PROPOSALS FOR A BROADER APPROACH OF „MISUSE OF DEVICES AND PROGRAMS' PROVISION IN COMBATING CYBER-DEPENDENT AND CYBER-ENABLED CRIMES

Maxim DOBRINOIU[*]

Abstract

The adoption, in 2001, in Budapest, of the Council of Europe Convention on Cybercrime brought an important step forward in the prevention and combatting cyber-related crimes, through the creation of a special indictment (Article 6) against the production, sale, procurement for use, import, distribution, import or making available of devices, computer programs, passwords or any other such data with the scope to further illegal access to a computer system, interception without right of a computer data transmission, an illegal data interference or an illegal system interference, offences comprised in the Articles 2 to 5 of the Convention. Although the offence in Article 6 represents the „mean-crime' in relation with the further commission of the above mentioned crimes against the confidentiality, integrity and availability of computer data and systems („purpose-crimes'), the nowadays Cybercrime phenomenon shows that the misuse of the devices and computer programs actually exceeds the legal boundaries of Articles 2 to 5, and (technically) impacts much of the other forms of cyber-related or cyber-enabled offences, especially in the FinTech area, electronic payment, blockchain, cryptocurrency etc. Taking into consideration the proliferation of illegal activities against personal information, confidential data or access credentials, especially the commercialization, especially in Dark Web, of codes, passwords, hacking tools, malware and other present or future cutting-edge system interference technologies, thus posing a great danger to the whole cyber-ecosystem, an improvement of Article 6, and of all the correspondent (related) articles in the special laws or the criminal codes adopted by the signatory countries, would contribute to the creation of an extensive and much comprehensive legal tool in the prevention and efficiently combating cybercrimes.

Keywords: *criminal liability, misuse of devices, cyber-dependent crimes, cyber-enabled crimes, CoE Convention on Cybercrime, illegal operations with devices and software.*

1. The context of computer programs and devices being used for committing cyber-related crimes

Generally, the phenomenon of cybercrime refers to a variety of criminal activities that are either committed against the computer data and systems or with the use of such automated 'tools'.

Under various names along the time, such as: *computer crime*, *e-crime*, *internet crime*, *digital crime*, *online crime*, *virtual crime*, *techno crime* or *net crime*, the 'cybercrime' has yet a not commonly agreed definition, although the term is somehow known and used since 1970s.

And this is to be confirmed by the latest studies on the domain, that 'the only consensus within the literature, is that there is no single clear, precise and universally accepted definition of cybercrime, a fact that

[*]Associate Professor, PhD, Faculty of Law, "Nicolae Titulescu" University of Bucharest (e-mail: maxim.dobrinoiu@univnt.ro).

is acknowledged by both academics and organizations alike'[1].

A simple, but comprehensive definition, we partially agree with, states that 'cybercrime is the use of a computer as the instrument to further illegal ends'[2]. For all that, we must admit that not only computers may be the material object or the tool of a crime, but also computer data (data, software, applications etc.), that should be regarded in a distinctive manner.

The relevant international organizations seem to also have failed somehow in finding a commonly acceptable definition on cybercrime. For all that, we may acknowledge the United Nations Office on Drugs and Crime' s definition 'cybercrime is an act that violates the law, which is perpetrated using information and communication technology (ICT)'[3].

The industry tends to see cybercrime as 'an illegal activity involving computers, the internet, or network devices'[4] or as 'illegal usage of any communication device to commit or facilitate in committing any illegal act'[5].

In the study '*Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies*', the authors[6] gathered from the literature different approaches of the term, as follows:

- Computer crime or computer-related crime;[7]
- '*any illegal behaviour directed by means of electronic operations that target the security of computer systems and the data processed by them' or 'any illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession and offering or distributing information by means of a computer system or network*'[8];
- '*actions 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 criminalization of such conduct*'[9];
- '*criminal acts committed using electronic communications networks and information systems or against such networks and systems*'[10];

[1] Kirsty Phillips, Julia C. Davidson, Ruby R. Farr, Christine Burkhardt, Stefano Caneppele, Mary P. Aiken, *Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies*, Forensic Sciences, 2022, 2(2), 379-398, https://doi.org/10.3390/forensicsci2020028, available at https://www.mdpi.com/2673-6756/2/2/28 (accessed on 14.04.2024).

[2] Michael Aaron Dennis, *Cybercrime*, Encyclopedia Britannica, 19 Apr. 2024, https://www.britannica.com/topic/cybercrime (accessed 28.04.2024).

[3] https://www.unodc.org/e4j/en/cybercrime/module-1/key-issues/cybercrime-in-brief.html.

[4] https://www.cisco.com/site/us/en/learn/topics/security/what-is-cybercrime.html.

[5] https://cybertalents.com/blog/what-is-cyber-crime-types-examples-and-prevention.

