Ministry of Education and Science of Ukraine
National University of "Kyiv-Mohyla Academy"
Faculty of Law
Department of Criminal and Criminal Procedural Law

Master's Thesis

specialization 081 "Law"

"The Directive 2013/40/EU on attacks against informational systems: a comparison aspect"

Author: Faculty of Law Student
Yuliia Bohach
Supervisor: Dr. Volodymyr Galagan
Professor of the Department of Criminal and Criminal Procedural Law
Reviewer: Dr. Illya Novoseltsev,
Ph.D, Senior Lecturer of the Department of Private Law

The Master's Thesis received

_____

Secretary of State Examination Board

_____

"___" _____ 20_____

Kyiv – 2020

Міністерство освіти і науки України
Національний університет «Києво-Могилянська академія»
Факультет правничих наук
Кафедра міжнародного та європейського права

Магістерська робота

Спеціальність 081 – Право

«Директива Європейського Парламенту і Ради ЄС 2013/40/ЄС про напади на інформаційні системи - порівняльний аспект»

Виконала: студентка 2-го року навчання
спеціальності 081 Право
Богач Юлія Василівна

Керівник Галаган В. І., професор, доктор юридичних наук,

Рецензент Новосельцев І. І., кандидат юридичних наук, старший викладач кафедри приватного права

Магістерська робота захищена
з оцінкою «_____»

Секретар ЕК _____
«___» _____ 20___р.

Київ – 2020

INTRODUCTION

Today, it is difficult to imagine a world without the Internet, computer devices, and other high-tech achievements. People have become so accustomed to their daily use that do not always understand how dependent they are. The main fields of activity such as public administration, banking, medical activities, trade, energy have already moved or are moving to electronic format. For this reason, the harm caused by the offences committed against information systems and data have may be not only significant but even disastrous.

Cybercrime is one the greatest dangers of our century. Attacks on information systems are carried out constantly. It is crucial that cyberspace differs from any other scene of crime. The absence of borders in cyberspace can damage information systems around the world from a completely different location. Cybercrime is usually transnational in nature. For this reason, it is important for states to fight cybercrime together, namely to create common standards of punishment for this type of crimes, to create a structure for exchanging information on the investigation of such crimes, to facilitate the collection of evidence abroad and to develop international cooperation for rapid and effective investigation.

In recent years, Ukraine has been severely affected by large-scale cyberattacks. In particular, one of the most famous attacks was committed through spreading the Petya virus in 2017 affecting systems of 'state bodies, airports, banks, media companies, delivery services and even the radiation monitoring systems at the former Chernobyl nuclear power plant'[1] and different private companies. Energy sector also suffered from cyberattacks in 2015, when systems of three energy companies were attacked by a malware, that resulted in the interruption of electricity supplying[2].

With a purpose of preventing and combating cyberattack, Ukraine has to build a strong cybersecurity system, which includes not only high-level protection measures but also appropriate criminal law provisions regarding computer crimes and criminal procedural provisions establishing the necessary forms of investigation measures and rules for effective mutual legal assistance.

[1] STRELCOV L. The System of Cybersecurity in Ukraine: Principles, Actors, Challenges, Accomplishments. *Springer.* November 2017. P. 7. [interactive]. [reviewed in 4 April 2020]. Available at: <https://www.researchgate.net/publication/321037340_The_System_of_Cybersecurity_in_Ukraine_Principles_Actors_Challenges_Accomplishments/citations>

[2] Ibid., p. 7-8.

In 2001 Ukraine signed the Convention on Cybercrime[3], but not all provisions are appropriately implemented in the national legislation. Basing on the Cybercrime Convention, the Directive 2013/40/EU on attacks against information systems was adopted in 2013[4]. This instrument is binding within EU Member States. However, regarding the Association Agreement, signed between the EU and Ukraine, and, in general, European direction of the development of Ukraine, the transposition of Directive provisions into Ukrainian legislation is probable in the future. Furthermore, the approximation of legislation to European standards may be useful to begin in the nearest future.

In order to investigate computer crimes effectively, Ukraine ought to adopt foreign, in particular, European experience, increase cooperation with foreign entities in different ways. The exchange of information, exchange of knowledge on methods of investigation computer crimes and collecting evidence are essential forms of cooperation for combating cyberattacks.

This paper has an *aim* to perform a comparative analysis of minimum standards established in the Directive 2013/40/EU on attacks against information system with a purpose to improve Ukrainian legislation.

The *objectives* of the paper are to analyze the provisions of the Directive 2013/40/EU on attacks against information system; define whether the Ukrainian legislation comply with the European minimum standards established by the Directive; find probable ways of improvement of the Ukrainian legislation combating cybercrimes within the Directive 2013/40/EU.

Our *first task* is to compare provisions of the Directive with the previous EU legislative acts and define novelties of the Directive. Our *second task* is to analyze the implementation of the Directive by the Member States taking to account failures as well as good practices. Our *third task* is to compare Ukrainian legislation on substantive criminal law with the Directive provisions and to find out ways of improvement of the Ukrainian legislation regarding the Directive requirements and practice of the Member States.

---

[3] 2001. Convention on Cybercrime. *European Treaty Series*. No. 185. [interactive]. [reviewed in 10 May 2020]. Available at: <http://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561>

[4] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA. *Official Journal of the European Union.* No. L 218/8. 14 August 2013. [interactive]. [reviewed in 10 May 2020]. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013L0040&from=EN>

Method of logical analysis will be used to define the features of an act which has to be punished under the national legislation of Member State in according to Directive requirements. It also will be used to understand the *actus reus* of the offences prescribed by the national law of Member States and Ukraine. Comparative method will be applied in two forms: historical and legal. Comparative historical method will be used to compare the Directive provisions with previous legal acts and to observe changes in the national legislation of Member States regarding the implementation of the Directive. Comparative legal method will be applied to examining the Ukrainian legislation on conformity with the Directive requirements and observing the differences between EU members' national legislation.

Many scientists devoted their works to the issues of European Union Criminal law, some of them explored the area of cybercrime in detail, and their works are used in this paper: Sara Summers[5], Christian Schwarzenegger[6], Paul De Hert[7], Francesko Calderoni and others. However, there is not too many research works dedicated exactly to the analysis of the Directive 2013/40/EU. The most fundamental works observed in this paper regarding the Directive are written by Ioannis Iglezakis[8], Krestina Brezinova[9], Libor Klimek[10].

The originality of the work lies in the detailed analysis of the Directive from the perspective of its implementation in the Member States' legislation and relevant court practice; and in the comparative analysis of the Ukrainian legislation regarding its conformity to the Directive minimum standards.

---

[5] SUMMERS S., SCHWARZENEGGER CH., EGE G., YOUNG F., *The Emergence of EU Criminal Law*. *Cyber Crime and the Regulation of the Information Society.* Oxford and Portland, Oregon: Hart Publishing 2014. P. 327.
[6] Ibid.

[7] HERT P., FUSTER G., KOOPS B., Fighting cybercrime in the two Europes: The added value of the EU framework decision and the council of Europe Convention. *Revue internationale de droit pénal*, vol. 77(3), 2006, p. 505. [interactive]. [reviewed in 10 May 2020]. Available at: <https://www.researchgate.net/publication/251058766_Fighting_cybercrime_in_the_two_Europes_The_added_value_of_the_EU_framework_decision_and_the_Council_of_Europe_convention>
[8] IGLEZAKIS I. *The legal regulation of Cyber Attacks.* 2016. Kluwer Law International B. V.: the Netherlands. P. 256.
[9] BŘEZINOVÁ K. *Company Criminal Liability for Unlawful Attacks against Information Systems within the Scope of EU Law.* Charles University in Prague Faculty of Law Research Paper No. 2017/II/3., 5 June 2017. P. 27. [interactive]. [reviewed in 2 March 2020]. Available at: <https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID2989005_code2308341.pdf?abstractid=2989005&mirid=1&type=2>
[10] KLIMEK L. Criminal Liability of Legal Persons in Case of Computer Crime: A European Union Response. International and Comparative Law Review, 2015, vol. 15, no. 2, p. 135-142. [interactive]. [reviewed in 2 April]. Available at: <https://www.researchgate.net/publication/322710330_Criminal_Liability_of_Legal_Persons_in_Case_of_Computer_Crime_A_European_Union_Response>

PART I. CRIMINAL LAW PROVISIONS UNDER CYBERSECURITY POLICY: THE EU AND UKRAINIAN APPROACHES

Part I. Chapter I. The place of the Directive 2013/40/EU among the international legislation regulating attacks against information systems

Cyberspace is a unique place for committing crimes as it creates a possibility for the offender to attack the information system halfway around the world. Consequently, an offender is looking for the most 'preferential' jurisdiction where several acts are not criminalized or may be considered minor, where the extradition is very low possible, or where the law-enforcement system is not adapted to investigate offences utilizing high-technologic means, in order to avoid liability for committed offences. The transnational dimension of cybercrime requires to create international harmonization legal instruments to settle common rules of determination the conduct as a crime and similar level of sanctions, establish rules for effective cooperation between countries towards investigation and prosecution attacks against information systems.

In order to fight cybercrime on the international level, in 2001, the Budapest Convention on Cybercrime was adopted[11]. 'The Convention is a collective response by members of the Council of Europe (46 States) and some non-member States to the challenge of cyber-crime'[12]. It was addressed to both material and procedural issues aiming to harmonize the national legislation of signors: prescribe common definitions of crimes against information systems, settle common investigation rules and increase international cooperation between countries through existing and new means of contact and communication[13].

Although the Budapest Convention, which is considered to be 'a first important international binding legal instrument to address the issue of cybercrime'[14], was signed by

[11] 2001. Convention on Cybercrime. *European Treaty Series*. No. 185. [interactive]. [reviewed in 10 May 2020]. Available at: <http://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561>

[12] CSONKA, P. The Council of Europe's convention on cyber-crime and other European initiatives. *Revue internationale de droit pénal*, vol. 77(3), 2006.P. 482. [interactive]. [reviewed in 10 May 2020]. Available at: < https://www.cairn.info/revue-internationale-de-droit-penal-2006-3-page-473.htm>

[13] Ibid, pp. 482-483.

[14] HERT P., FUSTER G., KOOPS B., Fighting cybercrime in the two Europes: The added value of the EU framework decision and the council of Europe Convention. *Revue internationale de droit pénal*, vol. 77(3), 2006, p. 505. [interactive]. [reviewed in 10 May 2020]. Available at: <https://www.researchgate.net/publication/251058766_Fighting_cybercrime_in_the_two_Europes_The_added_value_of_the_EU_framework_decision_and_the_Council_of_Europe_convention>

many countries yet in 2001, the states did not haste to ratify it[15]. The Convention does not include the threshold date for its ratification. Therefore, it became impossible to predict the time of approximation of the national legislation within signatory states, and the EU needed to establish its own effective legal instrument.

The Maastricht Treaty established the three-pillar structure of the EU[16], where the third pillar contained 'the Union competence in the field of Justice and Home Affairs'[17]. After the amendments of the Amsterdam Treaty the third pillar was narrowed to the 'Police and Judicial Co-operation in Criminal Matters'[18]. With the purpose of legal approximation, the Amsterdam Treaty introduced a new binding legal instrument of the framework decision[19].

'On 24th February 2005, the Council of the European Union (EU) adopted Framework Decision 2005/222/JHA on attacks against information systems with the objective of improving cooperation between judicial and other competent authorities, including the police and other specialised law enforcement services, through approximating national rules on criminal law in the area of attacks against information systems'[20].

The Framework decision has more limited scope comparing with the Convention as it is addressed only to EU Member-states and covers only three types of offences prescribed by the Convention: illegal access, illegal system interference and illegal data interference[21]. The Framework decision adopted the Convention approach to allow countries to decide whether to establish the element of 'breaching the security measure' as mandatory in case of illegal access and to define minor cases out of criminalization[22]. In contrast to the Convention, the Framework Decision established the deadline on the 16 March 2007 – till

[15] Chart of signatures and ratifications of Treaty 185 *Convention on Cybercrime.* [interactive]. [Reviewed in 03 May 2020]. Available at: <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures>

[16] MITSILEGAS V. *EU Criminal Law.* Oxford and Portland, Oregon: Hart Publishing 2009. P. 9

[17] Ibid., p. 10.

[18] SUMMERS S., SCHWARZENEGGER CH., EGE G., YOUNG F., *The Emergence of EU Criminal Law. Cyber Crime and the Regulation of the Information Society.* Oxford and Portland, Oregon: Hart Publishing 2014. p. 7.

[19] MITSILEGAS V. *EU Criminal Law.* Oxford and Portland, Oregon: Hart Publishing 2009. P. 16.

[20] DE HERT, P., GONZÁLEZ FUSTER, G. & KOOPS, B., Fighting cybercrime in the two Europes: The added value of the EU framework decision and the council of Europe Convention. *Revue internationale de droit pénal*, vol. 77(3), 2006, p. 505.

[21] Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems. *Official Journal of the European Union.* No. L 69/67. 16 March 2005. [interactive]. [reviewed in 3 May 2020].
Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32005F0222&from=EN>

[22] DE HERT, P., GONZÁLEZ FUSTER, G. & KOOPS, B., Fighting cybercrime in the two Europes: The added value of the EU framework decision and the council of Europe Convention. *Revue internationale de droit pénal*, vol. 77(3), 2006, p. 505-506.

this date, the national legislation of Member States had to be brought into conformity with the provisions of the Framework decision.

The Treaty of Lisbon, which was signed in 2007 and entered into force in 2009, abolished the three-pillar structure[23]. The new framework has led to changes in the legal regulation system, inter alia, in the field of substantive criminal law. In particular, the Treaty 'provides for the conversion of framework decisions into directives'[24]. Directives oblige the Member States to incorporate directive provisions into their national legislation until the specified date, defined in the Directive.

According to the article 83 TFEU 'The European Parliament and the Council may, by means of directives adopted in accordance with the ordinary legislative procedure, establish minimum rules concerning the definition of criminal offences and sanctions in the areas of particularly serious crime with a cross-border dimension (including computer crime) resulting from the nature or impact of such offences or from a special need to combat them on a common basis'[25].

Directive 2013/40/EU on attacks against information systems[26] was adopted on 12 August 2013 and replaced Council Framework Decision 2005/222/JHA.

'The purpose of the Directive is to create a common framework in the attacks against information systems, by establishing 'minimum rules concerning the definition of criminal offences and sanctions' in that field. The directive aims to tackle large-scale cyberattacks by requiring Member States to strengthen national cybercrime legislation and to introduce strict criminal sanctions.'[27]

Comparing with the Framework Decision, the Directive has broadened the scope of offences it is addressed to. Apart from the offences previously prescribed in the Framework decision (illegal access (art. 3), illegal system (art. 4) and data interference (art. 5), the

---

[23] CALDERONI F., The European legal framework on cybercrime: Striving for an effective implementation. *Crime, Law and Social Change* 54, 5 (2010) P. 15. [interactive]. [reviewed in 3 May 2020]. Available at: <https://www.researchgate.net/publication/227301292_The_European_legal_framework_on_cybercrime_Striving_for_an_effective_implementation>

[24] SUMMERS S., SCHWARZENEGGER CH., EGE G., YOUNG F., *The Emergence of EU Criminal Law*. *Cyber Crime and the Regulation of the Information Society.* Oxford and Portland, Oregon: Hart Publishing 2014. p. 46.

[25] Consolidated version of the Treaty on the Functioning of the European Union. *Official Journal of the European Union.* No. C 326/47. 26 October 2012. [interactive]. [reviewed in 10 May 2020]. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012E/TXT&from=EN>

[26] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA. *Official Journal of the European Union.* No. L 218/8. 14 August 2013. [interactive]. [reviewed in 10 May 2020]. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013L0040&from=EN>

[27] BIASIOTTI M. A., PIA J., *Handling and Exchanging Electronic Evidence Across Europe.* Springer, 2018. P. 171.

Directive obliges Member States to provide a relevant legislation on punishment for illegal data interception (art. 6) and illegal conduct linked to the tools for committing all offences mentioned before (art. 7). The Directive established several amendments to the aggravating circumstances. Regarding the wide-spread utilizing of 'botnets' as a tool to commit cyberattacks[28], the Directive established a rule of the imposition of harsher penalties 'where a significant number of information systems have been affected through the use of a tool, referred to in Article 7, designed or adapted primarily for that purpose'[29].

In addition to the circumstances prescribed in the Framework Decision (commitment in the framework of criminal organization and causing the serious damage[30]), the Directive included in the list of aggravating circumstances the commitment of the attack against critical infrastructure information system[31].

Another aggravating circumstance stipulated by the Directive in case 'any of the mentioned offences is committed by misusing the personal data of another person, with the aim of gaining the trust of a third party, thereby causing prejudice to the rightful identity owner'[32].

The Directive added some rules of jurisdiction establishment and did not include the method of jurisdiction conflict resolution, but instead referred to the Council Framework Decision 2009/948/JHA of 30 November 2009 on prevention and settlement of conflict of jurisdiction in criminal proceedings[33] .

Another essential changes, introduced in the Directive, are related to the procedural issues, in particular, exchange of information, monitoring and statistic. The last consists of obligation to collect and transmit statistical data to the Commission (art. 14). The information exchange was already introduced in the Framework Decision but the Directive added a rule of 8 hours for answers to urgent requests and generally aims to improve cooperation between Member States and within the State through effective work (without delays) of contact points and report channels (art. 13)[34].

---

[28] ENISA. The Directive on attacks against information systems. A Good Practice Collection for CERTs on the Directive on attacks against information systems. P/28/12/TCD, Version: 1.5, 24 October 2013. P. 3. [interactive]. [reviewed in 2 March 2020]. Available at: <https://www.enisa.europa.eu/publications/the-directive-on-attacks-against-information-systems/at_download/fullReport>

[29] Directive 2013/40/EU. Art. 9, p. 3.

[30] Framework Decision. Art. 7.

[31] Directive 2013/40/EU. Art. 9, p. 4c.

[32] Directive 2013/40/EU. Art. 9, p. 5.

[33] Directive 2013/40/EU. Recital 27.

[34] ENISA. The Directive on attacks against information systems. A Good Practice Collection for CERTs on the Directive on attacks against information systems. P/28/12/TCD, Version: 1.5, 24 October 2013. P. 4. [interactive]. [reviewed in 2 March 2020]. Available at: <https://www.enisa.europa.eu/publications/the-directive-on-attacks-against-information-systems/at_download/fullReport>

The provisions of the Directive will be analyzed in detail in the following chapters.

Part I. Chapter II. Ukrainian legislation

Ukraine signed the Cybercrime Convention on 23 November 2011 and ratified it on 7 September 2005[35]. However, the implementation process is continuing.

Examining the implementation of the first category of the offences introduced in the Convention, named 'Offences against the confidentiality, integrity and availability of computer data and systems' which are also prescribed in the Directive 2013/40/EU, it can be concluded that relevant criminal legislation corresponding to the Cybercrime Convention was established. However, as the Directive does not fully replicate the Convention provisions, and stated more precise minimum standards for criminalization of acts committed against information systems, the approximate correspondence of the Ukrainian legislation to the Convention does not mean that it conforms to the standards settled in the Directive.

The Ukrainian legislator tried to cover the offences of illegal access, illegal system interference and data interference under one article. Yes, article 361 of the Criminal Code of Ukraine, named 'unauthorized interference in the operation of computers, networks'[36], prescribes punishment for 'the unauthorized interference in the operation of computers, automated systems, computer networks or telecommunications networks, which led to the consequences of leakage, loss, falsification, blocking of information, distortion of the information processing or violation of its established route'[37]. Simultaneously, the Criminal Code additionally prescribes punishment for illegal data interference (unauthorized alteration, destruction or blocking of information) committed by a person who has a right to access to it under article 362. The offence of illegal system interference committed through massive messages distribution is covered by the article 363-1 of the Criminal Code of Ukraine. The illegal data interference is partly covered by the part 2 of the article 163, which prescribes penalties for 'the violation of the secrecy of correspondence, telephone conversations, telegraph or other correspondence transmitted by means of communication or via computer, committed due to the use of technical means designed for covert receipt

[35] On ratification on the Convention on Cybercrime. Law of Ukraine. 7 September 2005. [interactive]. [reviewed in 2 May 2020]. Available at: <https://zakon.rada.gov.ua/laws/show/2824-15>
[36] The Criminal Code of Ukraine. Law of Ukraine. 5 April 2001. No. 2341-III. [interactive]. [reviewed in 8 May 2020]. Available at: <https://zakon.rada.gov.ua/laws/show/2341-14/ed20010405>
[37] Ibid.

of information'[38]. Also, the Criminal Code of Ukraine introduces penalties for the illegal use of technical means designed for covert receipt of information under article 359 and for illegal collection of confidential information about a person under article 182. Therefore, illegal interception may also be covered by this set of crimes.

The offence of misuse of tools which may be designed to commit cyberattacks is covered by the article 363[1] of the Criminal Code of Ukraine, which stipulates the penalties for the 'creation for the use, distribution or sale of malicious software or hardware, as well as their distribution or sale'[39].

Most of the mentioned offences are established in section 16 of the Criminal Code of Ukraine, named 'Crimes in the field of use of computers, systems and computer and telecommunication networks'[40]. Also, this section includes some offences which are not stipulated by the Convention on Cybercrime, and does not include some prescribed by the Convention.

There is no definition of cybercrime or cyberspace in the Criminal Code of Ukraine. These terms are defined in the Law of Ukraine 'On the basic principles of cybersecurity in Ukraine'[41]. Therefore, the question may arise, whether it is correct to call crimes committed against information systems cybercrimes. However, for the purposes of this paper, the term 'cybercrime' meaning computer crime will be used.

If the provisions of Cybercrime Convention on substantive law are generally covered, the situation with the implementation of the procedural provisions is more difficult. For example, Ukraine did not implement provisions on the expedited preservation of stored computer data (art. 16) and on the expedited preservation and partial disclosure of traffic data[42]. Provisions of the Criminal Procedural Code on the temporary access to objects and documents cannot be applied in this case, as procedures fulfilled under them cannot be considered as expedited. Consequently, as there is no established mechanism for the expedited preservation of data, the provisional measures prescribed by the articles 29 and 30 of the Convention cannot be fulfilled by the 24/7 contact point of Ukraine within the international cooperation. Therefore, the problems on mutual legal assistance regarding no-implemented actions may also arise. Partially, the measures of improvement of the

[38] Ibid.
[39] Ibid.
[40] Ibid.
[41] On the basic principles of cybersecurity in Ukraine. Law of Ukraine. 10 May 2017.No. 2163-VIII. [interactive]. [reviewed in 9 May 2020]. Available at: <https://zakon.rada.gov.ua/laws/show/2163-19>
[42] Ukraine status regarding Budapest Convention. Council of Europe. [interactive]. [reviewed in 5 May 2020]. Available at: <https://www.coe.int/en/web/octopus/country-wiki/-/asset_publisher/hFPA5fbKjyCJ/content/ukraine/pop_up?inheritRedirect=false>

Ukrainian legislation are established in the Cybersecurity Strategy of Ukraine[43]. However, to reach effective results, concrete legal amendments have to be established.

Under article 22 of the Association Agreement concluded between the EU and Ukraine on 29 May 2014, the Parties agreed to 'cooperate in combating and preventing criminal and illegal activities'[44], including *inter alia* cybercrime. 'The Parties shall enhance bilateral, regional and international cooperation in this field, including cooperation that involves Europol. The Parties shall further develop their cooperation as regards, inter alia: the exchange of best practice, including on investigation techniques and crime research; the exchange of information in line with applicable rules; capacity-building, including training and, where appropriate, the exchange of staff; issues relating to the protection of witnesses and victims'[45].

Notwithstanding the fact that the Action plan for the implementation of the Association Agreement[46] does not include tasks regarding the adoption of the Directive 2013/40/EU provisions, I think that Ukrainian legislator should encourage amendments directed to the approximation *inter alia* criminal legislation on cybercrime to the European standards, in particular to those established in the Directive 2013/40/EU. For this reason, the conformity of the Directive provisions and Ukrainian relevant legislation will be analyzed in detail in the following chapters.

[43] On the decision of the National Security and Defense Council of Ukraine of January 27, 2016 'On the Cybersecurity Strategy of Ukraine'. Decree of the President of Ukraine. No. 96/2016. 15 March 2016. [interactive]. [reviewed in 11 May 2020]. Available at: <https://zakon.rada.gov.ua/laws/show/96/2016>

[44] Association Agreement between the European Union and its Member States, of the one part, and Ukraine, of the other part. *Official Journal of the European Union.* L 161/3. 29 May 2014. [interactive]. [reviewed in 9 May 2020]. Available at: <https://trade.ec.europa.eu/doclib/docs/2016/november/tradoc_155103.pdf>

[45] Ibid.

[46] On the implementation of the Association Agreement between Ukraine, of the one part, and the European Union, the European Atomic Energy Community and their Member States, of the other part. Regulation of the Cabinet of Ministers of Ukraine. 25 October 2017. No. 1106. [interactive]. [reviewed in 9 May 2020]. Available at: <https://zakon.rada.gov.ua/laws/show/1106-2017-%D0%BF>

PART II. TYPES OF THE OFFENCES PRESCRIBED BY THE DIRECTIVE 2013/40/EU

Part II. Chapter I. An illegal access

The first type of the offence prescribed by the Directive 2013/40/EU is illegal access. According to the Article 3 'Member States shall take the necessary measures to ensure that, when committed intentionally, the access without right, to the whole or to any part of an information system, is punishable as a criminal offence where committed by infringing a security measure, at least for cases which are not minor'[47].

Although the wording prescribing the offence was changed in comparison with the Article 2 of the Framework Decision, the general approach is saved: the Member States are allowed to choose whether to incriminate the illegal access if there was no security measure or not.

The interesting fact is that the proposal for the Directive did not contain such an option meaning any illegal access has to be deemed as a crime under the Directive regardless of the fact of breaching the informational system protection measures. According to this approach, even unprotected system may be hacked and this action must be incriminated as illegal access in the Member States' legislation[48]. Nevertheless, the concept did not find its establishment in the Directive which requires criminalization only in case of the 'infringing a security measure'.

However, Kristýna Březinová, comparing the wording of Article 3 of Directive and Article 2 of Framework Decision, concluded that 'illegal access to an information system executed without infringing a security measure, it is no longer a criminal offence'[49]. She is confident of the fact that Directive wording of an illegal access offence stated in Article 3 established a new approach of decriminalization of the illegal access without breaching the security measure meaning such actions are 'unworthy to be protected by means of a

[47] Directive 2013/40/EU.

[48] The Directive on attacks against information systems. A Good Practice Collection for CERTs on the Directive on attacks against information systems ENISA P/28/12/TCD, Version: 1.5, 24 October, 2013. P. 9. [interactive]. [reviewed in 2 March 2020]. Available at: <https://www.enisa.europa.eu/publications/the-directive-on-attacks-against-information-systems/at_download/fullReport>

[49] BŘEZINOVÁ K. *Company Criminal Liability for Unlawful Attacks against Information Systems within the Scope of EU Law.* Charles University in Prague Faculty of Law Research Paper. No. 2017/II/3., 5 June 2017. P. 13-14. [interactive]. [reviewed in 2 March 2020]. Available at: <https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID2989005_code2308341.pdf?abstractid=2989005&mirid=1&type=2>

European Union directive and consequently by national legislations in the area of criminal law'[50].

I do not agree with such an interpretation of the Directive provisions. In my opinion, this wording does not forbid the Member States to criminalize the illegal access without breaching the security measure (or access obtained in another way) in the national legislation and at the same time obliges the Member States to define the illegal access infringing the security measure as a crime in their national legislation.

Moreover, according to the information given in 'A Good Practice Collection for CERTs on the Directive on attacks against information systems' prepared in 2013 by ENISA – 'a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens'[51] - 'the Directive does not require any changes as compared to the Framework Decision, and legislation in all Member States can thus remain 'as is''[52]

According to the Section 138ab (1) of the Criminal Code of the Kingdom of Netherlands: 'Any person who intentionally and unlawfully gains entry to a computerized device or system or a part thereof shall be guilty of computer trespass...

Unlawful entry shall be deemed to have been committed if access to the computerized device or system is gained:

a. by breaching a security measure,

b. by a technical intervention,

c. by means of false signals or a false key, or

d. by assuming a false identity'.[53]

This wording of the article demonstrates that breaching a security measure is only one of the possible options to obtain access to the computer system illegally. But it has to be introduced in the Criminal Code in order to keep the national legislation of the Netherlands in accordance with EU Directive requirements.

[50] Ibid.

[51] The Directive on attacks against information systems. A Good Practice Collection for CERTs on the Directive on attacks against information systems ENISA P/28/12/TCD, Version: 1.5, 24 October, 2013. P. 2. [interactive]. [reviewed in 2 March 2020]. Available at: <https://www.enisa.europa.eu/publications/the-directive-on-attacks-against-information-systems/at_download/fullReport>

[52] Ibid., p. 9.

[53] The Criminal Code of the Kingdom of Netherlands (1881, amended on 2012). English version. [interactive]. [reviewed in 2 March 2020]. Available at: <https://www.legislationline.org/download/id/6415/file/Netherlands_CC_am2012_en.pdf>

The Criminal code of the French Republic (art. 323-1) established the wording of 'Fraudulently accessing or remaining within all or part of an automated data processing system'[54].

The practice of French courts demonstrates that access to the informational system cannot be fraudulent if the system is unprotected. During pending relevant cases judges make an assessment of the infringements of the security measures[55]. For instance, in the case *'Tati vs Kitetoa'* the journalist from France, named Antoine Champagne, was searching for 'holes' in companies' systems assuming the results on the website 'kitetoa.com'. Mostly, it was a way of earning money for him as after finding these systems holes he helped to fix them. Nevertheless, the Tati company sued Kitetoa also complaining on cracking their network and fraudulent access to the Tati databases. Opposing the claim, Champagne alleged that he used only 'open proxies on their system to access documents freely available on the system'[56] . The Court of appeal found Antoine Champagne non-guilty for committing a crime under the Article 323-1 as he 'cannot be accused of having access to or staying in the parts of the sites which can be reached by the simple use of a general public navigation software, these parts of the site, which are by definition not the object of any protection on the part of the operator of the site or of its service provider, having to be deemed not confidential in the absence of any indication to the contrary and of any obstacle to access'.[57]

Returning to Article 323-1 of the French Criminal Code I would like to draw your attention that French legislator criminalized not only the fraudulent accessing but also remaining within the system. There is one interesting case related to that provision, named *'Bluetouff case'*. 'Bluetouff' is a nickname of Mr. Olivier L., who obtained access to 'the French National Agency for Food Safety, Environment and Labor (ANSES)'[58] database

[54] The Criminal Code of the French Republic (as of 2005). English version. [interactive]. [reviewed in 2 March 2020]. Available at: <https://www.legislationline.org/download/id/3316/file/France_Criminal%20Code%20updated%20on%2012-10-2005.pdf>

[55] The Directive on attacks against information systems. A Good Practice Collection for CERTs on the Directive on attacks against information systems ENISA P/28/12/TCD, Version: 1.5, 24 October, 2013. P. 9-10. [interactive]. [reviewed in 2 March 2020]. Available at: https://www.enisa.europa.eu/publications/the-directive-on-attacks-against-information-systems/at_download/fullReport>

[56] ADAMS A. A., MCCRINDLE R. J., *Pandora's Box: Social and Professional Issues of the Information Age.* John Wiley&Sons Ltd. 2008. p. 12.

[57] Judgment of the Paris Court of Appeal. 30 October 2002. Case of Tati against Kitetoa.com. Hereafter unless another indicated, the translation is mine. [interactive]. [reviewed in 3 March 2020]. Available at: <https://www.kitetoa.com/Pages/Textes/Les_Dossiers/Tati_versus_Kitetoa/arret-cour-appel.shtml>

[58] BENSOUSSAN A. Unauthorized access to IT systems. *The Lexing Network informs you. Special International issue.* 2014 (7). P. 12. [interactive]. [reviewed in 6 April]. Available at: <https://www.alain-bensoussan.com/wp-content/uploads/2014/06/24295061.pdf>

and published some confidential information. 'He was prosecuted for fraudulent access and fraudulent remaining in an automated data processing system as well as theft of computer files'.[59] Although the Trial Court found him to be non-guilty, the Paris Court of Appeals 'confirmed there was no offense of fraudulent access to an IT system on the grounds that access (...) was actually allowed due to a technical failure in the login feature existing in the system, a failure that had been recognized by ANSES'[60].

However, regarding other offences the court ruling was changed and Bluetouff was found guilty. The Court of Appeal stressed that, after Bluetouff had obtained access, he was able to notice the authentication requirements of the website. Therefore, obviously that he was aware of the fact, that data is protected, and despite this, he continued surfing the website and collecting the data. Later the judgement was upheld by the French Court of Cassation.[61]

According to the Recital 17 of the Directive Preamble 'labour disputes as regards the access to and use of information systems of an employer for private purposes, should not incur criminal liability where the access under such circumstances would be deemed unauthorized and thus would constitute the sole basis for criminal proceedings'[62]. However, the question may arise whether to criminalize acts of illegal access committed by former workers.

To answer the question, the relevant case should be observed. In Italy, a worker received a notice of his resignation. After that, as he still knew the password, he entered the system without breaching a security measure and copied some company data. The Court found that disregarding the absence of the breach of the security measure, his access was unauthorized. Even the intent of his conduct is irrelevant as he had no right to enter the system if he did not work for the company anymore. Finally, he was accused of illegal access prescribed by the Article 615-ter of the Penal Code of Italy.[63]

As we can see, unlawful access to the information system is possible to commit without the breach of the security measure, and this act does not fall under the definition of labour dispute, which is out of criminal liability. Consequently, I think that for the offence

[59] Ibid.
[60] Ibid. p. 13.
[61] WATIN-AUGOUARD M. Data theft: the French Court of Cassation refines the Godfrain Law. *Fic Observatory.Com.* 4 August 2015. [interactive]. [reviewed in 5 March 2020]. Available at: <https://observatoire-fic.com/en/data-theft-the-french-court-of-cassation-refines-the-godfrain-law/>
[62] Directive 2013/40/EU.
[63] STANCHI A., PEDRONI A. *Unauthorised access of computer system by former employee.*13 April 2016. [interactive]. [Reviewed in 2 March 2020]. Available at: https://www.internationallawoffice.com/Newsletters/Employment-Benefits/Italy/Stanchi-Studio-Legale/Unauthorised-access-of-computer-system-by-former-employee#

of illegal access the essential element is the existence of security measure but not the breach of this measure. Therefore, I agree with the position that serious illegal access without breaching the security measure is worth to be determined on the Directive level in order to be punished in all Member States[64].

Nevertheless, as the Directive defined the breaching of the security measure as a mandatory dimension of an offence of illegal access, it has to be taken into account as we analyze minimum standards introduced by the Directive.

Examining the intent requirements of the offence, the Directive adopted from the Framework Decision and established a stricter rule in comparison with the Convention on Cybercrimes. The article 3 of the Directive obliges the Member States to punish illegal intentional access to informational system disregarding whether the offender had an intent to steal or modify information in contrast to the article 3 of the Convention which allowed to criminalize the relevant misconduct subject to the availability of '*the intent of obtaining computer data or other dishonest intent*'[65].

Consequently, offence of illegal access under the Directive is deemed to be intentional if the intent to breach the security measure exists. As it is impossible to figure out the evidence of the intent if the system has no protection measures, the same as to apply the 'without right' test, the access to the unprotected system cannot be punished as a criminal offence. The level of protection, meanwhile, is irrelevant as even a least attempt to find out a password or security key demonstrates the intent to reach the system which is not freely accessible. The security measure quality may be an essential issue when the perspective of civil liability of the affected company arises, but it does not make influence on the criminal liability of the offender.

The exclusion might be if the person did not know that the access was unauthorized and acted without any criminal intent as prescribed by the Recital 17 of the Directive Preamble.

The question may arise about the aim of 'single' access to the data. If the offender has obtained access to the system in order to alter or delete the information contained, his actions have to be qualified as illegal access (art. 3) and illegal data interference (art. 5). However, these actions may be committed independently to each other. For instance, the

[64] FREITAS P., GONÇALVES N. Illegal access to information systems and the Directive 2013/40/EU, *International Review of Law, Computers & Technology*, 29:1, 2015. P. 59. [interactive]. [reviewed in 12 May 2020]. Available at: <https://www.tandfonline.com/doi/full/10.1080/13600869.2015.1016278>
[65] Convention on Cybercrime.

illegal access without an intent to affect the data or the system is possible in case of '*grey hacking'*.

In fact, the offenders committing an illegal access, called 'hackers', are non-officially divided into three groups: 'white, grey and black hats'[66].

The conduct of 'white hackers' is out of the criminal liability as they commit authorized access according to the concluded agreement with the company in order to find 'holes' and weaknesses of the system, fix them and, as a result, improve the security system and prevent the possible attacks against it. For such kind of service, they acquire a fair payment and do not act illegally. The 'black' hackers usually move beyond the measures of illegal access and additionally steal or affect the data or the whole system. As a result, they are liable for several offences.[67]

The more difficult situation is with 'grey hats' whose conduct is partly similar to 'white hats', but they look for the weaknesses of the system and 'hack' it without the permission of the company[68]. Grey hackers appear after committing of the unlawful reaching the system and offer to fix the problems with security measures for a remuneration. This offer may be regarded as demand due to its nature as a company owner realizes the possible negative consequences of his or her refusal (e. g. the information will be deferred to the unfair competitor or even be published that may lead to the worse effect.) As the act of the grey hacker is impossible to qualify as extortion or fraud, the liability for illegal access as a separate offence has to be prescribed by the national law.

According to the Directive standards the intentional access without right to the protected informational system in case of breaching the security measure – exactly as a gray hacking - is illegal and has to be punished without taking into account the absence of the intent to affect the system or contained data.

Analyzing the Ukrainian legislation, the Criminal Code of Ukraine does not contain a separate article stipulating punishment for illegal access. The article 361 of the Criminal Code of Ukraine, named unauthorized interference, prescribes punishment for 'unauthorized interference into the operation of electronic computers (computers), automated systems, computer networks or telecommunication networks, which led to leakage, loss, falsification, blocking of information, distortion of the information

[66] What is the Difference Between Black, White and Grey Hat Hackers? *Norton.* [Interactive]. [Reviewed in 5 March 2020]. Available at: <https://us.norton.com/internetsecurity-emerging-threats-what-is-the-difference-between-black-white-and-grey-hat-hackers.html>
[67] Ibid.
[68] Ibid.

processing or to violation of its established route'[69]. This article is deemed to be general, covering offence of illegal access and illegal interference, meaning that access is already a system interference. For example, the leakage of information means that the secured information becomes accessible to others (individuals or legal persons) who do not have a right to access to it[70]. Furthermore, the leakage of information takes place even if the only one person obtains the access to information without right.[71]

However, the definition of the leakage of information does not answer the question whether the perpetrator has to commit additional actions which lead to the leakage (e. g. copy the information) or at least the access to the system is already an act which led to the leakage and has to be punished under the article 361 of the Criminal Code. Moreover, the illegal access to the information system is prescribed in article 212^6 of the Code of Ukraine of administrative offences and the act of 'illegal access to information stored, processed or transmitted in information (automated) systems'[72] may be punished by the low administrative fine.

The problem of distinguishing whether to impose criminal or administrative penalties may arise. V. Antypov argues that the distinction is based on the existence of socially dangerous consequences (leakage, loss of data, etc.).[73] Observing the court practice, it is difficult to come to the same conclusion (also because the term 'leakage' is imprecise). Mostly, administrative offences are committed by state authorities' employees who get unauthorized access to the information system of the Office while only the Head of the Office has a right to access. For example, the head of the sector of technical policy and use of forest resources Office was found guilty under the article 212^6 (part 1) of the Code of Ukraine of administrative offences 'to illegal access to the information system, which allowed him to get acquainted, receive and transmit official information to a public authority'[74] as he used an email account of the Office without right. In another case an

[69] The Criminal Code of Ukraine. Law of Ukraine. 5 April 2001. No. 2341-III. [interactive]. [reviewed in 8 May 2020]. Available at: <https://zakon.rada.gov.ua/laws/show/2341-14/ed20010405>

[70] Науково-практичний коментар Кримінального кодексу України за редакцією М. І. Мельника, М. І. Хавронюка. 11-те вид., переробл. та допов. Київ: ВД «Дакор», 2019. С. 1114

[71] МУЗИКА А., АЗАРОВ Д., *Законодавство України про кримінальну відповідальність за "комп'ютерні" злочини: науково-практичний коментар і шляхи вдосконалення*. К.: Вид. ПАЛИВОДА А. В., 2005. С. 27.

[72] The Code of Ukraine of Administrative offences. Law of Ukraine. 7 December 1984. No. 8073^1-X. [interactive]. [reviewed in 7 May 2020]. Available at:< https://zakon.rada.gov.ua/laws/show/80731-10/ed20200428>

[73] АНТИПОВ В. Диспозиції статей Кримінального кодексу України з кваліфікованими складами злочину потребують корегування. *Міжнародний юридичний вісник: актуальні проблеми сучасності (теорія та практика).*2017 (1) - С. 40. [interactive] [reviewed in 05 May 2020]. Available at: < http://nbuv.gov.ua/UJRN/muvnudp_2017_1_8>

[74] Judgement of Pervomaisky District Court of Chernivtsi. 14 August 2019. No. 725/3848/19. [interactive]. [reviewed in 7 May 2020]. Available at: <http://www.reyestr.court.gov.ua/Review/83693746>

offender was found guilty to the same offence because he without right 'made access to information stored and processed electronically in the automated system of the district state administration'[75] – opened and read the file named 'Letter on the socio-political situation in the area' during staying in the waiting room of the Head of the administration. I think, in this case the leakage of data took place. However, it could not lead to serious public danger consequences, therefore, the administrative penalties were imposed. Additionally, although the access was without right, there was no breach of the security measure.

In another case, the offender was found criminally liable under article 361 of the Criminal Code of Ukraine exactly for the fact of illegal access to the email account of his former employer. After he obtained access to the mailbox due to utilizing passwords copied before (in the times of his work), the offender got the information stored on the mail server mercedes-benz.dp.ua. The Court has found that in the case took place 'a leakage of the confidential and commercial information of customers of the former employer, which the offender tried to use in his own business'[76]. Obviously, this case leads to more serious public danger consequences than cases observed before. However, I do not think that a leakage of data shall be a threshold of defining the public danger level of the offence as it may take place in different cases. In my opinion, the boundary between criminal and administrative penalties for illegal access bases on the level of seriousness of the consequences not on their sole existence.

In general, I do not agree with the approach of Ukrainian Criminal Code, as the acts of access and interference are different by their nature, also considering that the interference may be preceded by an access. An access is focused on hacking the system (as a main purpose) and may be followed by acts affecting data. It can be committed as an independent crime without an intent to hinder the system or interrupt its functioning process. Observing the European legislation on offences against information systems becomes noticeable that penalties for illegal access and illegal interference are different due to the different level of public danger. The Criminal Code of the French Republic even imposes different penalties for just an access, access with harmful effect (data modification or alteration the functioning of the system) and system interference as a separate crime[77].

---

[75] Judgement of Nizhyn City District Court. 9 April 2020. No. 740/684/20. [interactive]. [reviewed in 7 May 2020]. Available at: <http://www.reyestr.court.gov.ua/Review/88689172>

[76] Judgment of Amur-Nizhnedneprovsky District Court of Dnipropetrovsk. 2 July 2013. No. 1-726 / 11. [interactive]. [reviewed in 7 May 2020]. Available at: <http://www.reyestr.court.gov.ua/Review/45323511>

[77] The Criminal Code of the French Republic (as of 2005). English version. [interactive]. [reviewed in 2 March 2020]. Available at: <https://www.legislationline.org/download/id/3316/file/France_Criminal%20Code%20updated%20on%2012-10-2005.pdf>

Consequently, I would offer the following changes to the Ukrainian legislation relating to the illegal access in order to approximate it with the European standards:

1) Separate the offence of illegal access from offence of the system interference. The separation may be done within one article (art. 361) under the condition of changing its title (keeping distinguishing the access and the interference) or due to additional article.

2) Provide the criminalization of unauthorized illegal access in case of breaching the security measure without necessary consequences as leakage, loss, falsification, blocking of information as these consequences are peculiar to another offences (system and data interference). For cases, when the unauthorized access leads to the consequences of stealing of the information, the additional provision may be inserted, prescribing harsher penalties. Additionally, cases of illegal access committed by other means different from breaching the security measure, may also be punished depending on its serious consequences.

3) Establish clear rules for the determination of the type of penalties which have to be imposed in case of illegal access (administrative or criminal).

Part II. Chapter II. Illegal system interference

The illegal system interference is the second type of the offence stipulated by the Directive. According to the Article 4 'Member States shall take the necessary measures to ensure that seriously hindering or interrupting the functioning of an information system by inputting computer data, by transmitting, damaging, deleting, deteriorating, altering or suppressing such data, or by rendering such data inaccessible, intentionally and without right, is punishable as a criminal offence, at least for cases which are not minor'[78].

Common features with other offences under the Directive are that interference must be committed: with intention but without right and the interference must not be a minor case. The term "without right" means an absence of consent. For example, this consent might be given by the system manager – a person authorized by the company[79]. Therefore, if the interference occurs under the agreement between such person and outsourced specialist in order to provide certain technical support services, there is no illegal system

[78] Directive 2013/40/EU.
[79] IGLEZAKIS I. *The legal regulation of Cyber Attacks.* 2016. Kluwer Law International B. V.: the Netherlands. P. 63

interference unless the computer specialist does not act strictly according to the agreement provisions in order to affect the system in a negative way.

Another question arises about the intent: whether it must be related to system interference or to the consequences in damage at the same time? For example, in Ukraine, the direct intent is required only for the act of illegal system interference but not for the consequences as the offender is aware of probable negative consequences, although he does not want them to occur[80].

Usually, national courts of the Member state do not constitute the intent of causing damage to be a mandatory element to criminalize an act of illegal interference. Nevertheless, if the interference was not sufficient to disturb the system but there is a strong evidence proving the intent to cause a serious harm, an offender can be pursued for an attempt[81]. According to the part 2 of the Article 8 of the Directive, 'Member States shall ensure that the attempt to commit an offence referred to in Articles 4 and 5 is punishable as a criminal offence'[82].

At first sight, it is difficult to make a distinction between the offences of illegal system interference and illegal data interference. In my opinion, these crimes may be distinguished on the ground of the purpose of their committing and caused damage simultaneously. The illegal system interference is focused on the disruption of the system and may be committed through different harmful actions with data, whereas the illegal data interference does not aim to interrupt or disturb the work of the whole system but rather to affect the data contained in the system. However, if the offender affected data and such actions led to the system interference, his conduct shall be qualified as the illegal system interference disregarding the intent.

The requirement of seriousness of hindering or interruption of the system has to be examined as not every interference is required to be determined as illegal system interference under the Directive. To prove the importance of this requirement, Ioannis Iglezakis cited the examples of court rulings both of which were issued in France.[83] The French Criminal Code (art. 323-2) prescribes a punishment for 'obstructing or interfering with the functioning of an automated data processing system'[84].

---

[80] Науково-практичний коментар Кримінального кодексу України за редакцією М. І. Мельника, М. І. Хавронюка. 11-те вид., переробл. та допов. Київ: ВД «Дакор», 2019. С. 1115.

[81] IGLEZAKIS I. *The legal regulation of Cyber Attacks.* 2016. Kluwer Law International B. V.: the Netherlands. P. 63

[82] Directive 2013/40/EU.

[83] IGLEZAKIS I. *The legal regulation of Cyber Attacks.* 2016. Kluwer Law International B. V.: the Netherlands. P. 62

[84] The Criminal Code of the French Republic (as of 2005). English version. [interactive]. [reviewed in 2 March 2020]. Available at:

In the first case, provided by the author, a man was found unguilty in committing crime under the article 323-2 as he used an automatic system to acquire an information (accessible) from the competitor's website but there was no disruption of the system and consequently no harmful effect to it. Whereas in another case, a person was accused of illegal system interference because of the attacking the email service with plenty of large empty e-letters causing the disturbance of the system which was assessed as a serious perturbation[85].

The Directive defines eight possible means of committing the offence of illegal system interference: inputting computer data, transmitting, damaging, deleting, deteriorating, altering, suppressing data, rendering data inaccessible.

However, according to the Report from the Commission to the European Parliament and the Council assessing the extent to which the Member States have taken the necessary measures in order to comply with Directive 2013/40/EU from 2017, Member States include in their legislation only several possible acts from this list. The most debatable means which are not included in the national legislation of the Member states are 'deteriorating' as it seems to be not clear enough, and 'rendering inaccessible'.[86]

Nevertheless, the system interference by rendering data inaccessible is deemed to be illegal under the Directive. In my opinion, this particular action must be included in the list as it is a popular way to attack a system. For instance, the famous Wannacry ransomware attack affected the medical centers of Great Britain through spreading a malware. As a result, it paralyzed the healthcare system as made the medical records inaccessible to employees.[87]

In fact, 'Wannacry' is 'a computer virus or more precisely a self-spreading worm, meaning that it replicated all by itself, finding new victims, breaking in and launching on the next computer automatically'.[88] A virus (including its different forms) is one of the

<https://www.legislationline.org/download/id/3316/file/France_Criminal%20Code%20updated%20on%2012-10-2005.pdf>

[85] IGLEZAKIS I. *The legal regulation of Cyber Attacks.* 2016. Kluwer Law International B. V.: the Netherlands. P. 62

[86] Report from the Commission to the European Parliament and the Council on assessing the extent to which the Member States have taken the necessary measures in order to comply with Directive 2013/40/EU on attacks against information systems and replacing Council Framework Decision 2005/222/JHA. Brussels, 13 September 2017. P. 7. [interactive]. [reviewed in 8 May 2020]. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017DC0474&from=en>

[87] Brandom R. UK hospitals hit with massive ransomware attack. *THE VERGE.* [interactive]. [reviewed in 5 May 2020]. Available at: <https://www.theverge.com/2017/5/12/15630354/nhs-hospitals-ransomware-hack-wannacry-bitcoin>

[88] WannaCry – the worm that just won't die. Naked Security by Sophos. 2019. [interactive]. [reviewed in 5 May 2020]. Available at: <https://nakedsecurity.sophos.com/2019/09/18/wannacry-the-worm-that-just-wont-die/>

most popular tools used to commit an attack against information system. Virus is a malware (malicious program) which 'infects the information system through installing a malicious code in order to deteriorate the information system or to extract vulnerable personal data from such a system. Usually viruses are transmitted as attachments to an e-mail or in a downloaded file or they can be present in a CD or other device'[89].

For example, Criminal Code of the Republic of Bulgaria highlights the virus among other acts of commission illegal system interference. Article 319 d stipulates punishment for the 'introducing a computer virus in a computer system or in a computer network as well as introducing another computer program which is intended to disrupt the work of a computer system or a computer network or to discover, erase, delete, modify or copy computer data without permission, where such is required, as long as it is not a graver crime'[90].

The most famous kinds of attacks against informational systems are called DoS (denial of service) and DDoS (distribution of denial of service) attacks. The main purpose of both is to make the system or even the whole network inaccessible due to the massive sending of huge data packets (messages containing enormous files) which the system is not able to process and respond to. As a result, the system is overloaded, and its functioning may be interrupted. [91] The main difference between these two types of attacks is that the DoS attack is committed from the single device, whereas the DDoS attack is committed through utilizing a system of connected devices, called a botnet. *'Botnet is a group of computers that are controlled by software containing harmful programs, without their users' knowledge'*[92]. These devices are already infected by a malware. Usually, their owners are not aware of that and cannot imagine that their devices are used for criminal purposes[93].

---

[89] BŘEZINOVÁ K. *Company Criminal Liability for Unlawful Attacks against Information Systems within the Scope of EU Law.* Charles University in Prague Faculty of Law Research Paper No. 2017/II/3., 5 June 2017. P. 16. [interactive]. [reviewed in 2 March 2020]. Available at: <https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID2989005_code2308341.pdf?abstractid=2989005&mirid=1&type=2>

[90] The Criminal Code of the Republic of Bulgaria (1968, amended 2017). English version. [interactive]. [reviewed in 6 March 2020]. Available at: <https://www.legislationline.org/download/id/8395/file/Bulgaria_Criminal_Code_1968_am2017_ENG.pdf>

[91] NAGY H., MEZEI K., The Organised Criminal Phenomenon on the Internet. *Journal of Eastern-European Criminal Law,* vol. 2016 (2). p. 141. HeinOnline.

[92] Cambridge Dictionary. [interactive]. [reviewed in 5 April 2020]. Available at: < https://dictionary.cambridge.org/dictionary/english/botnet>

[93] NAGY H., MEZEI K., The Organised Criminal Phenomenon on the Internet. *Journal of Eastern-European Criminal Law,* vol. 2016 (2). p. 141 - 142. HeinOnline.

Therefore, the DoS attack is a single-source attack, whereas the DDoS attack firstly involves infecting many computers creating 'botnets' and then has a larger power to attack the system. As a result, DDoS attacks create an advanced level of danger for the society. For this reason, the Directive established more severe penalties for crimes involving botnets and demands to criminalize botnets production. The Directive established a higher level of minimum maximum penalties for offences 'where a significant number of information systems have been affected through the use of a tool, referred to in Article 7, designed or adapted primarily for that purpose'[94].

The Criminal Code of Ukraine introduced two possible ways of criminalization of acts of illegal system interference. The first one is stipulated in Article 361: 'unauthorized interference into the operation of electronic computers (computers), automated systems, computer networks or telecommunication networks, which led to leakage, loss, falsification, blocking of information, distortion of the information processing or to violation of its established route'[95].

In fact, although the wording of the article differs from that prescribed in article 4 of the Directive, it corresponds to the Directive requirements. The Directive established serious hindering or interruption of the functioning of the system as the consequences of the system interference which may be caused by any action stipulated in the list (inputting computer data, transmitting, damaging, deleting, deteriorating, altering, suppressing data, rendering data inaccessible). Ukrainian legislator did not establish the means but widened the list of consequences. As a result, damaging, deleting, deteriorating may lead to the loss of data; altering may lead to its falsification; suppressing and rendering the data inaccessible may lead to its blocking; and any of these actions may lead to distortion of the data processing and violation of its established route. The article covers situations when the system was seriously hindered, or its functioning was interrupted as well as situations when only data but not the system was affected. Therefore, the illegal system interference and illegal data interference are covered by the common article. The separation of these two types of offences may be required to distinguish them on the basis of the public danger level. But anyway, the article corresponds to the offence of illegal system interference, prescribed by the Directive.

[94] Directive 2013/40/EU. Art. 9, p. 3.

[95] The Criminal Code of Ukraine. Law of Ukraine. 5 April 2001. No. 2341-III. [interactive]. [reviewed in 8 May 2020]. Available at: <https://zakon.rada.gov.ua/laws/show/2341-14/ed20010405>

The second way is prescribed by Article 363[1] 'Interference with the operation of electronic computers (computers), automated systems, computer networks or telecommunication networks through the mass distribution of telecommunication messages.'[96] The offence takes place if an act of the mass distribution of messages was intentional without the prior consent of the addressees and led to the hindering or interruption of the functioning of computers (computer), automated systems, computer networks or telecommunication networks[97]. The article does not distinguish whether such attack was committed by a single offender or due to the use of a botnet (DDoS attack). For example, in case *№ 296/1022/19* an offender created an automated task for mass distribution messages demanding to receive a callback and a feedback and used to attack the website. As a result, the system was overloaded and the website functioning was violated[98].

In case *№ 331/5129/18* an offender several times carried out the massive distribution of messages using a downloaded program 'LOIC' – software for DDoS attacks – that led to hindering and interruption of functioning of the automated system - personal computer with installed software.[99]

In both cases offenders were found guilty under the part 1 of the article 363[1] of the Criminal Code of Ukraine. The Directive defined using 'botnets' as aggravating circumstance drawing the attention to the danger of such kind of tool affecting the huge number of devices. Consequently, I think that such a qualifying feature of the offence should be included in article prescribing the offence of illegal system interference at least in cases when the botnet was designed or adapted to that purpose. The relevant provision should be included not only in article 363[1], which prescribes DDoS attacks but also in article 361, as botnets may also be used for different attacks.

Part II. Chapter III. Illegal data interference

The third type of the offences prescribed by the Directive 2013/40/EU, is named illegal data interference. According to the Article 5 of the Directive 'Member States shall take the necessary measures to ensure that deleting, damaging, deteriorating, altering or suppressing

[96] Ibid.
[97] Ibid.
[98] Judgement of Koroliovsky District Court of Zhytomyr. 21 February 2019. *No. 296/1022/19.* [interactive]. [reviewed in 5 May 2020]. Available at: <http://www.reyestr.court.gov.ua/Review/80006556>
[99] Judgement of Prymorsky District Court of Mariupol. 4 April 2019. *No. 331/5129/18.* [interactive]. [reviewed in 5 May 2020]. Available at: <http://www.reyestr.court.gov.ua/Review/80937191>

computer data on an information system, or rendering such data inaccessible, intentionally and without right, is punishable as a criminal offence, at least for cases which are not minor'[100].

An article reproduces the wording of article 4 of the Framework Decision. In comparison with the article of the Cybercrime Convention prescribing an offence of illegal data interference, the act of rendering data inaccessible was added to the wording prescribed by the Framework decision, and further was adopted by Directive. Nevertheless, the actus reus of the offence was modified since the Cybercrime Convention only by broadening the list of actions. Therefore, an offence of illegal data interference introduced in the Directive may be partially analyzed through the concept of the same offence previously introduced in the Cybercrime Convention.

According to the Explanatory Report to the Convention on Cybercrime dated from 23 November 2001, the article 4 on data interference aimed to provide protection to computer data and computer program – 'the protected legal interest here is the integrity and the proper functioning or use of stored computer data or computer programs'[101].

The question may arise whether the conduct affecting the computer program has to be qualified as data interference or system interference. The Directive provided us with a definition of computer data, which means 'a representation of facts, information or concepts in a form suitable for processing in an information system, including a programme suitable for causing an information system to perform a function'[102].

At the same time, the Directive defines the information system as 'a device which automatically processes computer data pursuant to a programme'[103]. Consequently, a computer program may be affected by a virus in the extent of the whole information system destruction. In my opinion, an attack against the computer program has to be qualified as illegal data interference unless it causes a serious hindering of the system or interruption of its processing.

Cybercrime Convention allows Parties to punish only those acts of data interference resulted in serious harm (amount defined pursuant to the national legislation)[104]. The Directive does not prescribe the similar provision but contains a relevant one. Yes, the

[100] Directive 2013/40/EU.
[101] Explanatory Report to the Convention on Cybercrime dated on 23 November 2001. European Treaty Series - No. 185. P. 11. [interactive]. [reviewed in 5 May 2020]. Available at: <https://rm.coe.int/16800cce5b>
[102] Directive 2013/40/EU. Art. 2.
[103] Ibid.
[104] Explanatory Report to the Convention on Cybercrime dated on 23 November 2001. European Treaty Series - No. 185. P. 11. [interactive]. [reviewed in 5 May 2020]. Available at: <https://rm.coe.int/16800cce5b>

Directive settled the requirement to punish an act of illegal data interference as a criminal offence, at least for cases which are not minor. However, it does not introduce the rules of determining, whether the case is minor or not. According to the recital 11 of the Directive Preamble 'Member States may determine what constitutes a minor case according to their national law and practice'[105]. Nevertheless, the disputable question is, whether Member states are allowed to establish a threshold of caused harm requiring only serious harm incurring. For example, the Lithuanian approach has been changed. Previously, the Criminal Code of the Republic of Lithuania stipulated punishment for data interference in case of incurring major damage (or serious harm)[106] as it was allowed under the Convention. Further, article 196 of the Criminal Code was modified: an act of data interference incurring damage (not major but any damage) is punishable as a criminal offence[107]. I think that such changes were required under the Directive as not all cases falling behind the serious harm threshold can be considered minor.

In fact, the offence of illegal data interference can be committed independently, for instance, due to spreading a virus; or after committing of an illegal access to the information system (e. g. computer, mobile phone, etc). For example, the case R v Steffan Needham, which was pending before Reading Crown Court, demonstrates the combination of an illegal access and data interference. IT consultant, previously sacked, used a 'former IT colleague's Login ID to enter the system and deleted data related to clients of his former employer from 23 servers'[108]. Needham was found guilty for under section 1 'Unauthorised access' and Section 3 'Unauthorised acts with intent to impair' of Computer Misuse Act 1990[109].

Another approach is introduced in Dutch legislation. Section 350A of the Criminal Code of the Kingdom of Netherlands distinguishes between the 'usual' data interference and data interference committed 'after having unlawfully gained access'[110], prescribing for

[105] Directive 2013/40/EU.
[106] SAULIŪNAS D. Legislation on cybercrime in Lithuania: development and legal gaps in comparison with the Convention on cybercrime. *Jurisprudence.* 2010, 4(122). P. 210–211. [interactive]. [reviewed in 5 May 2020]. Available at: <https://www.mruni.eu/upload/iblock/822/11_Sauliunas.pdf>
[107] The Criminal Code of the Republic of Lithuania (amended 2017). English version. [interactive]. [reviewed in 5 May 2020]. Available at: <https://www.legislationline.org/download/id/8272/file/Lithuania_CC_2000_am2017_en.pdf>
[108] Turner M. Case R v Steffan Needham. *Database: Computer Misuse Act 1990 cases.* [interactive]. [reviewed in 5 May 2020]. Available at: <http://www.computerevidence.co.uk/Cases/CMA.htm>
[109] Ibid.
[110] The Criminal Code of the Kingdom of Netherlands (amended 2012). English version. [interactive]. [reviewed in 5 April 2020]. Available at: <https://www.legislationline.org/download/id/6415/file/Netherlands_CC_am2012_en.pdf>

the last higher maximum penalty. Therefore, under Dutch legislation, two actions (access and data interference) committed with a common purpose are punished under one article.

The question may arise around the requirement 'without right'. Whether it relates to both: access to the data (or the system where this data is contained) and availability to affect the data? Or illegal data interference may take place in case an offender has a right of access to the system and, as a result, to its contained data, but has no right to modify, alter or delete this data?

For example, Article 362 of the Criminal Code of Ukraine establishes a punishment for unauthorized alteration, destruction or blocking of information committed by a person who has the right to access the system containing such data.

Nevertheless, I think that criminalization of such acts is behind of the scope of the Directive. Of course, a person who can reach the data lawfully may abuse his or her right to access the system and wrongfully affect the data through deletion, alteration or suppression. However, if somebody has a right to access, this person, probably, has labour relations with the system owner. I think that observed conduct shall be punished under the criminal law taking into consideration labour relations with a right to an authorized access.

Also, observing 'without right' concept we understand that a person who attacks the data of the company information system under the contractual relationship in order, for example, to check the security system, acts with a right and such conduct is considered to be lawful.

It is crucial to note that among listed actions there is no mention about an illegal obtaining of the information, its spread and use for private purposes. The reason is that these acts may be covered by the article prescribing the offence of an illegal access which led to the negative consequences. To qualify conduct as a data interference, it must lead to some modifications of data or its total disruption.

As we have analyzed before, the purpose of the current offence is to affect the data, not the system. Therefore, the attack against data may not lead to the interruption of the work of the system or its serious hindering. Nevertheless, the illegal data interference may cause the interruption or hindering the system. In this case, it is essential to distinguish between illegal data and system interferences. Analyzing the intent, system interference takes place if the person had an intent to affect the system not only the data. However, acts aimed to data disruption which resulted in system destruction shall be considered intentional as an offender could predict such negative consequences (had an indirect intent).

There is no separate article prescribing an offence of illegal data interference (committed by person without right to the system) in the Ukrainian legislation. Any conduct

directed on the computer data destruction, alteration, modification committed by person without right is criminalized by previously observed article 361 of the Criminal Code of Ukraine. Examining the disposition of the part 1 of article 361, we come to conclusion that 'unauthorized interference with the operation of electronic computers (computers), automated systems, computer networks or telecommunication networks'[111] means illegal access as well as illegal system interference. However, to be punished as a crime an act must result in 'leakage, loss, falsification, blocking of information, distortion of the information processing or violation of the established order of its routing'[112].

As we have already discussed, the article covers both situations: system interference and data interference, and, in fact, corresponds to the European minimum standards (at least, in terms of system interference). However, the wording is disputable. Whether the data interference will result in interference with the functioning process of the system?

On the one hand, the Ukrainian approach may seem better as it allows to facilitate criminal prosecution: any act committed without right against the computer system resulted in harm caused to this system or the data contained in the system is possible to qualify as a crime under article 361. On the other hand, legislator should take into account the fact of extremely fast technological development and its relation to cybercrime. New means of hacking, ways to interfere with the computer system, viruses and other malicious software appear every day. The legislation must be ready to punish any kind of attack against information system simultaneously regarding the Article 7 of the European Convention on Human Rights 'No one shall be held guilty of any criminal offence on account of any act or omission which did not constitute a criminal offence under national or international law at the time when it was committed'[113]. Consequently, I stand for widening the scope of actions, which have to be punished as a criminal offence, making clear distinction between them and their consequences.

The first task is to define the correct meaning of the interference prescribed in article 361: whether it contains only interference to system functioning or also to data stored in the system; whether illegal access to the informational system also falls under the definition of the interference. As we discussed before, the European legislator distinguishes among these terms. If we follow the proposal from the Chapter 1 to establish an article introducing punishment for an illegal access, the meaning of unauthorized interference settled in article

[111] The Criminal Code of Ukraine. Law of Ukraine. 5 April 2001. No. 2341-III. [interactive]. [reviewed in 8 May 2020]. Available at: <https://zakon.rada.gov.ua/laws/show/2341-14/ed20010405>
[112] Ibid.
[113] 1950. European Convention on Human Rights. [interactive]. [reviewed in 10 April 2020]. Available at:< https://www.echr.coe.int/Documents/Convention_ENG.pdf>

361 will change. At the same time, situations of data disruption without interference to the system functioning (illegal interference) are possible.

The Ukrainian Court practice does not demonstrate a lot of examples of destruction or alteration the data, punished under article 361. However, I would like to observe the case, where the faired IT worker is accused of the removal and destruction of the software product from the servers of his former employer. Previously he worked as IT specialist in Ukrainian company creating the website for a Norwegian company and had authorized access to the system and any information related to the project. After the release, he lost his right to access and, therefore, had an intent to the unauthorized access in order to obtain all information for his private purposes and delete it from the company's servers. It is important to emphasize, that it is a position of the District Court, prescribed in the ruling from 8 May 2018[114]. As this case is still pending before the Court of Appeal, the accused person cannot be found guilty.

In my opinion, such conduct shall be punished in two ways depending the probable legislation: 1) illegal access to the information system which lead to deleting computer data; 2) the set of crimes – an illegal access and illegal data interference, but not as a system interference as the system was not hindered by the mentioned actions. However, it is possible in case of changing the term of 'system interference'.

Consequently, I would offer to amend article 361 of the Criminal Code of Ukraine and separate actions of data interference and system interference. Firstly, it will encourage the level of clearness of the criminal legislation. Secondly, it will allow to avoid situations when data interference will be committed without interference to the system functioning and, as a result, may be out of criminal liability.

Part II. Chapter IV. Illegal data interception

The fourth type of offences prescribed by the Directive 2013/40/EU, is named illegal interception. According to Article 6 of the Directive 'Member States shall take the necessary measures to ensure that intercepting, by technical means, non-public transmissions of computer data to, from or within an information system, including electromagnetic emissions from an information system carrying such computer data,

[114] Judgement of Primorsky District Court of Odessa. 8 May 2018. *No. 522/8715/13-k.* Available at: <http://reyestr.court.gov.ua/Review/73869949>

intentionally and without right, is punishable as a criminal offence, at least for cases which are not minor'[115].

Notwithstanding the fact that the offence of illegal interception was not enshrined in the Framework Decision 2005/222/JHA, the Member States had to be already acquainted with it because of the previous establishment of the illegal interception under the Convention on Cybercrime. However, some interviewing countries (Luxembourg, Bulgaria) complained on the unclearness of their relevant legislation and its correct application. The questions arised concerning the confidentiality of communication within the company, malware testing[116].

The element 'without right' shall be estimated in such cases[117]. For example, if the mails received to the corporate mailbox are resending automatically to the director's mail account or a common company account within the labor agreement, the interception cannot be considered illegal as it was committed with right.

The Directive does not determine the grounds for lawful interception. Therefore, Member States decide this issue in their national legislation (for example, the police may obtain a judge order for interception during crime investigation or 'the surveillance is lawfully authorised in the interests of national security'[118]).

Under the recital 9 of the Directive Preamble 'interception includes, but is not necessarily limited to, the listening to, monitoring or surveillance of the content of communications and the procuring of the content of data either directly, through access and use of the information systems, or indirectly through the use of electronic eavesdropping or tapping devices by technical means'[119].

The offence of illegal interception must be committed with help of technical means. For example, to intercept the telecommunication data transfer an offender usually utilizes different wiretapping means as tracking devices. To intercept the deferral of computer data the means of advanced technical level may be involved.

It is essential to analyze whether the term 'non-public' is referred to the data or exactly to the process of transmission disregarding the nature of the data. Taking into the

---

[115] Directive 2013/40/EU.

[116] The Directive on attacks against information systems. A Good Practice Collection for CERTs on the Directive on attacks against information systems ENISA P/28/12/TCD, Version: 1.5, 24 October, 2013. P. 11. [interactive]. [reviewed in 2 March 2020]. Available at: <https://www.enisa.europa.eu/publications/the-directive-on-attacks-against-information-systems/at_download/fullReport>

[117] Explanatory Report to the Convention on Cybercrime. *European Treaty Series.* No. 185. 23 November 2001. P. 11. [interactive]. [reviewed in 5 May 2020]. Available at: <https://rm.coe.int/16800cce5b>

[118] Ibid.

[119] Directive 2013/40/EU.

account the wording 'non-public transmissions' established in the article, no matter the fact whether the data is accessible for public or not, the referral of this data between persons through computer devises has to be characterized as confidential, and as a result, transmission as "non-public'.[120].

Although the subject of the offence is a computer data, an article stipulating the criminal offence in the national legislation may also contain illegal interception of telecommunication data.

For instance, the Article 139 C of the Criminal Code of the Netherlands prescribes the penalty for the following actions: 'Any person who intentionally and unlawfully intercepts or records by means of a technical device data which is not intended for him and is processed or transferred by means of telecommunication or by means of a computerized device or system'[121]. This type of combination of different actions in the joint disposition of the article leads to the finding about the resemblance of these criminal acts. Under the Dutch legislation the main feature of the offence is the interception of data transmission. The type of the data depends on the way of its deferral: via computer devices or telecommunication means (e.g. a phone).

In 2016 the European Court of Human Rights rendered the decision in case *Brambilla and others V. Italy* after examining the circumstances of the case on the subject of violation of the Article 10 on the freedom of expression. In the case journalists used some radio equipment to intercept the conversations between police workers. The Court has agreed on the confidential status of the conversation and the illegality of acts committed by journalists in order to receive such kind of information. Furthermore, the Court draw attention to the proportionate penalties applied to the offenders – seizure of the equipment used for illegal interception and suspended sentences for all offenders. As a general rule, data interception is illegal unless it is allowed on the grounds and in accordance with the law. No exclusions for the journalistic activity may exist. In conclusion, Court found no violation of Article 10 of the Convention as the restrictions, prescribed by the criminal legislation in order to protect the confidential information, do not forbid the journalist to do their job. Therefore, the right of freedom of speech was not breached[122].

---

[120] Explanatory Report to the Convention on Cybercrime. *European Treaty Series.* No. 185. 23 November 2001. P. 10. [interactive]. [reviewed in 5 May 2020]. Available at: <https://rm.coe.int/16800cce5b>

[121] The Criminal Code of the Kingdom of Netherlands. (1881, amended on 2012). English version. [interactive]. [reviewed in 2 March 2020]. Available at: <https://www.legislationline.org/download/id/6415/file/Netherlands_CC_am2012_en.pdf>

[122] The conviction of journalists who illegally intercepted radio communications between law-enforcement officers did not infringe their right to freedom of expression. *Press Release issued by the Registrar of the Court ECHR 223* (2016).23 June 2016. [interactive]. [reviewed in 17 April 2020]. Available at: <

Predictably, in case with computer data the Court decision would be the same. The described approach relates to the 'without right' test and defining the conditions for a lawful interception.

Examining the information introduced in the report from the Commission to the European Parliament and the Council assessing the extent to which the Member States have taken the necessary measures in order to comply with Directive 2013/40/EU, it can be concluded, that generally Member States have adopted a relevant legislation to criminalize an illegal data interception. However, there are some exclusions related to the limited definition of the computer data[123].

For instance, the Criminal Code of the Republic of Bulgaria provides the exhaustive list of data 'signals, written text, image, sound, data or messages of any type'[124] which means that interception of transmission of another kind of data (not mentioned in the list) is not punishable under the Article 348A. Considering the fast science growth and digitalization expansion, I am inclined to think that limitation of the data definition and means of its transfer interception, is irrelevant. The broader definition is established, the longer this law will correspond to the demands of the times.

The Criminal Code of the Republic of Estonia stipulates the punishment for the offence of unauthorized surveillance (Art. 137): 'observation of another person in order to collect information relating to such person by a person without the lawful right to engage in surveillance'[125]. On the one hand, the disposition of the article has no limitation to the type of data and any intentional unauthorized act of data interception falls under the Article. On the other hand, it contains a global limitation as the information has to be related to the observed person. Therefore, not every conduct of data interception is punishable in Estonia.

The essential omission of the great number of Member States is the absence necessary legislation covering the interception of electromagnetic emissions[126]. In terms of

https://hudoc.echr.coe.int/app/conversion/pdf?library=ECHR&id=003-5415795-6778471&filename=Judgment%20Brambilla%20and%20Others%20v.%20Italy%20-%20interception%20of%20law-enforcement%20officers%27%20radio%20communications%20by%20journalists.pdf>

[123] Ibid.

[124] The Criminal Code of the Republic of Bulgaria (1968, amended 2017). English version. [interactive]. [reviewed in 6 March 2020]. Available at: <https://www.legislationline.org/download/id/8395/file/Bulgaria_Criminal_Code_1968_am2017_ENG.pdf

[125] The Criminal Code of the Republic of Estonia (2001, amended 2019). English version. [interactive]. [reviewed in 30 April 2020]. Available at: <https://www.legislationline.org/download/id/8244/file/Estonia_CC_am2019_en.pdf>

[126] Report from the Commission to the European Parliament and the Council on assessing the extent to which the Member States have taken the necessary measures in order to comply with Directive 2013/40/EU on attacks against information systems and replacing Council Framework Decision

Cybercrime Convention 'such emissions are not considered as 'data'…however, data can be reconstructed from such emissions'[127].

The relevant legislation regarding electromagnetic emissions is introduced, fot example, in the Romanian Criminal Code. 'This takes the form of capturing the present radiations or electromagnetic fields (on a scientifically determined distance) around any device subject to the transit of electrical or electromagnetic pulses. For example, by using a special device, people with certain interests can capture electromagnetic radiations around the target computer monitor and "translate" them, that is turning them into electrical impulses and then in alphanumeric characters.'[128]

Evaluating the Ukrainian legislation related to the offence of data interception, we can conclude that all probable variants of its commission are covered. The Criminal Code of Ukraine stipulates punishment for three different criminal acts. The first is prescribed by the part 2 of the Article 163, which establishes punishment for 'the violation of the secrecy of correspondence, telephone conversations, telegraph or other correspondence transmitted by means of communication or via computer, committed due to the use of technical means designed for covert receipt of information'[129]. The offence is committed when an offender is acquainted with the information contained in such a correspondence of a person.[130] However, the definition of information which may be intercepted is limited to the conversations (messages, correspondence and phone calls). Therefore, only one article 163 does not cover all probable cases of data interception. For this reason, the article 182 stipulates a punishment 'for the unlawful collection, storage, use, destruction, dissemination of confidential information about a person or unlawful alteration of such information'[131]. Obviously, that articles 163 and 182 were adopted in order to protect a right to respect for private and family life, prescribed by the article 8 of the Convention on Human Rights, preventing its infringements.

2005/222/JHA. Brussels, 13 September 2017. P. 7-8. [interactive]. [reviewed in 8 May 2020]. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017DC0474&from=en>

[127] Explanatory Report to the Convention on Cybercrime. *European Treaty Series.* No. 185. 23 November 2001. P. 10. [interactive]. [reviewed in 5 May 2020]. Available at: <https://rm.coe.int/16800cce5b>

[128] VASILESCU S. Illegal interception of computer data transmission in the regulation of the New Romanian Criminal Code. *Journal of Law and Administrative Sciences*. 2015 (3). P. 235. [interactive]. [reviewed in 8 May 2020]. Available at: <https://pdfs.semanticscholar.org/20f3/b4ce7c67c19d4cf51982b74d72458e8d8016.pdf>

[129] The Criminal Code of Ukraine. Law of Ukraine. 5 April 2001. No. 2341-III. [interactive]. [reviewed in 8 May 2020]. Available at: <https://zakon.rada.gov.ua/laws/show/2341-14/ed20010405>

[130] Науково-практичний коментар Кримінального кодексу України за редакцією М. І. Мельника, М. І. Хавронюка. 7-е вид., переробл. та допов. Київ: Юридична думка, 2010. С. 434.

[131] The Criminal Code of Ukraine. Law of Ukraine. 5 April 2001. No. 2341-III. [interactive]. [reviewed in 8 May 2020]. Available at: <https://zakon.rada.gov.ua/laws/show/2341-14/ed20010405>

However, to define the conduct as an illegal data interception, special technical means must be involved. The article 359 of Criminal Code of Ukraine stipulates a punishment for the illegal use of special technical means for covert receipt of information as well as their illegal acquisition and sale. In case, an offender illegally utilizes special technical means for covert receipt of information in order to intercept transmission of private correspondence or phone calls, he is liable under the part 2 of the article 163 or is liable for the set of offences, prescribed under articles 163 (part 2) and 359 (part 2)[132] in particular cases; to intercept transmission of confidential data - he is liable for the set of offences prescribed under articles 182 and 359[133]. Such technical means are forbidden to possess for citizens and non-public legal entities[134]. Means for covert receipt of information as well as means for secret surveillance may be allowed to use by law enforcement officers in accordance with the Criminal Procedure Code of Ukraine.

In conclusion, the provisions of Ukrainian criminal legislation related to the offence of illegal data interception widely cover the probable illegal acts. Nevertheless, the legislation needs some improvement regarding the interception of electromagnetic emissions as special provisions regarding such emissions are not introduced.

Part II. Chapter V. Offences related to the misuse of tools

The fifth type of the offence prescribed by the Directive 2013/40/EU consists of offences related to manufacturing and distribution of tools suitable for committing offences prescribed by Articles 3-6 of the Directive. According to the Article 7 ‘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 programme, designed or adapted primarily for the purpose of committing any of the offences referred to in Articles 3 to 6;

[132] Науково-практичний коментар Кримінального кодексу України за редакцією М. І. Мельника, М. І. Хавронюка. 7-е вид., переробл. та допов. Київ: Юридична думка, 2010. С. 1034.
[133] Ibid.
[134] About the ownership of certain types of property. Regulation of the Parliament of Ukraine. 17 June 1992. No. 2471-XII. [interactive]. [reviewed in 8 May 2020]. Available at: <https://zakon.rada.gov.ua/laws/show/2471-12>

(b) a computer password, access code, or similar data by which the whole or any part of an information system is capable of being accessed'[135].

Although, the relevant conduct was punishable under article 6 of the Convention on Cybercrime, the Framework Decision did not introduce the offence of misuse of devices. However, none of the interviewed Member States 'indicated that provisions on tools for committing offenses were missing in their jurisdictions'[136], but some ambiguities were still present.

Marimosa botnet case demonstrated a necessity of improvement of cybercrime legislation, particularly in Spain, as problems arised during the trial of the botnet developers[137] who could avoid punishment because of the absence a relevant legislation. Captain Cesar Lorenzana from the Spanish Civil Guard described the situation as follows 'In Spain, it is not a crime to own and operate a botnet or distribute malware. So, even if we manage to prove they are using a botnet, we will need to prove they also were stealing identities and other things, and that is where our lines of investigation are focusing right now'[138].

Marimosa botnet, which, besides being suitable for DoS attacks, was created to steal the data, including banking information (passwords, credit card numbers) and spread viruses, finally infected, approximately around 8-12 millions of computer devices[139].

Nevertheless, there was no punishment prescribed under the Spanish law for the owners and distributors of any harmful tools as computer viruses and botnets. Therefore, in case of absence another conduct considering to be criminal under the law, the botnet developers would avoid liability despite the fact of damages.

The case of *Marimosa botnet* was investigated by FBI, Spanish Guard and Slovenian police jointly[140]. In 2013 Slovenian court sentenced the creator of the botnet Matjaz

---

[135] Directive 2013/40/EU.

[136] The Directive on attacks against information systems. A Good Practice Collection for CERTs on the Directive on attacks against information systems ENISA P/28/12/TCD, Version: 1.5, 24 October, 2013. P. 12. [interactive]. [reviewed in 2 March 2020]. Available at: <https://www.enisa.europa.eu/publications/the-directive-on-attacks-against-information-systems/at_download/fullReport>

[137] PLOHMANN D., GERHARDS-PADILLA E., LEDER F. Botnets: Detection, Measurement, Disinfection & Defence. ENISA. Edited by Dr. Giles Hogben. P. 91. [interactive]. [reviewed in 7 May 2020]. Available at: < https://www.enisa.europa.eu/publications/botnets-measurement-detection-disinfection-and-defence/at_download/fullReport>

[138] KREBS B. Mariposa' Botnet Authors May Avoid Jail Time. *Krebs on Security.* [interactive]. [Reviewed in 12 April 2020]. Available at: <https://krebsonsecurity.com/2010/03/mariposa-botnet-authors-may-avoid-jail-time/>

[139] Suspected 'Mariposa Botnet' creator arrested. *Spacewar*. 28 July 2010. [interactive]. [reviewed in 9 May 2020]. Available at: <https://www.spacewar.com/reports/Suspected_Mariposa_Botnet_creator_arrested_999.html>

[140] Ibid.

Skorjanc to 4-years imprisonment and 'order him to pay a fine along with the expropriation of an apartment and a car that Skorjanc had bought with the money he earned by selling the computer virus to a Spanish crime group'[141].

According to the information provided by the Marimor regional court 'Skorjanc was found guilty of "creating a malicious computer programme for hacking information systems, assisting in wrongdoings and money laundering'[142].

It is interesting to note, that after the Directive adoption the Spanish criminal legislation was improved a lot. According to the Article 400 of the Criminal Code of the Kingdom of Spain 'manufacturing or possessing tools, materials, instruments, substances, machinery, computer programs or appliances specifically used to commit the offences described in the preceding Chapters, shall be punished with the penalty stated in each case for principals'[143]. Tools are defined more precisely in the articles devoted to the separate offences.

One of the main aims of the article 7 of the Directive is to criminalize acts of production and distribution of harmful programs disregarding that cyberattack and malware production are committed by different perpetrators or not. A person who creates a malicious program, botnet or another one realizes that his or her devices cannot be used without harmful effect. Therefore, the actions are usually intentional (except of cases when such tools are used for legitimate purpose'[144]) and do not need the establishment of a 'special intent' requirement.

For example, the French court found[145] that the simple fact of publishing an 'article specially adapted' for the realization of a computer hacking, results in criminal conviction[146]. The Criminal Code of French Republic (Art. 323-3-1) prescribes a punishment for 'the fact, without legitimate reason, of importing, owning, offering,

---

[141] Slovenian hacker sentenced to jail for 'malicious' program. *Physorg.* [interactive]. [Reviewed in 12 April 2020]. Available at: <https://phys.org/news/2013-12-slovenian-hacker-sentenced-malicious.html>

[142] Ibid.

[143] The Criminal Code of the Kingdom of Spain (1995, as of 2013). English version. [interactive]. [Reviewed in 12 April 2020]. Available at: <https://www.legislationline.org/download/id/6443/file/Spain_CC_am2013_en.pdf>

[144] Directive 2013/40/EU. Recital 16.

[145] The Directive on attacks against information systems. A Good Practice Collection for CERTs on the Directive on attacks against information systems ENISA P/28/12/TCD, Version: 1.5, 24 October, 2013. P. 13. [interactive]. [reviewed in 2 March 2020]. Available at: <https://www.enisa.europa.eu/publications/the-directive-on-attacks-against-information-systems/at_download/fullReport>

[146] CHAMPEAU G. La cour de cassation confirme que la publication de failles de sécurité exploitables est un délit. [interactive]. [Reviewed in 12 April 2020]. Available at: <https://www.numerama.com/magazine/14745-la-cour-de-cassation-confirme-que-la-publication-de-failles-de-securite-exploitables-est-un-delit.html>

transferring or making available equipment, an instrument, a computer program or any data designed or specially adapted to commit [illegal access, illegal system or data interference]'[147]. In the observed case, the company published on its website some information which, as was confirmed later, 'was disseminating a code exploiting a flaw in the WINDOWS graphics engine which had given rise to an alert by CERTA'[148].

The Court of Cassation upheld the decision of the Montpellier Court of Appeal and emphasized that 'there was no reason to look in the case for a fraudulent intent as it is an objective offence. The only issue which had to be verified is whether the author was aware of the possibility that the information, he published, could be exploited with pirating purposes'[149].

Nevertheless, some countries established relevant legislation which requires a specific intent[150]. For instance, according to the Criminal Code of Finland an intent 'to impede or damage data processing or the functioning or security of an information system or telecommunications system'[151] is mandatory to punish an offender 'who imports, obtains for use, manufactures, sells or otherwise disseminates or makes available a harmful program'[152].

Another problem is when the national legislation of Member State prescribes the liability for production and distribution only for the perpetrator of the cyberattack[153]. For example, according to the Criminal Code of Czech Republic (section 231) 'Whoever with

---

[147] The Criminal Code of the French Republic (as of 2005). English version. [interactive]. [reviewed in 2 March 2020]. Available at: <https://www.legislationline.org/download/id/3316/file/France_Criminal%20Code%20updated%20on%2012-10-2005.pdf>

[148] Est-il illégal de publier des failles de sécurité ? 24 December 2009. *Criminalités numériques.* [interactive]. [Reviewed in 12 April 2020]. Available at: <https://blog.crimenumerique.fr/tag/atteintes-aux-stad/>

[149] CHAMPEAU G. La cour de cassation confirme que la publication de failles de sécurité exploitables est un délit. [interactive]. [Reviewed in 12 April 2020]. Available at: <https://www.numerama.com/magazine/14745-la-cour-de-cassation-confirme-que-la-publication-de-failles-de-securite-exploitables-est-un-delit.html>

[150] Report from the Commission to the European Parliament and the Council on assessing the extent to which the Member States have taken the necessary measures in order to comply with Directive 2013/40/EU on attacks against information systems and replacing Council Framework Decision 2005/222/JHA. Brussels, 13 September 2017. P. 8. [interactive]. [reviewed in 8 May 2020]. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017DC0474&from=en>

[151] The Criminal Code of the Republic of Finland (1889, as of 2015). English version. [interactive]. [reviewed in 8 May 2020]. Available at: https://www.legislationline.org/download/id/6375/file/Finland_CC_1889_am2015_en.pdf>

[152] Ibid.

[153] Report from the Commission to the European Parliament and the Council on assessing the extent to which the Member States have taken the necessary measures in order to comply with Directive 2013/40/EU on attacks against information systems and replacing Council Framework Decision 2005/222/JHA. Brussels, 13 September 2017. P. 8. [interactive]. [reviewed in 8 May 2020]. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017DC0474&from=en>

the intent to commit a criminal offence of Breach of secrecy of correspondence or a criminal offence of Unauthorized access to computer systems and information media produces … a device…'[154].

Although Member States mostly introduced corresponding national legislation, there are still some loopholes and discrepancies which should be reconciled. Except of mentioned above, some countries' legislation does not 'cover all the refereed offences or the national measures are found in the lack of transposition of all the possible acts listed'[155].

As the offence of production and distribution of malicious programs was prescribed by the Cybercrime Convention as a 'Misuse of devices', the relevant legislation was established in Ukraine.

The Criminal Code of Ukraine (Article 361^1) stipulates punishment for:

1. 'creation for the purpose of use, distribution or sale;
2. the distribution;
3. the sale, -

of malicious software or hardware intended for unauthorized interference with the operation of electronic computers (computers), automated systems, computer networks or telecommunication networks'[156].

In general, this article corresponds to the Directive requirements, although the list of actions may be widened. I consider the absence of a list of malicious programs to be an advantage, as it is impossible to predict the invention of new tools that may be designed to commit cyberattacks and, as a result, impossible to establish the exhaustive list. Observing the court practice, we can conclude that different existing types of malicious programs are covered by the article (viruses, botnets, programs designed to select passwords, etc.).

For example, in case *№ 182/4213/18* the offender was found guilty under the article 361^1 for distribution the computer extortion-virus Petya. Man bought the malicious

[154] The Criminal Code of the Czech Republic (2009, as of 2011). English version. [interactive]. [reviewed in 8 May 2020]. Available at: <https://www.legislationline.org/download/id/6370/file/Czech%20Republic_CC_2009_am2011_en.pdf>

[155] Report from the Commission to the European Parliament and the Council on assessing the extent to which the Member States have taken the necessary measures in order to comply with Directive 2013/40/EU on attacks against information systems and replacing Council Framework Decision 2005/222/JHA. Brussels, 13 September 2017. P. 8. [interactive]. [reviewed in 8 May 2020]. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017DC0474&from=en>

[156] The Criminal Code of Ukraine. Law of Ukraine. 5 April 2001. No. 2341-III. [interactive]. [reviewed in 8 May 2020]. Available at: <https://zakon.rada.gov.ua/laws/show/2341-14/ed20010405>

software and shared the link to it on his YouTube Chanel already after huge 'Petya' attack against Ukrainian companies was committed, realizing a level of harm it can cause[157].

In another case *No. 310/4556/19*, the offender was found guilty the article 361[1] for the distribution of malicious software named 'Private Keeper' which allows the user 'to create brute force utilities designed for cracking accounts by selecting a login and password'[158]. In case *No. 640/953/17* the offenders were found guilty for the distribution of malicious software, named 'Owerflow Bot', designed for committing DDoS attacks[159].

Consequently, the article on the misuse of tools corresponds to the Directive Requirement. However, among the listed actions, the Directive, as well as previously Convention on Cybercrime, established 'the procurement for use'. For this reason, article 361[1] of the Criminal Code of Ukraine may be improved due to the widening of the list of actions of the actus reus of the offence.

[157] The judgement of Nikopol City District Court of the Dnipro region. 30 August 2018. No. 182/4213/18. [interactive]. [reviewed in 9 May 2020]. Available at: <http://www.reyestr.court.gov.ua/Review/76270022>

[158] Judgement of Berdyansk City District Court of Zaporizhia. 24 September 2019. No. 310/4556/19. [interactive]. [reviewed in 9 May 2020]. Available at: <http://www.reyestr.court.gov.ua/Review/84471272>

[159] Judgement of Kyiv District Court of Kharkiv. 23 March 2017. No. 640/953/17. [interactive]. [reviewed in 9 May 2020]. Available at: <http://reyestr.court.gov.ua/Review/65496457>

PART III. CRIMINAL LIABILITY FOR COMMISSION OF THE OFFENCES PRESCRIBED BY THE DIRECTIVE 2013/40/EU

Part III. Chapter I. Penalties standards

According to the Recital 10 of the Directive Preamble 'Member States should provide for penalties in respect of attacks against information systems. Those penalties should be effective, proportionate and dissuasive and should include imprisonment and/or fines'[160]. These features of penalties are common for any kind of criminal infringements within the EU and must be followed by the Member States due to the determination of relevant penalties in their national legislation[161].

The triad of 'effectiveness, proportionality and dissuasiveness' also known as 'minimum triad' was established by the ECJ (European Court of Justice) decision in Greek Maze case[162]. According to the paragraph 24 of the Court decision 'For that purpose, whilst the choice of penalties remains within their discretion (meaning discretion of Member States) they must ensure in particular that infringements of Community law are penalized under conditions, both procedural and substantive, which are analogous to those applicable to infringements of national law of a similar nature and importance and which, in any event, make the penalty effective, proportionate and dissuasive'[163].

To understand the importance of the 'triad requirements' it is necessary to analyze each of them separately but taking into consideration that all of them must be fulfilled simultaneously.

The proportionality principle is one of crucial parts of the 'rule of law' concept promoting the fair balance between the restriction of rights of a person (e. g. measures applied to the offender) and the consequences of his misconduct, the public danger level of the offence. In the Case C-94/05 *Emsland-Starke*, Case C-426/93 *Germany v Council* the Court has formed an approach: to comply with principle of proportionality there is must be an absolute certainty that 'the means which provision of EU law employs are suitable for

---

[160] Directive 2013/40/EU.

[161] TEFFER P. 'EU admits to problems in penalty regime'. 12 April 2018. [interactive]. [reviewed in 29 March 2020]. Available at: <https://euobserver.com/economic/141583>

[162] SATZGER H. *The Harmonisation of Criminal Sanctions in the European Union* - A New Approach. eucrim - The European Criminal Law Associations' Forum. 2019 (2). P. 116. [interactive]. [reviewed in 29 March 2020]. Available at: <https://eucrim.eu/media/issue/pdf/eucrim_issue_2019-02.pdf#page=41>

[163] EU Court of Justice. *21 September 1989. Commission V. Greece. Case No. 68/88.* (Greek Maize case). [interactive]. [reviewed in 30 March 2020]. Available at: <https://eur-lex.europa.eu/resource.html?uri=cellar:4f255660-f631-479c-91b7-7abaf62826d1.0002.06/DOC_1&format=PDF>

the purpose of achieving the desired objective and whether they do not go beyond what is necessary to achieve it'[164]. Therefore, while imposing penalties or applying interim measures the Court is obliged to assess the congruence between them and the level of public danger of the offence, the caused damage, mitigating evidence and aggravating circumstances.

The principle of dissuasiveness is directed to preventing the committing of new crimes. In other words, the imposed penalties shall have a deterrent effect. This requirement is difficult to measure but there are some significant points which must be considered. For instance, certain aggravating circumstances or the fact of repeatability may cause harsher penalties[165]. Although, at the first sight, it is the requirement of the proportionality principle, but we remember that all the criteria are strongly integrated. Therefore, complying the proportionality principle the Court estimates the impact of the aggravating circumstances and imposes stricter penalties, it also follows the principle of dissuasiveness as stricter penalties are necessary to restrain such offender from committing the crime repeatedly.

As a result, the Court decision will comply with the principle of effectiveness. An author distinguishes the following features of the effectiveness principle: 'the achieving of the objective set by law, ensuring the procedure is not over long and costly; existence of coercive measures; ensuring cooperation between different actors of the sanctioning procedure and their specialization'[166].

It is crucial to note that all criteria are related to both procedural and substantive conditions of penalties. Therefore, not only the term of sentence or an amount of fine must be in conformity with the criteria according to the committed offences but also the processual issues must fall under the requirements.

In case *Čalovskis v. Latvia*, the applicant 'alleged *inter alia* that his placement in a caged dock during a court hearing with the publication of his photographs in the media were in violation of Article 3'[167]. Applicant was accused of a chain of offences (fraud and

[164] Effectiveness, Proportionality and Dissuasiveness. *Eastern and Central European Journal on Environmental Law,* vol. 15, no. 2, 2012, p. 11-13. HeinOnline. [interactive]. [reviewed in 4 April 2020]. Available at: <https://heinonline.org/HOL/PrintRequest?public=true&handle=hein.journals/eceujevl15&div=13&start_page=11&collection=journals&set_as_cursor=0&men_tab=srchresults&print=section&format=PDFsearchable&submit=Print%2FDownload>

[165] Ibid. p. 12

[166] Ibid. p. 12-13

[167] The European Court of Human Rights. 24 July 2014. (Final 15 December 2014). Judgement *Čalovskis v. Latvia*. Case No. 22205/13, § 3.

computer crimes) in the USA[168] and was arrested in Latvia with a purpose of extradition[169]. During the detention hearing he was locked in a metal cage and the mass media spread his photos 'in the courtroom behind the metal bars and wearing a hood'[170].

In this case the proportionality principle was demonstrated. The Court assessed the circumstances: 'that no evidence before it attests to the applicant's having a criminal record. Likewise, he was not suspected of having committed a violent crime. The applicant was not placed in the metal cage because he posed a risk to order or security in the courtroom, because it was thought that he might resort to violence or abscond, or because there was a risk to his own safety'[171].

The Court concluded that 'the security arrangements in the courtroom were, in the circumstances, excessive and could have been reasonably perceived by the applicant and the public as humiliating'[172] and therefore, the article 3 of the Convention was violated.

The case supports the statement that criteria of effectiveness, proportionality and dissuasiveness must be also considered to the application of procedural measures.

Minimum maximum penalties

EU Directives settle minimum penalties standards mandatory to adoption by Member States. These standards may be established in two different ways. The most detailed one is called 'minimum maximum penalties' 'which obligates the Member States not to fall below a certain *maximum* penalty. A less precise stipulation is the so-called 'minimum maximum penalty range' which does not prescribe a specific value in relation to the lowest maximum penalty allowed, but instead grants Member States a scope within which the maximum penalty to be imposed may range'[173].

For instance, according to the part 2 of the Article 9 of the Directive 2013/40/EU 'Member States shall take the necessary measures to ensure that the offences referred to in Articles 3 to 7 are punishable by a maximum term of imprisonment of at least two years, at least for cases which are not minor'[174]. As the comparison, under the Framework Decision

[168] Ibid., § 7.
[169] Ibid., § 11-12.
[170] Ibid., §26
[171] Ibid., § 103.
[172] Ibid., § 107.
[173] SATZGER H. *The Harmonisation of Criminal Sanctions in the European Union* - A New Approach. eucrim - The European Criminal Law Associations' Forum. 2019 (2). P. 116. [interactive]. [reviewed in 29 March 2020]. Available at: <https://eucrim.eu/media/issue/pdf/eucrim_issue_2019-02.pdf#page=41>

[174] Directive 2013/40/EU.

2005/222/JHA offences were 'punishable by criminal penalties of a maximum of at least between one and three years of imprisonment'[175]. Consequently, the Directive 2013/40/EU adopted the 'minimum maximum penalty' standard in contrast to the Framework decision which allowed Member States to choose between 1 to 3 years of maximum sentence. In fact, in both cases Member States are not forbidden to exceed the minimum and establish harsher maximum penalties. Therefore, the 'minimum maximum penalty range' was almost the same as the 'minimum maximum penalty' standard but less strict as the starting point for minimum maximum penalty was 1 year for sentence[176]. Obviously, that Directive approach is stricter approach as it puts an obligation on Member States to determine the maximum penalty for any offence against the information system established by the Directive not less than 2 years.

The question may arise in connection with the different public danger level of the offences against informational systems: 'Is it fair enough to establish the equal minimum maximum penalty for the offences despite the different harmful effect which could be caused?' It is essential to keep in mind that Directive established the minimum standards and Member States are not forbidden to range the offences on the public danger criteria and impose harsher maximum penalties according to their national legislation. For example, under the Criminal code of France the illegal access to the informational system is punished by two year's imprisonment and a fine of €60,000 whereas the illegal system interference is punished by five years' imprisonment and a fine of €150,000[177]. Both penalties correspond to the minimum maximum standards of the Directive.

The Directive also established the aggravating circumstances which are the ground to enhance the liability level. For example, 'the offences of illegal system and data interference (articles 4 and 5) have to be punished for a maximum term of at least three years if the significant number of informational systems was affected due to the use of a tool (defined by article 7), previously designed or adopted for that purpose'[178]. As was already mentioned in the previous parts, this article is mainly addressed to botnets which may be used, for example, to commit DDoS attack,

[175] Framework Decision 2005/222/JHA. Art. 6, p. 2.
[176] SATZGER H. *The Harmonisation of Criminal Sanctions in the European Union* - A New Approach. eucrim - The European Criminal Law Associations' Forum. 2019 (2). P. 116. [interactive]. [reviewed in 29 March 2020]. Available at: <https://eucrim.eu/media/issue/pdf/eucrim_issue_2019-02.pdf#page=41>
[177] Criminal Code of the French Republic (as of January 2020). French version. Articles 323-1, 323-2. [interactive]. [reviewed in 5 April 2020]. Available at: <https://www.legislationline.org/documents/section/criminal-codes/country/30/France/show>
[178] Directive 2013/40/EU. Art. 9, p. 3.

More serious aggravating circumstances which increase the level of minimum maximum penalty to the 5 years' imprisonment are the following:

(a) commission of a crime within the framework of a criminal organization, as defined in Framework Decision 2008/841/JHA, irrespective of the penalty provided for therein;

(b) commission of a crime caused a serious damage;

(c) the illegal act was committed against a critical infrastructure information system[179].

The seriousness of damages may be defined by judges considering the circumstances of the exact case. In my opinion, a critical infrastructure information system may be regarded as such if it is vitally essential for the state functioning, for example affects any function or the Government activity[180].

According to the Cybersecurity strategy of Ukraine the defense of critical infrastructure information systems is a priority[181]. However, although the Procedure for the formation of the list of information and telecommunication systems of critical infrastructure of the state[182] is already adopted, the list is not still established. In my opinion, relevant provisions on the imposition of harsher penalties in case of committing attacks against critical infrastructure information systems have to be adopted.

The novelty of the Directive 2013/40/EU is the establishment of 'identity theft' as an aggravating circumstance of committing offences of illegal system or data interference unless it is defined as a separate crime under the national legislation of the Member State[183]. The identity theft means the misuse of personal data of another person with the aim of gaining the trust of a third party, thereby causing prejudice to the rightful identity owner[184].

---

[179] Ibid. Art.9, p.4.

[180] Criminal Code of the Republic of Malta (1854, amended December 2019). English version. Art. 337F (2a). [interactive]. [reviewed in 30 April 2020]. Available at: <https://www.legislationline.org/download/id/8555/file/Malta_Criminal_Code_amDec2019_en.pdf>

[181] On the decision of the National Security and Defense Council of Ukraine of January 27, 2016 'On the Cybersecurity Strategy of Ukraine'. Decree of the President of Ukraine. No. 96/2016. 15 March 2016. [interactive]. [reviewed in 11 May 2020]. Available at: <https://zakon.rada.gov.ua/laws/show/96/2016>

[182] Procedure for the formation of the list of information and telecommunication systems of critical infrastructure of the state. Regulation of the Cabinet of Ministers of Ukraine. No. 563. 23 August 2016. [interactive]. [reviewed in 11 May 2020]. Available at: < https://zakon.rada.gov.ua/laws/show/563-2016-%D0%BF>

[183] The Directive on attacks against information systems. A Good Practice Collection for CERTs on the Directive on attacks against information systems ENISA P/28/12/TCD, Version: 1.5, 24 October, 2013. P. 21. [interactive]. [reviewed in 2 March 2020]. Available at: <https://www.enisa.europa.eu/publications/the-directive-on-attacks-against-information-systems/at_download/fullReport>

[184] Directive 2013/40/EU. Art. 9, p. 5.

Therefore, the Directive gives to Member States the possibility to choose between different forms of criminalization of 'identity theft' instrument utilization but it does not allow to leave this technique behind the attention and, moreover, relevant liability.

For example, in the Criminal Code of Malta (article 337 F) the identity theft is defined as an aggravating circumstance in one row with a serious damage, commission within the criminal organization and affection of the critical infrastructure. Any of the mentioned circumstances if it follows the commission of the cyber offence) increases the level of penalties which shall be imposed.[185]

The Criminal code of the Republic of Estonia (article 157-2) defines an identity theft as an independent offence named 'Illegal use of another person's identity': 'Transmission of personal data that establish or may enable to establish the identity of another person, grant of access to the data or use thereof, without the consent of that person, with the aim to knowingly cause a misconception of that person by means of assuming that person's identity, if damage is caused thereby to the rights or interests of another person that are protected by law, or to conceal a criminal offence, is punishable by a pecuniary punishment or up to three years' imprisonment'[186].'

Notwithstanding the fact that identity theft is often used by offenders, in particular, to commit fraud, the Ukrainian legislation defines the identity theft neither a separate crime nor the aggravating circumstance nor the qualification feature of the crime. Consequently, criminal legislation of Ukraine needs some improvements on this matter.

Part III. Chapter II. Sanctions against legal persons for attacks against information systems

The corporate liability for crimes became not an exceptional but general rule within the EU.[187] The nature of legal person's liability may differ from state to state ('true' criminal,

[185] Criminal Code of the Republic of Malta (1854, amended December 2019). English version. [interactive]. [reviewed in 30 April 2020]. Available at: <https://www.legislationline.org/download/id/8555/file/Malta_Criminal_Code_amDec2019_en.pdf>

[186] Criminal Code of the Republic of Estonia (2001, amended 2019). English version. [interactive]. [reviewed in 30 April 2020]. Available at: <https://www.legislationline.org/download/id/8244/file/Estonia_CC_am2019_en.pdf>

[187] MONGILLO V. Corporate criminal liability and compliance programs. Volume II towards a common model in the European Union. Edited by Antonio Fiorella. JOVENE EDITORE 2012. Chapter III. P. 122. [interactive]. [reviewed in 5 May 2020]. Available at: <https://www.academia.edu/6224953/The_Allocation_of_Responsibility_for_Criminal_Offences_Between_Individuals_and_Legal_Entities_in_Europe>

para-criminal or administrative liability)[188] and there is no obligation for Member States to choose the only one form of corporate liability.

The criminal liability of legal persons for attacks against information systems was previously introduced in the Framework Decision and further fully adopted by the Directive. The Directive defines a legal person as 'an entity having the status of legal person under the applicable law but does not include States or public bodies acting in the exercise of State authority, or public international organisations'[189].

According to the part 1 of the Article 10 of the Directive 2013/40/EU Member States shall take the necessary measures to ensure that legal persons can be held liable for offences referred to in Articles 3 to 8, in case the act was committed for their benefit by any person, acting either individually or as part of a body of the legal person, and having a leading position within the legal person[190]. The leading position may be determined grounding on at least one of the following criteria: a power of representation of the legal person and/or an authority to take decisions on behalf of the legal person and/or an authority to exercise control within the legal person[191]. Usually, the one person in the company may be empowered by all competences mentioned above. But even the only one power in hands is enough to consider this person to have a leading position.

Furthermore, the Directive also requires to found the legal person liable in case of the lack of supervision or control by a 'leading position person' that allowed the commission, by a person under its authority, of any of the mentioned offences for the benefit of that legal person[192].

In both cases the element of 'the benefit of legal entity' is required. Therefore, the legal person cannot be liable for the independent actions of its employee who utilizes the company infrastructure to commit an attack against information system or abet its commission following his or her private purposes not the 'company benefit'.

Generally, the liability of legal persons for computer crimes may arise in different cases. For example, cases related to unfair business practice when the legal entity hires specialists to 'hack' the system and steal or damage the information of its rivals, to commit a system interference through malware sharing or by any other means in order to interrupt

[188] MONGILLO V. Corporate criminal liability and compliance programs. Volume II towards a common model in the European Union. Edited by Antonio Fiorella. JOVENE EDITORE 2012. Chapter II. p. 75. [interactive]. [reviewed in 5 May 2020]. Available at: <https://www.academia.edu/6224944/The_Nature_of_Corporate_Liability_for_Criminal_Offences_Theoretical_Models_and_EU_Member_State_Laws>

[189] Directive 2013/40/EU. Art. 2.

[190] Ibid. Art. 10, p. 1.

[191] Ibid.

[192] Ibid. Art. 10, p. 2

the other company business processes. Another variant exists when companies which conduct the producing and distribution of malware (and other tools to commit the attacks) or even organize the attacks, hiding their 'main activity', will be liable for such crimes. Another example of engaging the legal persons in commission of cybercrime attacks is usage of the entity infrastructure to commit any offence, prescribed by articles 3-8 of the Directive, providing some benefit instead (money, services, etc.). In this case, the company shall be liable for abetting the offence.

Regarding the 'benefit' element it is important to emphasize, that the offence prescribed by the part 2 of the Article 10 does not cover cases of failure of the legal person to provide an appropriate level of cybersecurity system. The Directive draw our attention to the issue of necessity to '*increase the resilience of information systems by taking appropriate measures to protect them more effectively against cyber attacks'*[193] but does not prescribe a criminal liability for not-providing these measures. It's emphasizes on the necessity to protect at least 'critical infrastructure from cyber attacks on the appropriate level to resist reasonably identifiable threats and vulnerabilities. Member States are encouraged to provide for relevant measures incurring liabilities in the context of their national law in cases where a legal person has clearly not provided an appropriate level of protection against cyber attacks'[194].

Usually, in case of not providing a necessary level of protection against cyber attacks the company may be held civil liability, for example, according to the GDPR rules[195].

According to the part 3 of the article 10 of the Directive 'the liability of legal persons shall not exclude criminal proceedings against natural persons who are perpetrators or inciters of, or accessories to, any of the offences referred to in Articles 3 to 8'[196].

The interesting changes occurred with the Belgium criminal law. Previously, the Belgian national legislation introduced the 'alternative liability model for legal entities and natural persons with the following rule: where both a natural and a legal person are involved only the person who committed the more serious fault may be convicted'[197]. Although this

[193] Ibid., Recital 26
[194] Ibid.
[195] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). [interactive]. [reviewed in 4 April 2020]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN
[196] Directive 2013/40/EU.
[197] MONGILLO V. Corporate criminal liability and compliance programs. Volume II towards a common model in the European Union. Edited by Antonio Fiorella. JOVENE EDITORE, 2012. P. 139-140. [interactive]. [reviewed in 5 May 2020]. Available at:

rule worked only in case 'where the liability of the legal person is engaged solely as a result of the intervention of an identified natural person unless the individual has identified the mistake knowingly and intentionally'[198], Nevertheless, the paragraph 2 of article 5 of the Belgian criminal code was changed in 2018 adopting the cumulative liability model which does not exclude the individual's liability in case of legal entity liability[199].

Article 11 of the Directive settled a requirement for Member States to ensure that a legal person held liable pursuant to Article 10(1) is punishable by effective, proportionate and dissuasive sanctions, which shall include criminal or non-criminal fines and which may include other sanctions, such as:

(a) exclusion from entitlement to public benefits or aid;

(b) temporary or permanent disqualification from the practice of commercial activities;

(c) placing under judicial supervision;

(d) judicial winding-up;

(e) temporary or permanent closure of establishments which have been used for committing the offence.

Labor Klimek offers to include provisions 'concerning confiscation in order to reduce the degree of variation between the national systems and to ensure that the requirements of 'effective, proportionate and dissuasive sanctions' sanctions are indeed met in all Member States'[200].

Kristina Brezinova suggests including in the list of sanctions 'the publication of a convicting sentence in public media such as newspapers, etc'[201]. She argues that this kind of sanctions may be effective in case a company is well-known. Therefore, the spreading

<https://www.academia.edu/6224953/The_Allocation_of_Responsibility_for_Criminal_Offences_Between_Individuals_and_Legal_Entities_in_Europe>

[198] The Criminal Code of the Kingdom of Belgium. (Previous version). [interactive]. [reviewed in 1 May 2020]. Available at: <https://issuu.com/ethics360/docs/penal_code__belgium_>

[199] The Criminal Code of the Kingdom of Belgium. (1867, as of 2018). [interactive]. [Reviewed in 1 May 2020]. Available at: <https://www.legislationline.org/download/id/8240/file/Belgium_CC_1867_am2018_fr.pdf>

[200] KLIMEK L. Criminal Liability of Legal Persons in Case of Computer Crime: A European Union Response. International and Comparative Law Review, 2015, vol. 15, no. 2, p. 141. [interactive]. [reviewed in 2 April]. Available at: <https://www.researchgate.net/publication/322710330_Criminal_Liability_of_Legal_Persons_in_Case_of_Computer_Crime_A_European_Union_Response>

[201] BŘEZINOVÁ K. *Company Criminal Liability for Unlawful Attacks against Information Systems within the Scope of EU Law.* Charles University in Prague Faculty of Law Research Paper No. 2017/II/3., 5 June 2017. P. 13-14. [interactive]. [reviewed in 2 March 2020]. Available at: <https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID2989005_code2308341.pdf?abstractid=2989005&mirid=1&type=2>

of information about crime committed by the enterprise may affect its reputation and lead to 'the worse punishment than for example a financial penalty'[202]. I do not agree with a proposal as the consequences of the application of this kind of sanctions are unpredictable. Therefore, it becomes impossible to assess whether the penalties correspond to criteria of effectiveness, proportionality and dissuasiveness. At the same time, I agree with the position of Libor Klimek to include 'confiscation' sanctions, which are already introduced by many national legislators.

For Ukraine the institute of corporate liability for crimes is new as was enacted only in 2014. Ukrainian legislator adopted a para-criminal form of corporate liability and established it only for a comprehensive list of crimes related to money laundering, corruption, terrorism and war crimes[203]. Legal entities cannot be liable for committing crimes against information systems according to the current Ukrainian legislation.

In my opinion, the current situation requires changes for several reasons. Firstly, notwithstanding the fact that approximation of law on cybercrime matters is not prescribed by the Association Agreement between the EU and Ukraine, we need to implement the EU standards to our legislation step by step as we are already on the way to the EU. Secondly, Ukraine suffers from cyber-war which held not only by individuals but rather legal persons from abroad which have to be prosecuted in Ukraine. Thirdly, founding the legal person liable for cyber attack gives an ability to enterprises and individuals who suffered from the crime to sue such entity and recover damages. Predictably, there are more chances to acquire a compensation from the legal entity rather than an individual who may be out of money or another property.

[202] Ibid.

[203] The Criminal Code of Ukraine. Law of Ukraine. 5 April 2001. No. 2341-III. Art. 96^3. [interactive]. [reviewed in 8 May 2020]. Available at: <https://zakon.rada.gov.ua/laws/show/2341-14/ed20010405>

PART IV. CYBERCRIME INVESTIGATION AND JURISDICTION CONFLICTS

Part IV. Chapter I. Determination of jurisdiction: general principles and problem issues

Cyberspace differs a lot from the common place and circumstances inherent in criminal conduct. Offenders who commit attacks against information systems are not limited to borders and can cause harm to victims all over the world. In contrast, states have to operate within limited territorial jurisdiction while prosecuting the cases[204]. For this reason, two crucial issues are apparent: the rules of enforcement jurisdiction must cover all possible situations of cybercrime commission to not leave any out of liability, and the legislation must be directed to enhanced cooperation between the states in order to investigate effectively.

The question of jurisdiction does not arise in case the crime was committed within the territory of the country by its national against the system on the territory of this country. Nevertheless, cyber-attacks tend to become transnational offences involving at least one foreign element in their 'inception, perpetration and/or direct or indirect effects. They are, in other words, what Kofi Annan called, *problems without a passport*'[205].

The Directive introduced the approach, previously established by the Convention on Cybercrimes and farther adopted by the Framework Decision, when the jurisdiction may be enforced according to either the principle of nationality or the principle of territoriality.

Indeed, the part 1 of the Article 12 of the Directive allows the Member States to establish their jurisdiction where the offence has been committed in whole or in part within their territory; or by one of their nationals, at least in cases where the act is an offence where it was committed.

The Cybercrime Convention also allows to prosecute the national if the offence is committed outside the territorial jurisdiction of any State. Although the Directive did not incorporate such a condition, it defines only a minimum rule when the jurisdiction may be enforced over the national containing the wording 'at least'. Therefore, the Directive does

---

[204] DR. ADEL AZZAM SAQF AL HAIT. Jurisdiction in Cybercrimes: A Comparative Study. *Journal of Law, Policy and Globalization*, Vol.22, 2014. P. 75. [interactive]. [reviewed in 2 March 2020]. Available at: < https://www.iiste.org/Journals/index.php/JLPG/article/viewFile/11050/11351>

[205] PERLOFF-GILES A. *Transnational Cyber Offenses: Overcoming Jurisdictional Challenges*. P. 196. [interactive]. [reviewed in 5 March 2020]. Available at: <https://cpb-us-w2.wpmucdn.com/campuspress.yale.edu/dist/8/1581/files/2018/02/191_Transnational-Cyber-Offenses-2i9mpg2.pdf>

not forbid to establish Member State jurisdiction by its national who committed a crime outside the territorial jurisdiction of any State but does not establish such requirement.

The specific nature of cybercrime leads to difficulties defining the territory of committing a crime as an offender usually utilizes the remote Internet connection and it is not always possible to find the place where the illegal actions were executed.[206]

At first sight, the problem seems to be soluble as information of the Internet user location may be revealed through the IP (Internet Protocol) address. However, experienced hackers and other cyber offenders used to find various tools and services providing the anonymity of their Internet access. As a result, identification of the territory where the crime took place may not be possible.[207]

Another example of the challenge to determine the territory of offence is DDoS attack conducted involving botnets which have no geographic limits meaning that malware produced by them can be spread across any borders[208]. All these botnets are targeted to the one or more 'victims' supposed to be attacked. All of them contain a single part of harmful information which has its own route of reaching the target system (usually the fastest) but this route does not seem to be direct geographically. Finally, investigation authorities will not be able to determine neither the routes of the spreading information nor the territory where the attack was conducted from[209].

Consequently, as looking for the territory of the offender faces large obstacles it seems to be easier to define the territory where the crime against cyber-security was committed by its harmful effects[210]. Nevertheless, the EU Directive on attacks against informational systems upheld the approach of jurisdiction exercising previously established

[206] IGLEZAKIS I. *The legal regulation of Cyber Attacks.* 2016. Kluwer Law International B. V.: the Netherlands. P.98.
[207] DASKAL J. The Un-Territoriality of data. *The Yale Law Journal.* P. 331. [interactive]. [reviewed in 3 March 2020]. Available at: <https://www.yalelawjournal.org/pdf/a.326.Daskal.398_qrhgeoar.pdf>

[208]OPHARDT, J. A. Cyber Warfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow's Battlefield. Duke Law & Technology Review, 2010. P. 12.[interactive]. [reviewed in 4 March 2020]. Available at: <https://heinonline.org/HOL/PrintRequest?collection=journals&handle=hein.journals/dltr2010&div=7&id=49&print=section&format=PDFsearchable&submit=Print%2FDownload>

[209] Ibid.
[210] IGLEZAKIS I. *The legal regulation of Cyber Attacks.* 2016. Kluwer Law International B. V.: the Netherlands. P.98.

by the Council of Europe Convention on Cybercrime and adopted by the Framework Decision[211].

According to the part 2 of the Article 12 of the Directive, the crime is deemed to be committed within the territory of the Member State (which is allowed to exercise its jurisdiction) in both cases: if the offender was physically present on its territory when commited a crime; or the offence is against an information system on its territory'[212].

None condition depends on the other. Member State can exercise its jurisdiction due to the physical presence of the offender whether or not the offence is against an information system on its territory. The same way Member State can establish its jurisdiction on the basis of the harmful effect on its territory regardless of the offender's whereabouts at the time of attack commission.

The novel of Directive is the ability of Member States to exercise jurisdiction in case the offender has his habitual residence in its territory or the offence is committed for the benefit of a legal person established in its territory. The latter was already introduced in the Framework Decision but regarding the Head Office establishment[213]. In any of these cases, the Member State shall inform the Commission where it decides to establish jurisdiction over an offence[214].

Probably, the 'legal person' rule of the jurisdiction establishment was introduced in the Directive with a purpose of encouragement the prosecution of legal persons acquiring benefit from the attacks against information systems. As despite the existing legislation stipulating the relevant criminal or administrative sanctions to legal persons for commission offences prescribed in Articles 3-8 of the Directive, the court practice of Member States is still poor.

Examining the 'habitual residence' rule, it may be difficult to define whether it relates more to the nationality principle, as the person may be bound with the state of habitual residence more than with the state of nationality, or the territoriality principle, as a place of habitual residence of an offender is likely to be a location of crime commission (for instance, in case of loss of location). In my opinion, the jurisdiction established on the 'habitual residence' is a form of extraterritorial jurisdiction as the offender may be prosecuted by the state of his habitual residence disregarding the location of crime.

[211] Ibid.
[212] Directive 2013/40/EU.
[213] Framework Decision. Art. 10, p. 1.
[214] Directive 2013/40/EU. Art. 10, p. 3.

Therefore, this rule is based on the nationality principle despite the link between the territoriality principle and the habitual residence.

As the Directive provides several cases for jurisdiction enforcement, high probability of jurisdiction conflicts exists. For example, the offender who is Romanian situated in Hungary attacks the information system located in Germany. As all three rules of jurisdiction determination may be applied, the existence of an effective instrument for conflict settlement is essential.

Previously, the Framework Decision contained a rule prescribed by the part 4 of the Article 10 : 'Where an offence falls within the jurisdiction of more than one Member State and when any of the States concerned can validly prosecute on the basis of the same facts, the Member States concerned shall cooperate in order to decide which of them will prosecute the offenders with the aim, if possible, of centralising proceedings in a single Member State'[215].

Ioannis Iglezackis draw our attention to the exclusion of the mentioned provision in the Directive 2013/40/EU[216]. Nevertheless, in the Recital 27 the Directive introduced the following rule: 'the coordination of prosecution of cases of attacks against information systems should be facilitated by the adequate implementation and application of Council Framework Decision 2009/948/JHA of 30 November 2009 on prevention and settlement of conflict of jurisdiction in criminal proceedings'[217].

Framework Decision 2009/948/JHA is a legal instrument dedicated to helping the Member States to reach the consensus in the jurisdiction establishment. Within the cooperation between the Member States, the exchange of information plays a crucial role as due to it the Member States are able to know about parallel proceedings involving the same person and agreed on the jurisdiction[218]. This instrument is essential as it provides execution of the principle 'ne bis in idem'.

[215] Framework Decision.
[216] IGLEZAKIS I. *The legal regulation of Cyber Attacks.* 2016. Kluwer Law International B. V.: the Netherlands. p. 95.
[217] The Directive 2013/40/EU. Recital 27.
[218] Council Framework Decision 2009/948/JHA of 30 November 2009 on prevention and settlement of conflicts of exercise of jurisdiction in criminal proceedings. Official Journal of the European Union. No.L 328/42. 15 December 2009. [interactive]. [reviewed in 11 May 2020]. Available at: < https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:328:0042:0047:EN:PDF>

Part IV. Chapter II. International cooperation on cybercrime investigation under the Directive 2013/40/EU

According to the ENISA Report, equally important are the procedural issues of the Directive concerning cooperation between law-enforcement organs within the EU, in particular, improvements of functioning the existing 24/7 contact points system and novelty of obligation of statistical data collection[219].

The 24/7 network system on cybercrime cooperation was introduced in the Cybercrime Convention[220]. According to the article 35 of the Convention 'each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures:

a) the provision of technical advice; b) the preservation of data pursuant to Articles 29 and 30 (stored computer data and traffic data); c) the collection of evidence, the provision of legal information, and locating of suspects'[221].

The Directive adopted an article 13 on information exchange (introduced before in the Framework Decision), adding some essential improvements. Previously, the Framework Decision contained a requirement of making the use of the existing network of operational points of contact available 24 hours a day and seven days a week. The Directive added the obligation to give a response within 8 hours to urgent requests. However, it also clarifies that within 8-hours period of time the Member State is obliged at least to provide the requesting party with the relevant information 'whether the request will be answered, and the form and estimated time of such an answer'[222]. It means, that there is no obligation to give a substantive response in 8 hours answering the issues of the request if the procedure needs more time, but the requesting party must be aware of what it is waiting for as soon as possible.

---

[219] The Directive on attacks against information systems. A Good Practice Collection for CERTs on the Directive on attacks against information systems ENISA P/28/12/TCD, Version: 1.5, 24 October, 2013. P. 3. [interactive]. [reviewed in 2 March 2020]. Available at: <https://www.enisa.europa.eu/publications/the-directive-on-attacks-against-information-systems/at_download/fullReport>

[220] Convention on Cybercrime.

[221] Ibid. art. 35.

[222] Directive 2013/40/EU. Art. 13, p.1.

'Those points of contact should be able to deliver effective assistance thus, for example, facilitating the exchange of relevant information available and the provision of technical advice or legal information for the purpose of investigations or proceedings concerning criminal offences relating to information systems and associated data involving the requesting Member State'[223]

However, it is important to emphasize that Directive did not established special rules for gathering evidence abroad[224]. Under the information exchange procedure, the parties may share the information which is accessible. For example, legal information (on national legislation issues), operative information (concerning particular criminal proceedings) or technical information (the form and process of application a request for mutual legal assistance). Usually, such information is auxiliary and cannot be used as evidence. In contrast, gathering evidence abroad is occurred according to the legislation of the requested party within the mutual legal assistance usually requiring a judge order or another approval.

The Directive encourages public private cooperation in order to prevent and combat cyberattacks, in particular, creation of the network for information exchange with service providers. In the Recital 23 of the Directive Preamble the forms of such cooperation are prescribed: 'support by service providers in helping to preserve potential evidence, in providing elements helping to identify offenders and, as a last resort, in shutting down, completely or partially, in accordance with national law and practice, information systems or functions that have been compromised or used for illegal purposes'[225]. In fact, these forms were introduced in the Cybercrime Convention to be executed by 24/7 contact points.

No doubts, the Directive aims to improve the cooperation within Member States to provide effective investigation of cybercrimes. However, it is important to understand that it does not abolish the mutual legal assistance requirements prescribed by the national legislation. And if the procedure of identification of IP address subscriber takes a lot of time because of the judicial procedure (receiving of a judge order, for example) established in the national legislation of the Member State, these rules cannot be evaded. Time-consuming issues of the mutual legal assistance procedures must be resolved through improving these provisions but not due to the simplifying the access to the information breaching the personal data protection rules. The cooperation must be improved 'fully respecting the rule of law'[226].

[223] Directive 2013/40/EU. Recital 22.
[224] IGLEZAKIS I. *The legal regulation of Cyber Attacks.* 2016. Kluwer Law International B. V.: the Netherlands. P. 98
[225] Directive 2013/40/EU. Recital 23;
[226] Ibid.

The Directive also obliges Member States to provide the Commission with the information on established points of contact in order to forward it to the other MS, particular EU agencies and bodies[227]. Additionally, the Directive requires to provide 'appropriate reporting channels in order to facilitate the reporting of the offences to the competent national authorities without undue delay'[228].

Although the Directive is addressed to cooperation only within the EU, the information exchange and mutual legal assistance with non-EU countries is equally important as cyberattacks are often committed from outside the EU.

Within the Ukraine EU Association Agreement, the cooperation with Europol and Eurojust increased. The Agreement on Operational and Strategic Cooperation between Ukraine and the European Police Office was signed on 14 December 2016 and ratified on 12 July 2017 when Ukraine appointed the Department of National Police for cooperation with Europol as contact point[229]. According to article 4 of the Agreement, the cooperation includes 'information exchange, the exchange of specialist knowledge, general situation reports, information on crime prevention methods…'[230] in order to combat different crimes, including computer crime[231]. The exchange of information with a purpose of combating serious crimes is also stipulated in the Agreement on cooperation between Ukraine and the European Union Agency for Criminal Justice Cooperation (Eurojust), which was signed on 27 June 2016 and ratified on 8 February 2017[232].

Ukraine fulfilled its obligations under the Cybercrime Convention regarding the 24/7 network and designated the Cyber-Police Department of the National Police of Ukraine to perform functions of the 24/7 point of contact. In terms of international cooperation the Cyber-Police Department is empowered to execute 'only police-to-police type of requests related to cybercrime and electronic evidence. It can provide assistance in the investigation of criminal offences connected with computer systems and exchange of operative

[227] Ibid. Art. 13(2);
[228] Ibid. Art. 13(3);
[229] The Agreement on Operational and Strategic Cooperation between Ukraine and the European Police Office. Law of Ukraine. 12 July 2017. [interactive]. [reviewed in 10 May 2020]. Available at: <https://zakon.rada.gov.ua/laws/show/984_001-16>;
[230] The Agreement on Operational and Strategic Cooperation between Ukraine and the European Police Office. 14 December 2016. [interactive]. [reviewed in 10 May 2020]. Available at: < https://www.europol.europa.eu/sites/default/files/documents/agreement_on_operational_and_strategic_cooperation_ukraine.pdf>
[231] Ibid., annex 1;
[232] The Agreement on cooperation between Ukraine and the European Union Agency for Criminal Justice Cooperation. Law of Ukraine. 8 February 2017. [interactive]. [reviewed in 10 May 2020]. Available at: <https://zakon.rada.gov.ua/laws/show/984_024-16>;

information (that is not the evidence in criminal proceedings)'[233]. If the requesting party needs aid within the mutual legal assistance, it cannot be provided solely by the Cyber-Police Department. Requests on mutual legal assistance can be executed only through the Ministry of Justice of Ukraine (if the request was submitted within the court proceeding) or through the General Prosecutor's Office (if the request was submitted within investigation stage)[234].

In fact, one of the largest obstacles for the effective cooperation between states is that procedures of mutual legal assistance are too time-consuming whereas investigation of crimes committed in cyberspace requires for speed reaction and fast gathering of evidence. In order to combat attacks against information systems effectively, the Cybercrime Convention introduced the set of actions on the mutual assistance regarding provisional measures (articles 29-34), particularly, measures on the assistance on the expedited preservation of stored computer data and traffic data expedited, including its partial reveal. These functions had to be fulfilled by the 24/7 contact point in order to combat cybercrimes effectively and fast.

However, these provisions were not appropriately implemented in the Ukrainian legislation. The Criminal Code of Ukraine does not even contain the term of 'electronic evidence'. To improve current situation, the definition of 'electronic evidence' has to be established in the Criminal Procedural Code of Ukraine as well as methods of gathering such type of evidence[235]. The necessity to improve the Ukrainian legislation regarding Convention provisional measures is established in the Cybersecurity Strategy of Ukraine. Particularly, paragraph 4.5 stipulates, inter alia, the following measures:

- 'improvement of procedural methods for collecting evidence in electronic form related to crime, improvement of classification, methods, means and technologies of identification and recording of cybercrimes, conducting expert research;
- establishment of the blocking procedure by operators and telecommunication providers of a certain (identified) information resource (information service) under a court decision;

[233] Cybercrime and cybersecurity strategies in the Eastern Partnership region. Updated report 2018. Bucharest, January 2019. P. 50. [interactive]. [reviewed in 10 May 2020]. Available at: <https://rm.coe.int/eap-cybercrime-and-cybersecurity-strategies/168093b89c>;
[234] The Criminal Procedural Code of Ukraine. Article 545. [interactive]. [reviewed in 10 May 2020]. Available at: <https://zakon.rada.gov.ua/laws/show/4651-17#n4235>;
[235] Департамент Кіберполіції України. Кіберполіція обговорила з представниками Ради Європи вдосконалення законодавства. *Інформаційний портал: СТОПКОР.* 1 лютого 2020. [interactive]. [reviewed in 10 May 2020]. Available at: < https://stopcor.org/kiberpolicziya-obgovoryla-z-predstavnykamy-rady-yevropy-vdoskonalennya-zakonodavstva/>;

- standardization of the procedure for making mandatory instructions by telecommunications operators and providers on the urgent recording and subsequent storage of computer data, storage of traffic data; real-time collection of traffic data and the real-time interception of content data
- settlement of the issue of the possibility of urgent procedural actions in real time with the use of electronic documents and electronic digital signature;
- introduction of a special procedure for removing information from telecommunications channels in the case of cybercrime investigation'[236].

The fulfilment of this strategy, appropriate establishment of listed measures, also within international cooperation, will encourage the cooperation on combating cybercrime.

The last but not the least obligation for Member Stated stipulated by the article 14 of the Directive is related to monitoring and statics on crimes prescribed by the articles 3-7. In the Recital 24 the Directive emphasized on the importance of collecting the 'comparable data on the offences'[237] with a purpose to make it 'available to the competent specialised Union agencies and bodies, such as Europol and ENISA, in line with their tasks and information needs, in order to gain a more complete picture of the problem of cybercrime and network and information security at Union level and thereby to contribute to formulating a more effective response'[238].

According to the article 14 of the Directive 'Member States are required to implement a system for the recording, production and provision of statistical data on the offences in the Directive, including at a minimum the number of offences and their follow-up, and indicating on an annual basis the number of reported cases investigated, the number of persons prosecuted, and the number of persons convicted. This data should be reported to the Commission and published in a statistical report'[239].

During the interviewing Member States before the Directive adoption ENISA defined the most significant obstacles which tackled the data collecting. Firstly, there is no single body or institution responsible for collecting and reporting information (in each Member State). There may be several such institutions (for example, the police and the prosecutor's

[236] On the decision of the National Security and Defense Council of Ukraine of January 27, 2016 'On the Cybersecurity Strategy of Ukraine'. Decree of the President of Ukraine. No. 96/2016. 15 March 2016. [interactive]. [reviewed in 11 May 2020]. Available at: <https://zakon.rada.gov.ua/laws/show/96/2016>
[237] Recital 24
[238] Ibid.
[239] The Directive on attacks against information systems. A Good Practice Collection for CERTs on the Directive on attacks against information systems ENISA P/28/12/TCD, Version: 1.5, 24 October, 2013. P. 29. [interactive].

office) which provide with a different with a different information. Consequently, the only one institution shall be appointed to collect and report the data on cybercrime[240].

Secondly, the differences on substantive criminal law prescribing the offences committed against information systems distort statistics. For example, if an act of *fishing* may be qualified differently in the Member States (fraud or identity theft), the statistical data becomes incomparable as one Member State does not include the data on fishing cases to the report on cybercrime[241].

Also, ENISA draws the attention to the latent criminal activity as many private companies, suffered from cybercrime, try to avoid the official prosecution as they are not willing to reveal their private business data to public authorities[242].

Collecting and sharing of the information about offences committed against information system is an essential part of cooperation on preventing and combating cybercrimes. Police may follow 'the routes' of offenders, observe their conduct and dynamic of committed offences. Consequently, the systems requiring higher level of protection may be defined and defended, the connections between offenders may be revealed, and in general the investigation process will be more effective.

CONCLUSIONS

To estimate the results of the paper, we should answer the questions which were initially defined in the introduction.

1. In this paper, we compared the provisions of the Directive 2013/40/EU with the Framework Decision and the Convention on Cybercrime. In fact, the Directive is based on the Cybercrime Convention and encourages its implementation by all possible means.

[240] Ibid.
[241] Ibid.
[242] Ibid.

The Directive has a wider scope of regulation than Framework Decision but narrower than Convention. Mainly Directive regulates issues on substantive criminal law regarding combating Cybercrime as it stipulates the offences of illegal access, illegal data interference, illegal system interference, illegal interception and offences related to the tools. However, its contribution to the procedural provisions is essential. The Directive aims to increase the cooperation within the Union as well as outside the EU. To combat cyber attacks effectively, the cooperation must be substantive and fast. For this reason, the Directive obliged the contact points of the States to provide answers to urgent requests within 8 hours. However, this requirement settled not for the substantive answers but rather for primary (consulting). Another crucial novelty is the obligation on data collection and sharing. The Directive established a stricter penalties approach changing the 'range' to a concrete term of imprisonment as a minimum maximum penalty. The most crucial novelties of the Directive are related to the aggravating circumstances: identity theft, botnets and critical infrastructure.

2. In general, Member States fulfilled their obligations to implement the Directive provisions. Problem issues may arise mainly regarding the list of actions prescribed by the article as many countries do not include the full list and omit some actions. Also, discrepancies arise regarding some additional conditions of punishment prescribed by the national legislation of the Member States. For instance, when an act may be punished only in case it caused a serious harm, or only in case of special intent, it falls behind the Directive and minimum standards are not adhered. On the other hand, the Directive does not oblige the Member States to change their legislation if it seems to be even stricter. For example, in this paper the debatable issue on the element of breaching the security measure for the criminalization of allegal access was discussed. It is important to understand that Directive does not oblige to decriminalize the conduct.

3. Although the Ukrainian legislation partially corresponds to the Cybercrime Convention (on substantive law provisions), it may be improved considering the Directive standards and foreign experience.

Firstly, the offences of illegal access, illegal system interference and illegal data inference should be defined under separate articles, or at least under different parts of an article. The actus reus of these offences must be strongly distinguished and maximum penalties should range regarding the level of public danger of the offence. Moreover, the offence of illegal access to the information system has to be punished at least in case of breaching the security measure, even in case of the absence of consequences, as 'hacking'

is already an intentional offence which does not require to result in major harm. At the same time, I would not recommend the adoption of the Directive approach on the imposition of punishment only in case of hacking a security measure, as the offence similar by its harm may be committed by different means. Regarding the offence of illegal data interception, it needs some improvements concerning electromagnetic emissions. The article, prescribing the offence on the misuse of tools should widen the list of prescribed actions, including the 'procurement for use'. I appreciate the novelties of the Directive on the aggravating circumstances. I'm convinced, that offences which committed through botnets, must be punished stricter as such attacks affect not only the devices of the 'victim' but also those which were used for the criminal purpose not by their will. The establishment of a list of information systems of critical infrastructure is necessary not only because of the need to protect them better, but also for establishment higher penalties for attacks against such systems. The last but not the least (from the substantive criminal law) is improvements regarding the identity theft.

The implementation of the procedural provisions of the Cybercrime Convention is also essential within international cooperation, as for today, the 24/7 contact point of Ukraine for today is not effective enough because of the lack of relevant legislation.

LIST OF REFERENCES

I. Regulatory legal acts

- **International Legal Acts**

1. 1950. European Convention on Human Rights. [interactive]. [reviewed in 10 April 2020]. Available at:< https://www.echr.coe.int/Documents/Convention_ENG.pdf>

2. 2001. Convention on Cybercrime. *European Treaty Series*. No. 185. [interactive]. [reviewed in 10 May 2020]. Available at: <http://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561>

- **European Legal Acts**

1. Consolidated version of the Treaty on the Functioning of the European Union. *Official Journal of the European Union.* No. C 326/47. 26 October 2012. [interactive]. [reviewed in 10 May 2020]. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012E/TXT&from=EN>

2. Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA. *Official Journal of the European Union.* No. L 218/8. 14 August 2013. [interactive]. [reviewed in 10 May 2020]. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013L0040&from=EN>

3. Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems. *Official Journal of the European Union.* No. L 69/67. 16 March 2005. [interactive]. [reviewed in 3 May 2020]. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32005F0222&from=EN>;

4. Association Agreement between the European Union and its Member States, of the one part, and Ukraine, of the other part. *Official Journal of the European Union.* L 161/3. 29 May 2014. [interactive]. [reviewed in 9 May 2020]. Available at: <https://trade.ec.europa.eu/doclib/docs/2016/november/tradoc_155103.pdf>

5. The Agreement on Operational and Strategic Cooperation between Ukraine and the European Police Office. 14 December 2016. [interactive]. [reviewed in 10 May 2020]. Available at: <https://www.europol.europa.eu/sites/default/files/documents/agreement_on_operational_and_strategic_cooperation_ukraine.pdf>

- **The national legislation of Member States**

1. The Criminal Code of the Kingdom of Belgium. (Previous version). [interactive]. [reviewed in 1 May 2020]. Available at: <https://issuu.com/ethics360/docs/penal_code__belgium_>
2. The Criminal Code of the Kingdom of Belgium. (1867, as of 2018). [interactive]. [Reviewed in 1 May 2020]. Available at: <https://www.legislationline.org/download/id/8240/file/Belgium_CC_1867_am2018_fr.pdf>

3. The Criminal Code of the Republic of Bulgaria (1968, amended 2017). English version. [interactive]. [reviewed in 6 March 2020]. Available at: <https://www.legislationline.org/download/id/8395/file/Bulgaria_Criminal_Code_1968_am2017_ENG.pdf
4. The Criminal Code of the Republic of Estonia (2001, amended 2019). English version. [interactive]. [reviewed in 30 April 2020]. Available at: <https://www.legislationline.org/download/id/8244/file/Estonia_CC_am2019_en.pdf>
5. The Criminal Code of the Republic of Lithuania (amended 2017). English version. [interactive]. [reviewed in 5 May 2020]. Available at: <https://www.legislationline.org/download/id/8272/file/Lithuania_CC_2000_am2017_en.pdf>
6. The Criminal Code of the Republic of Malta (1854, amended December 2019). English version. [interactive]. [reviewed in 30 April 2020]. Available at: <https://www.legislationline.org/download/id/8555/file/Malta_Criminal_Code_amDec2019_en.pdf>
7. The Criminal Code of the Kingdom of Netherlands. (1881, amended on 2012). English version. [interactive]. [reviewed in 2 March 2020]. Available at: <https://www.legislationline.org/download/id/6415/file/Netherlands_CC_am2012_en.pdf>
8. The Criminal Code of the Kingdom of Spain (1995, as of 2013). English version. [interactive]. [Reviewed in 12 April 2020]. Available at:

<https://www.legislationline.org/download/id/6443/file/Spain_CC_am2013_en.pdf>

9. The Criminal Code of the Republic of Finland (1889, as of 2015). English version. [interactive]. [reviewed in 8 May 2020]. Available at: https://www.legislationline.org/download/id/6375/file/Finland_CC_1889_am2015_en.pdf>
10. The Criminal Code of the French Republic (as of 2005). English version. [interactive]. [reviewed in 2 March 2020]. Available at: <https://www.legislationline.org/download/id/3316/file/France_Criminal%20Code%20updated%20on%2012-10-2005.pdf>
11. The Criminal Code of the French Republic (as of January 2020). French version. [interactive]. [reviewed in 5 April 2020]. Available at: <https://www.legislationline.org/documents/section/criminal-codes/country/30/France/show>

- **Ukrainian national legislation**

1. On the implementation of the Association Agreement between Ukraine, of the one part, and the European Union, the European Atomic Energy Community and their Member States, of the other part. Regulation of the Cabinet of Ministers of Ukraine. 25 October 2017. No. 1106. [interactive]. [reviewed in 9 May 2020]. Available at: <https://zakon.rada.gov.ua/laws/show/1106-2017-%D0%BF>
2. The Agreement on Operational and Strategic Cooperation between Ukraine and the European Police Office. Law of Ukraine. 12 July 2017. [interactive]. [reviewed in 10 May 2020]. Available at: <https://zakon.rada.gov.ua/laws/show/984_001-16>;
3. The Agreement on cooperation between Ukraine and the European Union Agency for Criminal Justice Cooperation. Law of Ukraine. 8 February 2017. [interactive]. [reviewed in 10 May 2020]. Available at: <https://zakon.rada.gov.ua/laws/show/984_024-16>;
4. The Criminal Code of Ukraine. Law of Ukraine. 5 April 2001. No. 2341-III. [interactive]. [reviewed in 8 May 2020]. Available at: <https://zakon.rada.gov.ua/laws/show/2341-14/ed20010405>

5. The Criminal Procedural Code of Ukraine. Article 545. [interactive]. [reviewed in 10 May 2020]. Available at: <https://zakon.rada.gov.ua/laws/show/4651-17#n4235>
6. The Code of Ukraine of Administrative offences. Law of Ukraine. 7 December 1984. No. 8073[1]-X. [interactive]. [reviewed in 7 May 2020]. Available at:< https://zakon.rada.gov.ua/laws/show/80731-10/ed20200428>
7. On the basic principles of cybersecurity in Ukraine. Law of Ukraine. 10 May 2017.No. 2163-VIII. [interactive]. [reviewed in 9 May 2020]. Available at: <https://zakon.rada.gov.ua/laws/show/2163-19>
8. On the decision of the National Security and Defense Council of Ukraine of January 27, 2016 'On the Cybersecurity Strategy of Ukraine'. Decree of the President of Ukraine. No. 96/2016. 15 March 2016. [interactive]. [reviewed in 11 May 2020]. Available at: <https://zakon.rada.gov.ua/laws/show/96/2016>
9. Procedure for the formation of the list of information and telecommunication systems of critical infrastructure of the state. Regulation of the Cabinet of Ministers of Ukraine. No. 563. 23 August 2016. [interactive]. [reviewed in 11 May 2020]. Available at: < https://zakon.rada.gov.ua/laws/show/563-2016-%D0%BF>
10. About the ownership of certain types of property. Regulation of the Parliament of Ukraine. 17 June 1992. No. 2471-XII. [interactive]. [reviewed in 8 May 2020]. Available at: <https://zakon.rada.gov.ua/laws/show/2471-12>

II. Special literature

1. ADAMS A. A., MCCRINDLE R. J., *Pandora's Box: Social and Professional Issues of the Information Age*. John Wiley&Sons Ltd. 2008. p. 666.
2. АНТИПОВ В. Диспозиції статей Кримінального кодексу України з кваліфікованими складами злочину потребують корегування. *Міжнародний юридичний вісник: актуальні проблеми сучасності (теорія та практика)*. 2017 (1). С. 34-42.
1. BIASIOTTI M. A., PIA J., *Handling and Exchanging Electronic Evidence Across Europe*. Springer, 2018. P. 420.
2. BŘEZINOVÁ K. *Company Criminal Liability for Unlawful Attacks against Information Systems within the Scope of EU Law*. Charles University in Prague

Faculty of Law Research Paper No. 2017/II/3., 5 June 2017. P. 27. [interactive]. [reviewed in 2 March 2020]. Available at: <https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID2989005_code2308341.pdf?abstractid=2989005&mirid=1&type=2>

3. CALDERONI F., The European legal framework on cybercrime: Striving for an effective implementation. *Crime, Law and Social Change* 54, 5 (2010) P. 339-357. [interactive]. [reviewed in 3 May 2020]. Available at: <https://www.researchgate.net/publication/227301292_The_European_legal_framework_on_cybercrime_Striving_for_an_effective_implementation>
4. CSONKA, P. The council of europe's convention on cyber-crime and other European initiatives. *Revue internationale de droit pénal*, vol. 77(3), 2006. P. 473-501.
5. DASKAL J. The Un-Territoriality of data. *The Yale Law Journal*. P. 326-398. [interactive]. [reviewed in 3 March 2020]. Available at: <https://www.yalelawjournal.org/pdf/a.326.Daskal.398_qrhgeoar.pdf
6. HERT P., FUSTER G., KOOPS B., Fighting cybercrime in the two Europes: The added value of the EU framework decision and the council of Europe Convention. *Revue internationale de droit pénal*, vol. 77(3), 2006, p. 505. [interactive]. [reviewed in 10 May 2020]. Available at: <https://www.researchgate.net/publication/251058766_Fighting_cybercrime_in_the_two_Europes_The_added_value_of_the_EU_framework_decision_and_the_Council_of_Europe_convention>
7. IGLEZAKIS I. *The legal regulation of Cyber Attacks.* 2016. Kluwer Law International B. V.: the Netherlands. P. 256.
8. KLIMEK L. Criminal Liability of Legal Persons in Case of Computer Crime: A European Union Response. International and Comparative Law Review, 2015, vol. 15, no. 2, p. 135-142. [interactive]. [reviewed in 2 April]. Available at: <https://www.researchgate.net/publication/322710330_Criminal_Liability_of_Legal_Persons_in_Case_of_Computer_Crime_A_European_Union_Response>
9. MITSILEGAS V. *EU Criminal Law.* Oxford and Portland, Oregon: Hart Publishing 2009. P. 366.
10. Науково-практичний коментар Кримінального кодексу України за редакцією М. І. Мельника, М. І. Хавронюка. 7-е вид., переробл. та допов. Київ: Юридична думка, 2010. 1288 с.

11. Науково-практичний коментар Кримінального кодексу України за редакцією М. І. Мельника, М. І. Хавронюка. 11-те вид., переробл. та допов. Київ: ВД «Дакор», 2019. 1384 с.

12. MONGILLO V. Corporate criminal liability and compliance programs. Volume II towards a common model in the European Union. Edited by Antonio Fiorella. JOVENE EDITORE 2012. Chapter II. p. 55-120. [interactive]. [reviewed in 5 May 2020]. Available at: <https://www.academia.edu/6224944/The_Nature_of_Corporate_Liability_for_Criminal_Offences_Theoretical_Models_and_EU_Member_State_Laws>

13. MONGILLO V. Corporate criminal liability and compliance programs. Volume II towards a common model in the European Union. Edited by Antonio Fiorella. JOVENE EDITORE 2012. Chapter III. P. 121-169. [interactive]. [reviewed in 5 May 2020]. Available at: <https://www.academia.edu/6224953/The_Allocation_of_Responsibility_for_Criminal_Offences_Between_Individuals_and_Legal_Entities_in_Europe>

14. МУЗИКА А., АЗАРОВ Д., *Законодавство України про кримінальну відповідальність за "комп'ютерні" злочини: науково-практичний коментар і шляхи вдосконалення*. К.: Вид. ПАЛИВОДА А. В., 2005. 120 с.

15. NAGY H., MEZEI K., The Organised Criminal Phenomenon on the Internet. *Journal of Eastern-European Criminal Law,* vol. 2016 (2). p. 137-149. HeinOnline.

16. OPHARDT, J. A. Cyber Warfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow's Battlefield. Duke Law & Technology Review, 2010. [interactive]. [reviewed in 4 March 2020]. Available at: <https://heinonline.org/HOL/PrintRequest?collection=journals&handle=hein.journals/dltr2010&div=7&id=49&print=section&format=PDFsearchable&submit=Print%2FDownload>

17. PERLOFF-GILES A. *Transnational Cyber Offenses: Overcoming Jurisdictional Challenges.* P. 196. [interactive]. [reviewed in 5 March 2020]. Available at: <https://cpb-us-w2.wpmucdn.com/campuspress.yale.edu/dist/8/1581/files/2018/02/191_Transnational-Cyber-Offenses-2i9mpg2.pdf>

18. SATZGER H. *The Harmonisation of Criminal Sanctions in the European Union* - A New Approach. eucrim - The European Criminal Law Associations' Forum. 2019 (2).

P. 115-120. [interactive]. [reviewed in 29 March 2020]. Available at: <https://eucrim.eu/media/issue/pdf/eucrim_issue_2019-02.pdf#page=41>

19. SAULIŪNAS D. Legislation on cybercrime in Lithuania: development and legal gaps in comparison with the Convention on cybercrime. *Jurisprudence*. 2010, 4(122). P. 203–219. [interactive]. [reviewed in 5 May 2020]. Available at: <https://www.mruni.eu/upload/iblock/822/11_Sauliunas.pdf>
20. STRELCOV L. The System of Cybersecurity in Ukraine: Principles, Actors, Challenges, Accomplishments. *Springer*. November 2017. P. 7. [interactive]. [reviewed in 4 April 2020]. Available at: <https://www.researchgate.net/publication/321037340_The_System_of_Cybersecurity_in_Ukraine_Principles_Actors_Challenges_Accomplishments/citations>
21. SUMMERS S., SCHWARZENEGGER CH., EGE G., YOUNG F., *The Emergence of EU Criminal Law. Cyber Crime and the Regulation of the Information Society*. Oxford and Portland, Oregon: Hart Publishing 2014. P. 327.
22. FREITAS P., GONÇALVES N. Illegal access to information systems and the Directive 2013/40/EU, *International Review of Law, Computers & Technology*, 29:1, 2015. P. 50-62. [interactive]. [reviewed in 12 May 2020]. Available at: <https://www.tandfonline.com/doi/full/10.1080/13600869.2015.1016278>
23. VASILESCU S. Illegal interception of computer data transmission in the regulation of the New Romanian Criminal Code. *Journal of Law and Administrative Sciences*. 2015(3). P. 230 -238. [interactive]. [reviewed in 8 May 2020]. Available at: <https://pdfs.semanticscholar.org/20f3/b4ce7c67c19d4cf51982b74d72458e8d8016.pdf>
24. DR. ADEL AZZAM SAQF AL HAIT. Jurisdiction in Cybercrimes: A Comparative Study. *Journal of Law, Policy and Globalization*, Vol.22, 2014. P. 75-84. [interactive]. [reviewed in 2 March 2020]. Available at: <https://www.iiste.org/Journals/index.php/JLPG/article/viewFile/11050/11351>
25. Effectiveness, Proportionality and Dissuasiveness. *Eastern and Central European Journal on Environmental Law,* vol. 15, no. 2, 2012, p. 11-13. HeinOnline. [interactive]. [reviewed in 4 April 2020]. Available at: <https://heinonline.org/HOL/PrintRequest?public=true&handle=hein.journals/eceujevl15&div=13&start_page=11&collection=journals&set_as_cursor=0&men_tab=srchresults&print=section&format=PDFsearchable&submit=Print%2FDownload>

III. Court Jurisprudence

1. The European Court of Human Rights. 24 July 2014. (Final 15 December 2014). Judgement *Čalovskis v. Latvia*. Case No. 22205/13
2. EU Court of Justice. *21 September 1989. Commission V. Greece. Case No. 68/88.* (Greek Maize case). [interactive]. [reviewed in 30 March 2020]. Available at: <https://eur-lex.europa.eu/resource.html?uri=cellar:4f255660-f631-479c-91b7-7abaf62826d1.0002.06/DOC_1&format=PDF>
3. Judgment of the Paris Court of Appeal. 30 October 2002. Case of Tati against Kitetoa.com. Hereafter unless another indicated, the translation is mine. [interactive]. [reviewed in 3 March 2020]. Available at: <https://www.kitetoa.com/Pages/Textes/Les_Dossiers/Tati_versus_Kitetoa/arret-cour-appel.shtml>
4. Judgement of Pervomaisky District Court of Chernivtsi. 14 August 2019. No. 725/3848/19. [interactive]. [reviewed in 7 May 2020]. Available at: <http://www.reyestr.court.gov.ua/Review/83693746>
5. Judgment of Amur-Nizhnedneprovsky District Court of Dnipropetrovsk. 2 July 2013. No. 1-726 / 11. [interactive]. [reviewed in 7 May 2020]. Available at: <http://www.reyestr.court.gov.ua/Review/45323511>
6. Judgement of Koroliovsky District Court of Zhytomyr. 21 February 2019. *No. 296/1022/19.* [interactive]. [reviewed in 5 May 2020]. Available at: <http://www.reyestr.court.gov.ua/Review/80006556>
7. Judgement of Prymorsky District Court of Mariupol. 4 April 2019. *No. 331/5129/18.* [interactive]. [reviewed in 5 May 2020]. Available at: <http://www.reyestr.court.gov.ua/Review/80937191>
8. Judgement of Nizhyn City District Court. 9 April 2020. *No. 740/684/20.* [interactive]. [reviewed in 7 May 2020]. Available at: <http://www.reyestr.court.gov.ua/Review/88689172>
9. Judgement of Primorsky District Court of Odessa. 8 May 2018. *No. 522/8715/13-k.* Available at: <http://reyestr.court.gov.ua/Review/73869949>
10. The judgement of Nikopol City District Court of the Dnipro region. 30 August 2018. *No. 182/4213/18.* [interactive]. [reviewed in 9 May 2020]. Available at: <http://www.reyestr.court.gov.ua/Review/76270022>
11. Judgement of Berdyansk City District Court of Zaporizhia. 24 September 2019. *No. 310/4556/19.* [interactive]. [reviewed in 9 May 2020]. Available at: <http://www.reyestr.court.gov.ua/Review/84471272>
12. Judgement of Kyiv District Court of Kharkiv. 23 March 2017. *No. 640/953/17.* [interactive]. [reviewed in 9 May 2020]. Available at: <http://reyestr.court.gov.ua/Review/65496457>

IV. Other practical material

- **Reports**

1. The Directive on attacks against information systems. A Good Practice Collection for CERTs on the Directive on attacks against information systems ENISA P/28/12/TCD, Version: 1.5, 24 October, 2013. P. 2. [interactive]. [reviewed in 2 March 2020]. Available at: <https://www.enisa.europa.eu/publications/the-directive-on-attacks-against-information-systems/at_download/fullReport>
2. Report from the Commission to the European Parliament and the Council on assessing the extent to which the Member States have taken the necessary measures in order to comply with Directive 2013/40/EU on attacks against information systems and replacing Council Framework Decision 2005/222/JHA. Brussels, 13 September 2017. P. 13. [interactive]. [reviewed in 8 May 2020]. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017DC0474&from=en>
3. Explanatory Report to the Convention on Cybercrime dated on 23 November 2001. European Treaty Series - No. 185. P. 60. [interactive]. [reviewed in 5 May 2020]. Available at: <https://rm.coe.int/16800cce5b>
4. Cybercrime and cybersecurity strategies in the Eastern Partnership region. Updated report 2018. Bucharest, January 2019. P. 50. [interactive]. [reviewed in 10 May 2020]. Available at: <https://rm.coe.int/eap-cybercrime-and-cybersecurity-strategies/168093b89c>

- ***Material observing Court Jurisprudence***

5. BENSOUSSAN A. Unauthorized access to IT systems. *The Lexing Network informs you. Special International issue.* 2014 (7). P. 20. [interactive]. [reviewed in 6 April]. Available at: <https://www.alain-bensoussan.com/wp-content/uploads/2014/06/24295061.pdf>
6. WATIN-AUGOUARD M. Data theft: the French Court of Cassation refines the Godfrain Law. *Fic Observatory.Com.* 4 August 2015. [interactive]. [reviewed in 5 March 2020]. Available at: <https://observatoire-fic.com/en/data-theft-the-french-court-of-cassation-refines-the-godfrain-law/>
7. STANCHI A., PEDRONI A. *Unauthorised access of computer system by former employee.*13 April 2016.
8. [interactive]. [Reviewed in 2 March 2020]. Available at: https://www.internationallawoffice.com/Newsletters/Employment-Benefits/Italy/Stanchi-Studio-Legale/Unauthorised-access-of-computer-system-by-former-employee#
9. Turner M. Case R v Steffan Needham. *Database: Computer Misuse Act 1990 cases.* [interactive]. [reviewed in 5 May 2020]. Available at: <http://www.computerevidence.co.uk/Cases/CMA.htm>
10. The conviction of journalists who illegally intercepted radio communications between law-enforcement officers did not infringe their right to freedom of

expression. *Press Release issued by the Registrar of the Court ECHR 223* (2016).23 June 2016. [interactive]. [reviewed in 17 April 2020]. Available at: < https://hudoc.echr.coe.int/app/conversion/pdf?library=ECHR&id=003-5415795-6778471&filename=Judgment%20Brambilla%20and%20Others%20v.%20Italy%20-%20interception%20of%20law-enforcement%20officers%27%20radio%20communications%20by%20journalists.pdf>

11. CHAMPEAU G. La cour de cassation confirme que la publication de failles de sécurité exploitables est un délit. [interactive]. [Reviewed in 12 April 2020]. Available at: <https://www.numerama.com/magazine/14745-la-cour-de-cassation-confirme-que-la-publication-de-failles-de-securite-exploitables-est-un-delit.html>
12. Est-il illégal de publier des failles de sécurité ? 24 December 2009. *Criminalités numériques.*[interactive]. [Reviewed in 12 April 2020]. Available at: <https://blog.crimenumerique.fr/tag/atteintes-aux-stad/>

- ***Other material***

13. Chart of signatures and ratifications of Treaty 185 *Convention on Cybercrime.* [interactive]. [Reviewed in 03 May 2020]. Available at: <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures>
14. What is the Difference Between Black, White and Grey Hat Hackers? *Norton.* [Interactive]. [Reviewed in 5 March 2020]. Available at: <https://us.norton.com/internetsecurity-emerging-threats-what-is-the-difference-between-black-white-and-grey-hat-hackers.html>
15. PLOHMANN D., GERHARDS-PADILLA E., LEDER F. Botnets: Detection, Measurement, Disinfection & Defence. ENISA. Edited by Dr. Giles Hogben. P. 91. [interactive]. [reviewed in 7 May]. Available at: < https://www.enisa.europa.eu/publications/botnets-measurement-detection-disinfection-and-defence/at_download/fullReport>
16. Департамент Кіберполіції України. Кіберполіція обговорила з представниками Ради Європи вдосконалення законодавства. *Інформаційний портал: СТОПКОР.* 1 лютого 2020. [interactive]. [reviewed in 10 May 2020]. Available at: < https://stopcor.org/kiberpolicziya-obgovoryla-z-predstavnykamy-rady-yevropy-vdoskonalennya-zakonodavstva/>
17. LOHNER A., BEHR N. Corporate Liability in Germany. *Global Compliance News.* [interactive]. [reviewed in 1 May 2020].
18. Available at: <https://globalcompliancenews.com/white-collar-crime/corporate-liability-in-germany/>
19. Brandom R. UK hospitals hit with massive ransomware attack. *THE VERGE.* [interactive]. [reviewed in 5 May 2020]. Available at: <https://www.theverge.com/2017/5/12/15630354/nhs-hospitals-ransomware-hack-wannacry-bitcoin>
20. WannaCry – the worm that just won't die. Naked Security by Sophos. 2019. [interactive]. [reviewed in 5 May 2020]. Available at:

21. <https://nakedsecurity.sophos.com/2019/09/18/wannacry-the-worm-that-just-wont-die/>
22. KREBS B. Mariposa' Botnet Authors May Avoid Jail Time. *Krebs on Security*. [interactive]. [Reviewed in 12 April 2020]. Available at: <https://krebsonsecurity.com/2010/03/mariposa-botnet-authors-may-avoid-jail-time/>
23. Suspected 'Mariposa Botnet' creator arrested. *Spacewar*. 28 July 2010. [interactive]. [reviewed in 9 May 2020]. Available at: <https://www.spacewar.com/reports/Suspected_Mariposa_Botnet_creator_arrested_999.html>
24. Slovenian hacker sentenced to jail for 'malicious' program. *Physorg*. [interactive]. [Reviewed in 12 April 2020]. Available at: <https://phys.org/news/2013-12-slovenian-hacker-sentenced-malicious.html>
25. TEFFER P. 'EU admits to problems in penalty regime'. 12 April 2018. [interactive]. [reviewed in 29 March 2020]. Available at: <https://euobserver.com/economic/141583>
26. Cambridge Dictionary. [interactive]. [reviewed in 5 April 2020]. Available at: < https://dictionary.cambridge.org/dictionary/english/botnet>

SUMMARY

In the first part of the work I compared the provisions of the Directive with the Cybercrime Convention and the Framework Decision. Also, I analyzed the general provisions of the criminal Ukrainian legislation on combating cybercrimes.

In the second part of the work I made a comparative analysis the provisions of the Directive on the offences of illegal access, illegal data interference, illegal system interference, illegal interception and offences related to the tools and compared them with the Ukrainian legislation. Relevant proposals for the improvement of the Ukrainian legislation are presented.

In the third part I analyzed the minimum maximum penalties prescribed by the Directive and sanctions against legal persons. I concluded that the relevant liability for legal person for cybercrimes has to be established in Ukraine.

The fourth part of my research I devoted to the procedural aspects of the Directive, including information exchange, monitoring and statistics.