article 325 of the New Criminal Code.
[23] Article 249 of the New Criminal Code.
[24] Article 374 of the New Criminal Code.
[25] Article 138 of the New Criminal Procedure Code.
[26] Vasiu Ioana, Vasiu Lucian, *The Cybercrime Challenge: Does the Romanian Legislation Answer Adequately?*, „Law Review", vol. III, issue 2, 2013, p. 5.

161/2003 is just that such offences were considered as being related offences to those belonging to cybercrime area.

In the meantime, the implementation of the Article 10 of the Budapest Convention has been carried out through the Law 8/1996 on copyright and related rights [27]. It should however further be stressed that there are legal systems where the copyright infringements are much more detailed and severe regulated and that, *de lege ferenda*, the national legislator could take into consideration to ensure a more complete and strictly framework in this field.

Overall, it can be concluded that the current Romanian legal framework on cybercrime constitutes a coherent legal basis for protecting our rights in the cyberspace and particularly the New Criminal Code provides "useful tools to the practitioners in combating a wide range of criminal behaviour against computer data systems and telecommunication."[28]

3. Cybersecurity: an emergency objective for the European Union

The fighting against cybercrime is not possible without a secure system[29] behind it. Though it may seem excessive at first sight, "the fighting" term is a proper one, as long as the threat of a cyber war is as real as possible.

Cybersecurity may be defined as being "the effort to protect information, communications, and technology from harm caused either accidentally or intentionally; important to emphasize is that a cyber attack is profoundly distinct from a physical attack. Further, cybersecurity is the effort to ensure the confidentiality, integrity, and availability of data, resources, and processes through the use of administrative, physical, and technical controls" [30]

At the European level, in order ensure the security against the cyber attacks, it was adopted a first legislative act focused on this subject matter-the Directive 2016/1148 concerning measures for a high common level of security of network and information systems across the Union[31], known as "NIS Directive" (Directive on Security of Network and Information Systems)[32].

The "NIS Directive" was transposed into Romanian legislation through Law no. 362/2018 on ensuring a high common level of security of network and information systems.[33]

As Romania received a letter of formal notice from the Commission because of the inadequate transposition of the Directive on cybersecurity, the Law no. 362/2018 was amended by the Emergency Ordinance no. 119 /2020[34].

It is to be emphasized that Austria, Bulgaria, Belgium, Croatia, Denmark, France, Greece, Hungary, Ireland, Latvia, Lithuania, Luxembourg, the Netherlands, Poland, Portugal, and Spain were subjects to the same infringement procedure, as well.

Such a widespread mis transposition may be explained by the novelty and complex character of the subject matter to be regulated and harmonized and it is an indicator that the Member States will need a significant period of time to integrate it in their national law.

Even at the European level the legislation is in the process of development and recalibration.

---

[27] Published in the Romanian Official Monitor no. 26/1996, amended and completed, republished in the Romanian Official Monitor no. 489/2018.

[28] Dobrinoiu Maxim, *Considerations on the Efficiency of the Romanian New Criminal Code in Combating Cybercrime*, CKS 2013, p. 36.

[29] Technically, the cybersecurity is"the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security or electronic information security. The term applies in a variety of contexts, from business to mobile computing, and can be divided into a few common categories" https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security, accessed on December 2021.

[30] De Amos N. Guiora. *Cybersecurity: Geopolitics, Law, and Policy* published by Routledge, 2017, p. 17.

[31] Published in the Official Journal 194/2016.

[32] See Ramses A. Wessel, *Cybersecurity in the European Union: Resilience through Regulation?*, The Routledge Handbook of European Security Law and Policy, Routledge, 2019, p. 283-300.

[33] Published in the Romanian Official Monitor no. 21/2019. The Emergency Ordinance No. 119/ 2020 has as goal to the regulate the CERT-RO's function and and the Interinstitutional Working Group for the Determination of the Threshold Values Necessary for Determining the Significant Disruptive Effect of Incidents at the Networks and Computer Systems for essential service operators ('GdLINIS').

[34] Published in the Romanian Official Monitor no. 658/2020.

Despite the fact that the European framework on network and information security is recent, and its transposition by the Member States into the national legislation is even more recent, the "NIS Directive" shall be modified through "NIS 2 Directive".

On 16 December 2020, the European Union Commission published its proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity. [35].The draft of the "NIS 2 Directive" was adopted on 28 October 2021 by the European Parliament's Committee on Industry, Research and Energy revising the Directive 2016/1148 on Security of Network and Information Systems.

It is uncommon to amend a Directive after such a short time and a general comparative analysis of the goal of each legislative act may lead to some conclusions regarding the European legislator will. The most relevant reason for adoption of a new European cybersecurity law is the regulatory purpose.