[6] See also Kirsty Phillips *et alii*, *op.cit.*

[7] *United Nations Manual on the Prevention and Control of Computer-related Crime*, United Nations, NY, USA, 1994 (accessed by Google Scholar on 14.04.2024).

[8] UN Congress Crimes Related to Computer Networks. *10th UN Congress on the Prevention of Crime and the Treatment of the Offenders*, UN, Vienna, Austria, 2000 (available at https://www.unodc.org/documents/congress/Previous_Congresses/10th_Congress_2000 accessed on 14.04.2024).

[9] Council of Europe, *Convention on Cybercrime*, European Treaty Series ETS-185, Budapest, Hungary, 2001, p.1-25, available at https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561.

[10] Commission of the European Communities, *Communication from the Commission to the European Parliament, the Council and the Committee of the Regions: Towards a General Policy on the Fight against Cyber Crime*, Bruxelles, Belgium, 2007, vol. 267 (accessed through Google Scholar on 14.04.2024).

- '*a broad range of different criminal activities where computers and information systems are involved either as a primary tool or as a primary target*'[11].

The most interesting issue in analyzing the phenomenon of cybercrime is the categorization. While most of the authors rely on a two-factor category of cybercrime, there are also specialists that argue in the favor of a three-factor categorization of cybercrimes.

The dual-approach is based mainly on distinguishing between 'cyber-dependent' and 'cyber-enabled' crimes. This option derives from the most accepted official and academic visions on cybercrime[12], whereas computer systems and data represent the target (object) of the illegal conduct or the tools that facilitate the commission of other (traditional) crimes.

According to some authors, 'cyber-dependent crimes are crimes that arose with the advent of technology and cannot exist outside the digital world, e.g. hacking, such as ransomware attacks or hacktivism'[13]. In contrast, 'cyber-enabled crimes are traditional crimes that predate the advent of the technology, and are now facilitated or have been made easier by cyber technology. Cyber-enabled crimes range from white-collar crime to drug-trafficking, online harassment, cyberterrorism and beyond'[14].

On the top of these classifications, there is the opinion of authors D. Wall and A. Pattavina[15] that cybercrime may be regarded from three perspectives:

'*Cyber-dependent crimes or true cybercrimes*', where the computer is the target and the crime could not happen without a computer, i.e. truly new opportunities for crime, e.g. hacking, malware and DoS/DDoS, parasitic computing*;*

'*Cyber-enabled crimes or hybrid crimes*', where a computers and data may be involved, but the crime could still be perpetrated without them, i.e. new opportunities for traditional crimes, e.g. frauds, scams, ID Theft, and phishing;

'*Cyber-assisted crimes or the use of computer in traditional crime*', where the computer and data simply constitute the tool for the commission traditional crimes, e.g. frauds, pyramid schemes, stalking, harassment, criminal communications.

As most of the researchers recognize, the significant classification system of cybercrime is provided by the notorious *Council of Europe (CoE) Convention on Cybercrime*, signed in Budapest in 2001. This instrument, supplemented by additional protocols over time, made a particular classification of computer crimes, as shown below:

1. Offences against confidentiality, integrity and availability of computer data and systems

- Illegal access (article 2)
- Illegal interception (article 3)
- Data interference (article 4)
- System interference (article 5)
- Misuse of devices (article 6)

[11] European Commission, *Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, Brussels, Belgium, 2013 (accessed through Google Scholar on 14.04.2024).

[12] See also Kirsty Phillips *et alii*, *op.cit.*

[13] See Mike McGuire, Samantha Dowling, *Cybercrime: A Review of the Evidence: Summary of Kedy Findings and Implications*, Home Office, London, UK, 2013 (available through Google Scholar).

[14] *Ibidem*.

[15] David S. Wall, *The Internet as a Conduit for Criminal Activity* (October 21, 2015). Information Technology and the Criminal Justice System, A. Pattavina, ed., pp. 77-98, Sage Publications, Inc., 2005 (revised 2010, 2015), Available at SSRN: https://ssrn.com/abstract=740626.

2. Computer-related offences

- Computer-related forgery (article 7)
- Computer-related fraud (article 8)

3. Content-related offences

- Offences related to child pornography (article 9)

4. Offences related to infringements of copyright and related rights

- Offences related to infringements of copyright and related rights (article 10)

5. Acts of a racist and xenophobic nature committed through computer systems

It is worth mentioning that, in 2013, the European Union adopted and enforced the Directive 2013/40/EU[16], that made available a definition of criminal offences in the area of attacks against information systems, as well as a categorization of such offences:

- Article 3 - Illegal access to information systems
- Article 4 - Illegal system interference
- Article 5 - Illegal data interference
- Article 6 - Illegal interception
- Article 7 - Tools used for committing offences
- Article 8 - incitement, aiding and abetting and attempt.

Analyzing the last two important pieces of legislation, one could come to the conclusion that, although slightly different (in concepts and definitions), both documents fail to provide with a general understanding of the concept of cybercrime, but offer a broad perspective of the crimes that may be committed against the computer systems and data.

2. Legal provisions on illegal operations with computer data, applications and devices

A distinct attention of this article is paid to the offence of *misuse of devices*, as it is considered as a 'facilitating-offence'[17] and a helpful mean of committing other crimes in the area of computer systems and data (cybercrime).

The offence of misuse of devices first appeared officially in the CoE Convention on Cybercrime, in Article 6 (with the same name).

According to this document, the CoE Convention on Cybercrime urged states '*to adopt such legislative and other measures to establish as criminal offence, when committed intentionally and without right:*

a) the production, sale, procurement for use, import, distribution or otherwise making available:

- a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Articles 2 through 5;
- a computer password, access code or similar data by which the whole or any part of a computer system is capable of being accessed, with the intent that it be used for the purpose of committing any offences established in Article 2 through 5, and

b) the possession of an item referred to in paragraph a.i or ii above, ***with the intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5'[18].***

[16] Directive 2013/40/Eu of the European Parliament and of the Council on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, Official Journal of the European Union 2013, 218, 8-14, available online at https://eur-lex.europa.eu/legal-content/EN (accessed on 20.04.2024)

[17] Versus a 'facilitated-offence' or the 'target offence' that is committed using the outcomes of the 'facilitating-offence'.

[18] Article 6, CoE Convention on Cybercrime (ETS no. 185, available at https://rm.coe.int , accessed on 20.04.2024).

One could very easily note, as we also underlined in the text, that the European legislator in 2001 regarded all the acts comprised in Article 6 as offences only if committed with the intent or for the purpose of committing a specific set of offences, namely those provided in Articles 2, 3, 4 and 5.

It is a curious approaching of this offence, mainly because it fails to take into consideration that all the acts mentioned in Article 6 (facilitating-offence) could be also used in committing of other crimes and offences, particularly those mentioned in the CoE Convention itself in Article 7 – Computer-related forgery, and Article 8 - Computer-related fraud, and also in Article 9 – Offences related to child pornography (as 'facilitated-offences' or 'target-offences').

It is a surprisingly decision of the lawmakers of that time to let apart the offences provided in Articles 7 to 9, as being possible 'facilitated-offences' ('target-offences'), as they are usually committed, from the technical point of view, by the means of devices, programs, applications, codes or other similar data.

The Directive 2013/40/EU also addresses the 'misuse of devices', and states, in Article 7 - Tools used for committing offences, that '*member states shall take the necessary measures to ensure that the intentional production, sale, procurement for use, import, distribution or otherwise making available, of one of the following tools, without right and* ***with the intention that it be used to commit any of the offences referred to in Articles 3 to 6****, is punishable as a criminal offence, at least for cases which are not minor:*

a) a computer program, designed or adapted primarily for the purpose of committing any of the offences referred to in Articles 3 to 6;

b) a computer password, access code, or similar data by which the whole or any part of the information system is capable of being accessed.'.

It is worth remembering (see above mentions) that Articles 3 to 6 of the Directive refer to offences that are generally committed against data and computer systems.

Again, the European lawmakers made a clear distinction between the so called 'cyber-dependent offences' and 'cyber-enabled offences', and urged Member States to adopt legislative measures to indict (as 'facilitating-offence') the conduct related to the production, sale, procurement, distribution or making available of computer programs or codes only in the situation that the respective acts are committed without right and with the intention to serve for the further commission of just the 'computer-dependent offences' (as 'facilitated-offences').

This time, also, the mentioned acts (see Article 7) cannot be regarded as offences unless the target-offence itself is not one against a computer system or data.

Having these two important pieces of legislation in place, the European Member States did take measures and established different legal solutions to comply.

Thus, the proposals of a distinct legal provision criminalizing the misuse of devices and programs have further been adopted in the substantive criminal law of many countries, such as:

Austria - Section 126c of the Criminal Code[19] considers the crime of „misuse of computer programs arid access data' the alternative acts of producing, introducing, distributing, selling or otherwise making

[19] https://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Documents/CountryProfiles/567-LEG-country%20profile%20Austria%20_30%20May%2007_En.pdf.

available '*a computer program or a compatible equipment which has been obviously created or adapted due to its particular nature to commit an unlawful access to a computer system (sect. 118a), an infringement of the secrecy of telecommunications (sect. 119), an unlawful interception of data (sect. 119a), a damaging of data (sect. 126a) or an interference with the functioning of a computer system (sect. 126b)*'. So, the Austrian legislator backed the CoE Convention and incriminates the misuse of device and data only in the case of a specific sort of computer crimes: the computer-dependent crimes.

Belgium - art. 550bis of the Criminal Code, in paragraph (5) punishes the person who '*unduly possesses, produces, sells, obtains with a view to his use, imports, distributes or makes available in another form, any device, including computer data, primarily designed or adapted for allowing the commission of the offences provided for in paragraph (1) to (4)*[20]', while art. 550ter, in paragraph (4) addresses the same illegal conduct, but in connection with the offences of data interference (alteration, deletion, damaging) and system interference (preventing the correct functioning of a computer system…). One can note that these 'misuse of device and programs'-like offences in the Belgian legislation are linked with the further commission (or further intent to commit) of only cyber-dependent offences, as also envisaged by Article 6 of the CoE Convention on Cybercrime.

Bulgaria - art. 319e of the Criminal Code[21] only considers a crime when a perpetrator circulates computer or system passwords thus causing disclosure of personal data or an information representing a state secret, so no entirely mapping with the CoE Convention on Cybercrime Article 6.

Canada - art. 342.2 of the Criminal Code, amended by the 'Protecting Canadians from Online Crime Act' (SC 2014, c.31)[22], refers to '*everyone who, without lawful excuse, makes, possesses, sells, offers for sale, imports, obtains for use, distributes or makes available a device that is designed or adapted primarily to commit an offence under section 342.1*[23] *or 430*[24]*, under circumstances that give rise to a reasonable inference that the device has been used or was intended to be used to commit such an offence*'. Also in this case, the provision only covers the situation when the material acts of this offence are put in a direct link with the commission (or with the intent to the commission) of a computer-dependent crime.

Czech Republic - on its Criminal Code[25] has Section 231 under the name of 'Obtaining and possession of access device and computer system passwords and other such data' that criminalize any conduct of a person who '*produces, puts into circulation, imports, exports, transits, offers, provides, sells, or otherwise makes available, obtains for him/herself or for another, or handles – a device or its component, process, instrument or any other means, including a*

[20] Illegal access to computer data and systems, damage caused to computer system and data, and data interference.

[21] https://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Documents/CountryProfiles/567-LEG-country%20profile%20Bulgaria%20_9%20May%2007_En.pdf.

[22] https://laws-lois.justice.gc.ca/eng/annualstatutes/2014_31/page-2.html#docCont.

[23] Unauthorized use of computer.

[24] Section 430 (1.1) Mischief in relation to computer data.

[25] https://antislaverylaw.ac.uk/wp-content/uploads/2019/08/Czech-Republic-Criminal-Code.pdf.

computer program designed or adapted for unauthorized access to electronic communications network, computer system.…'. Partially mapping with the Article 6 of the CoE Convention on Cybercrime, the Czech legislators considered the offence of Section 231 only in the context of the perpetrator's intent to commit a 'breach of secrecy of correspondence' (under Section 182-1 b), c)) or a criminal offence of 'unauthorized access to computer systems and information media' (under Section 230 paragraphs (1), (2)). So to say, one facilitated cyber-enabled offence and one facilitated cyber-dependent offence.

Cyprus - adopted the Law 22(III)/2004[26] – revised, that actually copy-pasted and slightly adapted the legal provisions from the CoE Convention on Cybercrime. Thus, Article 8 of Law 22(III)/2004 is a reproduction of Article 6 of the Convention, and therefore the criminalizing of the 'misuse of devices' is linked with the intent of the perpetrator to commit only a cyber-dependent offence, as stated by the law.

Estonia - art. 216[1] of the Criminal Code[27] maps with the Article 6 of the CoE Convention on Cybercrime and consider an offence of 'Preparation of computer-related crime' the conduct of a person '*for the purposes of committing the criminal offences provided in articles 206[28], 207[29], 208, 213[30] or 217[31] of this Code.…*'. One can observe that, the Estonian Penal Code extended the applicability of the 'misuse of devices and programs' also to a cyber-enabled crime, respectively the computer-related fraud (art. 213).

Finland - chapter 34, sections 9a and 9b of the Criminal Code[32], criminalize the conduct of possessing, importing, acquiring for use, manufacturing, selling or otherwise making available or disseminating devices, computer programs, information system's passwords, access codes or equivalent information, as well as instructions for the manufacturing of a computer program or a set of programming instructions, with the intent to cause harm, to damage the data processing or the functioning of a information system or a communication system, or to decode or disable the technical protection of electronic communications or the protection of an information system. It is worth noting that the target offence represents, also in this case, a computer-dependent offence, thus in accordance with the provision of Article 6 of the CoE Convention on Cybercrime.

France - art. 323-3-1 of the Criminal Code[33] maps in part with the provisions of Article 6 of the CoE Convention, and criminalize '*the import, possession, offering, distributing or making available of an equipment, an instrument, a program or computer data, created or specially adapted for the commission of one or more crimes, as*

[26]https://www.olc.gov.cy/olc/olc.nsf/ECB669A2EBF5FE75C225871100236DEC/$file/The%20Convention%20of%20the%20Council%20of%20Europe%20on%20Cybercrime%20(Ratification)%20Law%of%202004%20%20L.22(III)-2004.pdf.

[27]https://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Documents/CountryProfiles/567-LEG-country%20profile%20ESTONIA%20_april%202008_.pdf.

[28] Interference in computer data.

[29] Hindering of operation of computer system.

[30] Computer-related fraud.

[31] Unlawful use of computer system.

[32] https://www.finlex.fi/fi/laki/kaannokset/1889/en18890039.pdf.

[33]https://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Documents/CountryProfiles/567-LEG-country%20profile%20France%20_26%20March%2007_En.pdf.

provided by articles 323-1[34] *to 323-3.*'. As noted, the French legislator preferred to indict the so-called 'misuse of device and programs' just with the conditions of further commission of a cyber-dependent crime.

Germany - art. 202c of the Criminal Code[35] maps for a large percentage with the Article 6 of the CoE Convention, and relates the '*creating, procuring for himself or another party, selling, giving over to another party, disseminating or otherwise providing access to passwords, security codes….computer programs whose purpose is to commit such an act*' to the preparation of '*a criminal offence pursuant to section 202a*[36] *or 202b*[37]'. We observe that the German legislator remained in the same paradigm of computer-dependent crimes when it comes to the 'misuse of devices and programs'.

Hungary - art. 300/E of the Criminal Code[38] partially maps with the Article 6 of the CoE Convention, and conditions the unlawful conduct by the commission of an offence under art. 300/C, that covers both cyber-dependent crimes (such as illegal access to a computer system and data, and data interference) and cyber-enabled crimes (such as computer-related fraud – alignment 3).

Ireland - Offences Related to Information Systems Act 2017, section 6[39] (use of computer programme, password, code or data for purposes of section 2, 3, 4 or 5) represents a copy of the provisions of Article 6 of the CoE Convention on Cybercrime, and relates the 'misuse of devices and programs' only to the other offence of the same law, mentioned in section 2[40], section 3[41], section 4[42] and section 5[43], thus computer-dependent offence.

Italy - in the Penal Code[44], article 615 quarter '*whoever, in order to obtain a profit for himself or others or to cause damage to others, illegally procures, reproduces, disseminates, communicates or delivers, codes, keywords or other means suitable for access to a computer system or electronically, protected by security measures, or in any case provides indications or instructions suitable for the aforementioned purpose*', while article 615 quinquies '*whoever, with the aim of illicitly damaging a computer or telematic system, the information, data or programs contained therein or pertinent to it or to favor the total or partial interruption or alteration of its functioning, procures, produces , reproduces, imports, disseminates, communicates, delivers, or, in any case, makes equipment, devices or computer programs available to others*'. One could easily observe that the Italian legislators mapped with the Article 6 of the CoE

[34] Illegal access to a computer system and system interference.

[35] https://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Documents/CountryProfiles/567-LEG-country%20profile%20Germany%20_1%20June%2007_En.pdf.

[36] Data espionage (unauthorized access to data).

[37] Data interception.

[38]https://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Documents/CountryProfiles/567-LEG-country%20profile%20Hungary%20_7%20June%2007_En.pdf.

[39] https://www.irishstatutebook.ie/eli/2017/act/11/section/6/enacted/en/html#sec6.

[40] Accessing information system without lawful authority.

[41] Interference with information system without lawful authority.

[42] Interference with data without lawful authority.

[43] Intercepting transmission of data without lawful authority.

[44] https://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Documents/CountryProfiles/567-LEG-country%20Italy%20_26%20%20April%202008_pub.pdf.

Convention on Cybercrime, and considered the offence only if committed in connection with another computer-dependent crime.

Lithuania - art. 198-2 of the Criminal Code maps with the general provisions of the Article 6 of the CoE Convention on Cybercrime, and relate the respective offence of 'Illegal possession of the devices, computer program, passwords, access codes and other data with intent to commit a crime' by the further commission of certain articles of the Code, such as art. 166[45], art. 196[46], art. 197[47], art. 198[48], and art. 198-1[49]. Despite the existence of article 166 that refers to the breaching of the private correspondence inviolability, the rest of the target offences are generally those comprised also in Article 6 of the CoE Convention on Cybercrime, meaning computer-dependent crimes.

Netherlands - Section 139d of the Criminal Code[50], states in paragraph (2) that 'any person who: a. manufactures, sells, obtains, imports, distributes or otherwise makes available or has in his possession a technical device that has been primarily adapted or designed for the commission of such serious offences, or b. sells, obtains, distributes or otherwise makes available or has in his possession a computer password, access code or similar data that can be used for accessing a computer device or system or a part thereof, with the intent of using it in the commission of a serious offence, as referred to in section 138ab(1)[51], 138b[52] or 139c[53]'. Obvious that the Dutch legislators not entirely mapped the Article 6 of the CoE Convention, but still connected the 'misuse of devices and programs' (Section 139d) with the commission of cyber-dependent offences (as described above).

Poland - in Chapter XXXIII – crimes against the protection of information in the Penal Code[54], there is Article (Rule) 269b criminalized the conduct of a person who '*manufactures, acquires, disposes of, or provides facilities to other persons or computer programs designed to commit an offence referred to in Art. 165 paragraph (1) point (4)[55], Art. 267 paragraph (2)[56], Art. 268a paragraph (1)[57]…, Art. 269 paragraph (2)[58], or Art. 269a[59], and the computer passwords, access codes or other data, allowing access to information stored in a computer system or network of ICT*'. With a single exception (the offence mentioned in Art. 165 paragraph (1), point (4)), the offence of 'misuse of devices and programs' merely enclose references to other cyber-dependent offences, mapping with the

[45] Violation of inviolability of a person's correspondence.
[46] Unlawful influence on electronic data.
[47] Unlawful influence on an information system.
[48] Unlawful interception and use of data.
[49] Unlawful connection to an information system.
[50] https://legislationline.org/sites/default/files/documents/f3/Netherlands_CC_am2012_en.pdf.
[51] Computer trespass (Illegal access).
[52] Hindering the access to or use of a computer device or system.
[53] Illegal interception of data.
[54] https://eurcenter.net/wp-content/uploads/2020/09/Criminal-Procedure-Code-of-Poland-1997-amended-2004.pdf.
[55] Endanger the life and health by impairing, preventing, or otherwise affecting the automatic processing, collection or transmission of data.
[56] Unlawful obtaining of information.
[57] Data interference.
[58] Destroying / damaging a device.
[59] System interference.

'request' of the Article 6 of the CoE Convention on Cybercrime.

Portugal - Law no. 109/2009 on the Cybercrime[60] states in Article 3 – Computer Forgery, paragraph (4), that '*whoever imports, distributes, sells or holds for commercial purposes any device that allows the access to a computer system, to a payment system, to a communications system or to a conditioned access service*', while in Article 4 – Computer Damage, paragraph (3) shows that '*the same penalty of paragraph (1) will be applied to those who illegally produce, sell, distribute or otherwise disseminate to one or more computers or to other systems devices, software or other computer data intended to produce the unauthorized actions described in that paragraph*[61]'. Finally, the Article 6 – Illegal access, paragraph (2), states that '*the same penalty will be applied to whoever illegally produces, sells, distributes or otherwise disseminates within one or more computer systems devices, programs, a set of executable instructions, code or other computer data intended to produce the unauthorized actions described under the preceding paragraph*[62]'. Analyzing the above-mentioned legal provisions, we can notice that the Portuguese legislators mapped somehow the Article 6 of the CoE Convention on Cybercrime, and conditioned the 'misuse of devices and programs' by the existence of only a cyber-dependent crime.

Romania - art. 365 of the Criminal Code[63] represent a copy of the Article 6 of the CoE Convention on Cybercrime, and it is obvious that the offence of 'Illegal operations with devices and computer programs' is only linked with the target offences mentioned in Articles 360 to 364[64], meaning just cyber-dependent crimes.

Spain - has a distinct situation in terms of the legal provisions in its Criminal Code[65] for 'misuse of device and programs', and the principal sections are: **197ter** – that mainly deals with producing, acquiring for use, importing of computer programs and passwords or codes with the intent to further illegal access computer systems and data, personal data interference and eavesdropping of electronic communications, **264ter** – that deal with unauthorized producing, acquiring of or importing computer programs, passwords or codes and similar data with the intent of committing any of the offences mentioned in sections 264[66] and 264bis[67]. There is also section **400** that refers to the 'manufacture, receipt, obtainment or possession of tools (…) computer data or programs (….) with the intent to commit the criminal offences' related to forgery (documents, currency, cards).

Sweden - although there is no distinct offence dealing with the 'misuse of devices and programs', in Section 9c of the Chapter

[60] https://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/portuguesecybercrime_law.pdf.

[61] Meaning the deletion, altering, destroying, in whole or in part, damaging, removing or rendering unusable or inaccessible programs or other computer data of others.

[62] Meaning the "illegal access to a computer system'.

[63] http://www.vertic.org/media/National%20Legislation/Romania/RO_Criminal_Code.pdf.

[64] Art. 360 – Illegal access to a computer system, art. 361 – Illegal interception of a transmission of data, art. 362 – Data interference, art. 363 – System interference, and art. 364 - Unauthorized transfer of computer data.

[65] https://www.mjusticia.gob.es/es/AreaTematica/DocumentacionPublicaciones/Documents/Criminal_Code_2016.pdf.

[66] Altering the integrity of computer data.

[67] System interference.

4 in the Swedish Criminal Code[68], the legislators criminalized the '*installation of a technical device with the intent to breach telecommunication secrecy or to perform….an unlawful interception*'.

United States of America - art. 2512 of Chapter 119 in Title 18 of the Criminal Code[69] on the manufacturing, distribution, possession, and advertising of wire, oral, or electronic communication intercepting devices prohibited considers the aforementioned offence only in connection with illegal interception of electronic communications or oral communications. Art. 1030 'fraud and related activity in connection with computers' of Chapter 47, in paragraph (5) has a provision that addresses the '*transmission of a program, information, code, or command, and as a result of such conduct, (a person) intentionally causes damage without authorization, to a protected computer*'. So, the US legislators did not take to much attention to what kind of target offences to related the 'misuse of devices and programs', while preferred to cope with this issue on a case-by-case basis, and depending on the topic of the chapter.

As we previously demonstrated in another study's results[70], almost all the above legal provisions have certain features in common, such as:

- the reference to products like: computer programs, applications, computer data, devices, passwords or codes etc.;
- the products are either prohibited *de jure*, or their use may be unlawful, without right, without a legitimate reason etc.;
- the products are described as being *designed, made, created, produced, manufactured, adapted* etc. as for being used in a sort of specific type of crimes (offences), mainly cyber-dependent offence, but also cyber-enabled offences;
- the existence of the intent or the scope (target) to commit further offences.

Analyzing all the above mentioned national legal provisions, we may draw the conclusion that the overwhelming majority of them are mapping or are inspired by the Article 6 of the CoE Convention on Cybercrime, that is *per se* a good thing. At least, there is an agreed framework in what regards the 'misuse of devices and programs'.

The common thing for many of them is the legislators' decision to criminalize the 'misuse of devices and programs' only if in connection with specific or general computer-dependent offences, that we may accept from a national criminal justice policy point of view.

Notwithstanding the foregoing, there are states that approached the issue in a slightly different way, by criminalizing the 'misuse of devices and programs' in connection with both cyber-dependent offences and cyber-enabled offences, and even with other kind of offences (e.g. Austria – infringement of the secrecy of communications, Bulgaria – disclosure of personal data and state secrets, Czech Rep. – breach of secrecy of correspondence, Germany – data espionage, Lithuania – breaching the secrecy of correspondence, Poland – endangering the life and health by impairing, preventing or otherwise affecting the automatic processing, collection or

[68]https://www.government.se/contentassets/7a2dcae0787e465e9a2431554b5eab03/the swedish-criminal-code.pdf.

[69] https://www.law.cornell.edu/uscode/text/18/part-I/chapter-119.

[70] See Maxim Dobrinoiu, *Criminal Liability in the Case of Vendors of Software and Hardware Further Used in Cybercrime Cases*, International Conference 'Challenges of the Knowledge Society', Bucharest, 2022, Nicolae Titulescu University Publishing House (available at http://cks.univnt.ro/download/cks_2022).

transmission of data, Portugal – access to a conditioned access service, Spain – committing offence related to forgery, Sweden – breach of telecommunications secrecy).

So, it appears that not only the cyber-dependent or cyber-enabled offences could be a 'target offence' that may justify the criminalization of the 'misuse of devices and programs' offence, but many other illegal conducts, when committed with the help of specially designed devices, computer systems, computer data, passwords or codes.

3. Types of Cyber-enabled offences as 'facilitated-offences' by misusing devices and programs

As official papers, studies and research materials found, the cyber-enabled offences are usually crimes/offences that do not traditionally depend on computer systems, computer data or electronic devices, but they suffered modifications over time in scale and form by the use of computers, networks or means of electronic communications. Among them, the most prevalent, for our analysis, are:

- **Economic related cybercrimes** - cyber fraud, fraudulent financial operations, card cloning, financially motivated Phishing (Spear Phishing, Smishing, Vishing, Quishing) or Pharming, Ransomware, Scareware, Intellectual property crimes, CEO fraud – Business Email Compromise (Whaling), establishment and operation of illegal online marketplaces, illegal online gambling, online money-laundering, digital wallet draining, establishment and operation of criminal digital assets exchanges, mixers, stablecoins, illegal or criminal decentralized finance (DeFi), account takeover etc.;
- **Non-necessarily economic related cybercrimes** - cyber forgery (Email Spoofing, Web Spoofing, Hyperlink Spoofing, Caller ID Spoofing), non-financially motivated Phishing and Pharming, ID Theft, establishment, operation and provision of end-to-end encrypted communications platforms and services etc.;
- **Individual related cybercrimes** – Social Engineering, Virtual Mobbing, Cyberstalking, Cyber-bullying, online harassment, illegally disclosure of private data, illegally accessing of electronic communications services (e.g. social media), online or electronic child sexual offences, online hate speech, online extortion, commercialization of online identities and credentials, romance scams, online sexual grooming etc.;
- **Government related cybercrime** – Cyber-espionage, Cyber-terrorism, Hacktivism, online recruitment and training for terrorist or ideologically purposes, online illegal propaganda, creation and distribution of fake new, interference with voting systems, online violations of human rights etc.

As observed by analyzing the above-mentioned illegal activities (offences, crimes etc.), there is a common link between all of them: the use of computer data, devices or even systems, as well as the intent to commit further (cyber-related) offences.

From a technical perspective, many of these cyber-enabled crimes rely on devices, programs, applications, passwords, codes and other same digital data that ease, facilitate or make possible the commission of the illegal or unauthorized material acts.

On the other hand, in many legislations, there are offences that for being committed require 'digital tools' (as instruments), and they are not necessarily regarded as computer-enabled crimes (such as: the counterfeiting of banknotes with a computer system and a printer, misleading and altering reality in an official document, written on a computer system by a public servant etc.).

4. Conclusions

This article has the meaning to draw attention of the fact that the EU lawmakers and other legislators, from Europe and beyond, missed to approach the offence generally called '*the misuse of devices and programs*' from a broader perspective of the outcomes, namely the possibilities that the material and technical acts of this 'facilitating-offence', as well as their results, may very well facilitate or may constitute the foundation for the commission of another offences, and not necessarily those 'cyber-dependent'.

In our opinion, taking into consideration the fast-evolving cybercrime ecosystem, and the large implementation of new technologies, legislators and law enforcement agencies must keep the pace with the continuously, newly, complex and more sophisticated tactics, techniques and procedures, as well as with the tools used by cybercriminals in performing their nefarious activities in cyberspace or in the visible, natural and traditional environment.

For that, we think that they need to adopt a much larger perspective in what regards the production, the commercialization, the detaining and the making available of devices, computer programs, applications, passwords, codes or other similar data, considering a criminal behavior not only when the intent is to further affect computer data and systems, but also when this intent is directed towards committing other sort of traditional or new kind of crimes and offences (see cyber-enabled crimes and offences).

In order this to happen, and the legal systems to be prepared for what comes next in the field of cybercrime (and not only), the legislators have to urgently adapt the national criminal laws with relevant and comprehensive legal provisions that also cover the way in which the computer systems, the electronic devices, the programs and applications, as well as the passwords, credentials or other such data may be used, intentionally and without right, to enable the commission of all sort of offences, irrespective if they are against the confidentiality, integrity and availability of computer systems and data or against other legal protected social values.

Such a discussion may arise, for example, about the creation, production, selling, acquiring, importing/exporting, making available etc. of AI-powered tools that are nowadays on a high trend as key enablers of committing both cyber crimes as well as other traditional crimes or even new type of crimes.

Another interesting issue may be related with the creation, procurement and distributing of digital tools that may be used in FinTech crimes, that are generally cyber-enabled crimes.

In the absence of a correct and comprehensive legal provision in place, the national criminal law systems (as well as law enforcement agencies) may not apply the principle *nullum crimen sine lege*, while struggling to use the existing legislation approaching the new faces of more technologized offences.

The idea of this article is to emphasize the need for a legislation update, with the following two aspects:

1. The definition of 'cyber-dependent crimes' and 'cyber-enabled crimes'

2. The modification of the related articles on 'misuse of devices and programs' adding also the 'cyber-enabled crimes' as target offences that may be intended to be committed or even committed with the prohibited devices, computer programs, passwords, codes or likewise data.

References

- Dobrinoiu, Maxim, 'Criminal Liability in the Case of Vendors of Software and Hardware Further Used in Cybercrime Cases', International Conference 'Challenges of the Knowledge Society', Bucharest, 2022, Nicolae Titulescu University Publishing House.
- Dobrinoiu, Vasile *et alii*, *Noul Cod penal comentat*, 3rd edition, Universul Juridic Publishing House, Bucharest, 2016.
- Phillips, Kirsty, Davidson, Julia C., Farr, Ruby R., Burkhardt, Christine, Caneppele, Stefano, Aiken, Mary P., 'Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies', *Forensic Sciences*, 2022, 2(2), 379-398.
- McGuire, Mike, Dowling, Samantha, *Cybercrime: A Re-view of the Evidence: Summary of Kedy Findings and Implications*, Home Office, London, UK, 2013.
- Wall, David S., *The Internet as a Conduit for Criminal Activity* (October 21, 2015), *Information Technology and the Criminal Justice System*, A. Pattavina, ed., pp. 77-98, Sage Publications, Inc., 2005 (revised 2010, 2015).
- Criminal Code of Austria.
- Criminal Code of Belgium.
- Criminal Code of Bulgaria.
- Criminal Code of Canada.
- Criminal Code of Cyprus.
- Criminal Code of the Czech Republic.
- Criminal Code of Estonia.
- Criminal Code of Finland.
- Criminal Code of France.
- Criminal Code of Germany.
- Criminal Code of Hungary.
- Ireland - Offences Relating to Information Systems Act 2017.
- Criminal Code of Italy.
- Criminal Code of Lithuania.
- Criminal Code of the Netherlands.
- Criminal Code of Poland.
- Criminal Code of Portugal.
- Criminal Code of Romania.
- Criminal Code of Spain.
- Criminal Code of Sweden.
- Criminal Code of the United States of America.