The "NIS Directive" applies to water transport, digital infrastructure, energy, healthcare, transport, banking and financial market sectors, as well as to those legal persons providing digital service for remuneration at the individual request at a distance using electronic means.[36]

Comparatively, the "NIS 2 Directive" aims to extend the covered areas and it shall include the following sectors and subsectors[37]:

- essential entities, such as energy, transport banking, financial market infrastructures, health, manufacture of pharmaceutical products including vaccines, drinking water, digital infrastructure, public administration, space and

-important entities, such as postal and courier services, waste management, chemicals, food, manufacturing of medical devices, computers and electronics, machinery equipment, motor vehicles and digital providers.

Furthermore, the new Directive sets out goals relating to incident response, supply chain security, encryption and vulnerability disclosure obligations[38] and as regards the improvement of the cooperation between European Union Member States.

To conclude, the "NIS 2 Directive" has three main objectives:

- to extend the level of cyber-resilience of a comprehensive set of businesses from a wide range of sectors;
- to improve the level of cyber-resilience in the industries that are already regulated;
- to improve the incident response of the national authorities, of the public and private entities and the cooperation at the European level in this regard.

The legislative process is in progress and it's obviously that for the European Union and its Member States the cybersecurity represents a central issue, an emergency objective to be efficiently achieved, so that to mitigate in the future the vulnerabilities and the risks in the event of cyber-attacks.

4. Conclusions

The cybersecurity law and the cybercrime law are getting increasingly important in the international, European and Romanian legislative frame.

The digital connectivity is growing rapidly, to the extent that more and more our activities are taking place on a cyber basis, providing a perfect environment for cybercrimes. The evolution of technology has led to the expansion of criminal methods and, consequently, there is an essential necessity to continuingly assure the prevention and the combating cybercrime through coherent and well-founded legal measures.

The law constitutes the key player in solving the challenges brought up by the virtual life in

[35] Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 COM/2020/823 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2020%3A823%3AFIN, accessed on December 2021.
[36] See the recitals of the Directive 2016/1148.
[37] According to the Annex I and to the Annex II of the Commission Proposal.
[38] Commission Proposal, p. 43.

the new digital age. The domestic legal measures having as starting point the Budapest Convention are protecting against cybercrimes to a certain extent, with the observation that a constantly improving of the legal basis is necessary. *De lege ferenda*, on the one hand, the provisions stipulating the prohibited behaviours have to respond more properly to the up-to-date and clarity requirements, keeping up with the development of technology, and, on the other hand, the sanctions have to be reshaped in order to represent consistent remedies.

As the offences committed in the cyberspace and the cybersecurity are strongly interconnected, the ensuring of the security of network and information systems is a priority at the European and national level, the "NIS Directive" (NIS) Directive being just the beginning of a EU-wide legal framework in the field of cybersecurity. Currently, the rhythm of regulatory activity is an effervescent, continuously growing one, and the health crisis and the relocation of activities in the online medium have determined the intensification of the legislative process in this domain.

Bibliography

1. Craig, Paul, de Burca, Grainne, *EU Law. Text, cases, materials*, seventh edition, Oxford University Press, New-York, 2020.
2. De Amos N. Guiora. *Cybersecurity: Geopolitics, Law, and Policy*, Routledge, 2017.
3. Dobrinoiu Maxim, *Considerations on the Efficiency of the Romanian New Criminal Code in Combating Cybercrime*, CKS 2013.
4. Vasiu Ioana, Vasiu Lucian, *The Cybercrime Challenge: Does the Romanian Legislation Answer Adequately?*, „Law Review", vol. III, issue 2, 2013.
5. Nadiia Shulzhenk. Snizhana Romashkin, *Internet fraud and transnational organized crime*, „Juridical Tribune-Tribuna Juridica", Volume 10, Issue 1, March 2020.
6. Cristina Elena Popa Tache, *Administrative Review and Reform Movements from the Perspective of International Investment Law*, in Julien Cazala, Velimir Zivkovic (editors), *Administrative Law and Public Administration in the Global Social System, (Contributions to the 3rd International Conference. Contemporary Challenges in Administrative Law from an Interdisciplinary Perspective, October 9, 2020)*, ADJURIS – International Academic Publisher, 2020, pp. 212-217.
7. Ramses A. Wessel, *Cybersecurity in the European Union: Resilience through Regulation?*, The Routledge Handbook of European Security Law and Policy, Routledge, 2019.
8. Convention on Cybercrimes, Council of Europe, adopted at Budapest, 23rd Nov. 2001.
9. Report - *The Budapest Convention on Cybercrime:benefits and impact in practice*, Cybercrime Convention Committee, Council of Europe, 2020.
10. Law 161/2003, Title III - Prevention and combating cybercrime.
11. The New Criminal Code.
12. Directive 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.
13. Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity.