UNIVERSITY OF TIMISOARA
FACULTY OF LAW

UNIVERSITY OF PÉCS
FACULTY OF LAW

JOURNAL OF EASTERN-EUROPEAN CRIMINAL LAW

No. 2/2020

Edited biannually by courtesy of the Criminal Law Departments within the Law Faculties of the West University of Timisoara and the University of Pécs

UNIVERSUL JURIDIC

2020

Universul Juridic Publishing House

Edited by Universul Juridic Publishing House

Copyright © 2020, UNIVERSUL JURIDIC S.R.L.

All rights on this edition are reserved to Universul Juridic Publishing House

No part of this volume can't be copied without the subscription of Universul Juridic Publishing House

The journal is indexed in databases SSRN, EBSCO, HeinOnline.

ISSN 2360–4964

Redactor:	Ciprian Radu
Tehnoredactor:	Tania Militaru
Copertă:	Aurelian Leahu

Redacţie:
tel.: 0732.320.666
e-mail: redactie@universuljuridic.ro

Distribuţie:
tel.: 021.314.93.15
fax: 021.314.93.16
e-mail:
distributie@universuljuridic.ro

editurauniversuljuridic.ro

Editura Universul Juridic

Portal:
tel.: 0725.683.560
e-mail: portal@universuljuridic.ro

universuljuridic.ro

Universul Juridic

Librăria UJmag:
tel.: 0733.673.555; 021.312.22.21
e-mail: comenzi@ujmag.ro

ujmag.ro

Ujmag.ro

WEST UNIVERSITY OF TIMISOARA
FACULTY OF LAW

UNIVERSITY OF PÉCS
FACULTY OF LAW

Center of Research in Criminal Sciences
FACULTY OF LAW
West University of Timisoara

JOURNAL OF EASTERN-EUROPEAN CRIMINAL LAW

❍ BOARD OF EDITORS ❍

Editors-in-Chief

Lect. dr. LAURA STĂNILĂ
West University of Timisoara
Faculty of Law

Prof. dr. ZORAN PAVLOVIC
University of Novi Sad
Faculty of Law

Conf. dr. FLAVIU CIOPEC
West University of Timisoara
Faculty of Law

Prof. dr. ISTVÁN GÁL
University of Pécs
Faculty of Law

Honorary Member
Prof. dr. VIOREL PAȘCA

Editors

Dr. CSONGOR HERKE
Dr. SILVIA SIGNORATO
Dr. MIHÁLY TÓTH
Dr. IOANA CELINA PAȘCA
Dr. LÁSZLÓ KŐHALMI
Dr. ZOLTÁN ANDRÁS NAGY
Dr. CSABA FENYVESI
Dr. RUXANDRA RĂDUCANU

SCIENTIFIC BOARD

Prof. dr. Ulrich Sieber, director Max Planck Institute for International Criminal Law; Prof. dr. Ye Qing. Chancellor Law Institute of SASS, Shanghai; Prof. dr. Zoran Stojanović, University of Belgrade, Faculty of Law; Prof. dr. Vid Jakulin, University Lublijana, Faculty of Law; Prof. dr. Roberto E. Kostoris, Ordinario di Diritto processuale penale nell'Università di Padova; Prof. dr. Zoran Pavlovic, Faculty of Law for Business and Judiciary; Prof. dr. Tudorel Toader, Chancellor University A.I. Cuza Iasi, Faculty of Law, Justice minister; Prof. dr. Florin Streteanu, University „Babes-Bolyai" Cluj-Napoca, Faculty of Law; Prof. dr. Valerian Cioclei, Bucharest University, Faculty of Law; Prof. dr. Elek Balazs, Debrecen University, Faculty of Law; Prof. dr. Silvio Riondato, Università degli Studi di Padova; Prof. dr. Yuri Pudovochkin, Russian State University of Justice; dr. sc. Matko Pajčić, assistant professor, Law Faculty, University of Split, Croatia, prof. dr. François Rousseau, Université de Nantes, dr. habil. István Resperger, Associate Professor, National University of Public Sevice Budapest; dr. habil. József Boda PhD, associate Professor National University of Public Sevice, Budapest; Gary Hill, Scientific Coordinator of the International Scientific and Professional Advisory Council of the United Nations Crime Prevention and Criminal Justice Program (ISPAC), prof. dr. Ovidiu Predescu, General secretary of Academy of Legal Sciences of Romania.

The board of editors shall not take responsibility for the authors' opinions; therefore the authors are exclusively responsible for the former.

FOR CONTRIBUTORS

Journal of Eastern-European Criminal Law could stand out as a unique publication, at least in this part of the world, as an outcome of the partnership between specialists in Criminal law and Criminal Procedure law from the law faculties of the West University in Timisoara and the University in Pecs, who aimed at presenting, in a different language from their own, the serious amendments of criminal legislation that occurred in their countries in the post-communist era, an essential requirement for the rule of law. We envisage this journal, published semesterly, to be open to all researchers in the academic environment from the former communist countries, to professors, PhD students, but also, to magistrates and other professionals interested in the evolution of criminal legislation and in the more and more firm response to be given to the criminal phenomenon, while observing the fundamental human rights.

Our concerns aim at enlisting the Journal in additional databases, others than the ones in which the magazine is presently indexed, **namely Social Science Research Network (SSRN), EBSCO and HeinOnline.**

Any correspondence with the journal editors shall be sent with the mention „for the Journal of Eastern-European Criminal Law" at the following mail addresses:

laura.stanila@e-uvt.ro; flaviu.ciopec@e-uvt.ro; gal.istvan@ajk.pte.hu; zoran.pav@hotmail.com

For the time being, the journal cannot pay copyright compensation, any collaboration article shall therefore be voluntarily submitted.

Non-patrimonial copyright is protected, so any reproduction, representation, adaptation, translation and/or modification, partial or total, or transfer to a site of the articles, without consent of the authors, is prohibited.

The articles to be published shall be written in the following forma:

Title (capital letters, bold type, centered, 14)

Author(s)' name *(e.g. Sandra Marked[1], Werner Taylor[2], Roland G. Rowling[3]) (italics, bold type, centered, 12)*

Scientific degree, position (in order of the marking number), centered

Abstract and key words: Times New Roman font type, size 12.

The **text** shall be typed on A4 size (white copy paper), margins: left 3 cm, others 2.5 cm, Times New Roman font type, size 12.

Headings (chapter titles) shall be in capitals, with a blank line preceding and following them.

Within chapters, subheadings shall be italicized with a blank line preceding and following them.

References shall be listed **at the end of the paper, in alphabetical order.**

The recommended form of the list of references at the end of the paper: 1. Lippman, M: *Contemporary Criminal Law*, London: Sage Publications, 2007, p...

The paper shall be written exclusively in English and shall be accompanied by an abstract in English (10-15 lines).

THE BOARD OF EDITORS

Contents

Silvia Signorato
A New Right in Criminal Procedure Implied by Human Dignity:
The right to Non-Automated Judicial Decision-Making 9

Laura Stanila
New Species of Criminal Phenomena: Organized Cybercrime 17

Zoran S. Pavlović
About Legality of *On Line* Trials in Criminal Procedure 33

Giulia Lanza
Fake News and the Challenges of Criminal Law 43

Nikola Paunovic
New Technologies and Freedom of Expression with the Reference to the
Case Law of European Court of Human Rights 66

Fenyvesi Csaba
Future Developments and Challenges in Criminalistics as Part of
Criminal Justice 74

Aleksandar R. Ivanović
Online Hate Speech in the Time of the Covid-19 Crisis and Challenges for
Serbian Criminal Justice System 88

Dávid Tóth, Zsolt Gáspár
Jurisdictional Challenges of Cybercrime 101

Matei-Ciprian Graur
The Refusal to Carry Out Unpaid Work for the Benefit of the Community
by the Defendant – From Right to "Procedural Trap" 119

Goran Maričić, Gojko Pavlović
Necessity of the Regulation of Virtual Currency in Bosnia and
Herzegovina in the EU Harmonisation Process 129

Marina Matic Boskovic
Implications of New Technologies on Criminal Justice System 137

A New Right in Criminal Procedure Implied by Human Dignity: The right to Non-Automated Judicial Decision-Making

Silvia Signorato*

Abstract

The right to respect for human dignity is a fundamental right that gives substance to all other rights. Human dignity is inviolable. It prevents any reification of man and postulates respect for the Kantian categorical imperative, which states that «Act in such a way that you treat humanity, whether in your own person or in the person of any other, never merely as a means to an end, but always at the same time as an end».

However, information technology poses new challenges regarding human dignity. This article analyses this issue in relation to the possibility of criminal judgements being issued by machines. In some cases, this kind of judgement is considered acceptable by Article 11 of directive (EU) 2016/680. However, a question must be asked: Does such automated judicial decision-making respect human dignity or not?

The article shows the incompatibility of robotic decisions with the right to respect for human dignity. Consequently, Article 11 of Directive (EU) 2016/680, in that part in which it admits that such judgments can be issued if authorized by Union or Member State law, should be regarded as unlawful.

Keywords: *human dignity, robotic decision, right to non-automated judicial decision-making in criminal matters, Article 11 of Directive (EU) 2016/680, algorithm, machine learning.*

I. Human dignity: An introduction

Human dignity is a multifaceted concept. Such a term comes from the Latin *dignus*. In the legal field, as has happened in other fields, the meaning of the term *dignity* has evolved over time. Initially, its meaning was close to that of *merit* and was associated with a high status in some languages. For example, this is one of the reasons why in the US Declaration of Independence, adopted on 4 July 1776, the term *dignity* is not used.

Therefore, the meaning of the term *human dignity* changes over time. The significant historical evolution of the concept of *human dignity* is reflected in legal semantics. What happened during the Second World War, with unimaginable atrocities against civilian populations, thinking in particular of the Holocaust, brought this concept to the center of the legal debate[1].

---

* PhD, Assistant Professor in Criminal Procedure, University of Padua (Italy), Lecturer in Criminal Procedure, University of Innsbruck (Austria). Contact: silvia.signorato@unipd.it.

[1] A. Barak, *Human dignity as a value and as a right in international documents*. In *Human Dignity: The Constitutional Value and the Constitutional Right*, Cambridge, Cambridge University Press, 2015, pp. 34-48, doi:10.1017/CB09781316106327.005.

There is a need for the protection of human dignity both in times of peace and in times of war[2], and in any situation, including criminal trials.

For this reason, treaties and international documents began to speak explicitly of human dignity. This was an epochal transition.

This happened first with the Preamble of the Charter of the United Nations, signed on 26 June 1945, where faith in the word "dignity" was reaffirmed.

Afterwards, the Universal Declaration of Human Rights proclaimed by the United Nations General Assembly in Paris on 10 December 1948 explicitly mentioned human dignity in the preamble[3] as well as in some articles[4]. In particular, Article 1 provides that «All human beings are born free and equal in dignity and rights. They are endowed with reason and conscience and should act towards one another in a spirit of brotherhood».

At the European Level, the Convention for the Protection of Fundamental Rights and Fundamental Freedoms (better known as the European Convention on Human Rights), which opened for signature in Rome on 4 November 1950 and came into force in 1953, did not mention human dignity. Nevertheless, this fundamental right is frequently recalled in judgements of the European Court of Human Rights (ECHR).

Instead, human dignity is claimed by the Charter of Fundamental Rights of the European Union (Charter), proclaimed on 7 December 2000. The Charter provides for the inviolability of this right. In particular, Article 1 states: «Human dignity is inviolable. It must be respected and protected».

Human dignity is a fundamental right. It gives substance to the rights laid down in the Charter. As early as 2001 the Court of Justice of the European Union (CJEU)[5] made

---

[2] I.C. Paşca, *Drept penal international*, Bucureşti, Universul Juridic, 2020, p. 116.

[3] The Preamble first specifies that the *"recognition of the inherent dignity and of the equal and inalienable rights of all members of the human family is the foundation of freedom, justice and peace in the world, has evolved over the years"*. This Preamble also claims that *"the peoples of the United Nations have in the Charter reaffirmed their faith in fundamental human rights, in the dignity and worth of the human person and in the equal rights of men and women and have determined to promote social progress and better standards of life in larger freedom".*

[4] See Articles 1, 22, and 23.3. Article 22 provides that *"Everyone, as a member of society, has the right to social security and is entitled to realization, through national effort and international cooperation and in accordance with the organization and resources of each State, of the economic, social and cultural rights indispensable for his dignity and the free development of his personality".* Moreover, Article 23.3 provides that *"Everyone who works has the right to just and favourable remuneration ensuring for himself and his family an existence worthy of human dignity, and supplemented, if necessary, by other means of social protection".* The human dignity is also mentioned by: *UN Declaration on the Elimination of All Forms of Racial Discrimination* (20 November 1963), *International Covenant on Civil and Political Rights and the International Covenant on Economic, Social and Cultural Rights* (16 December 1966); *Final Act of the Helsinki Conference on Security and Cooperation in Europe* (1 August 1975); *Convention on the Elimination of All Forms of Discrimination against Women* (18 December 1979); *African Charter on Human and Peoples' Rights* (27 June 1981); *Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment* (10 December 1984); *Convention on the Rights of the Child* (20 November 1989); Protocol No. 13 to *European Convention on Human Rights concerning the abolition of the death penalty in all circumstances* (3 May 2002); *International Convention for the Protection of All Persons from Enforced Disappearance* (20 December 2006); *Convention on the Rights of Persons with Disabilities* (13 December 2006); *Second Optional Protocol to the International Covenant on Civil and Political Rights on the abolition of the death penalty* (15 December 1989); *Optional Protocol to the Convention on the Elimination of All Forms of Discrimination against Women* (6 October 1999); *Council of Europe Convention on Action against Trafficking in Human Beings* (16 May 2005); *Optional Protocol to the Convention on the Rights of the Child on a communications procedure* (19 December 2011); *Optional Protocol to the International Covenant on Economic, Social and Cultural Rights* (10 December 2008).

[5] See CJEU, 9 October 2001, Netherlands vs. Parliament and Council, Case C-377/98, at grounds 70-77.

clear that the right of human dignity is part of Union law. However, the problem remained that the Charter did not have a binding force, being only a source of "soft law"[6].

The Treaty of Lisbon, which was signed on 13 December 2007 and came into force on 1 December 2009, provided that the Charter is a primary law of the Union, therefore assigning to the Charter the same legal status of the Treaties (6.1 TEU). Regarding this fact, Kostoris[7] highlighted: *"this is a crucial step that brought about significant consequences for the general framework of the multilevel protection of fundamental rights. Indeed, the Charter, enjoying now the status of primary EU law, is binding on both secondary EU law and Member States law. In addition, it must be stressed that the Charter not only has codified the fundamental rights that had been recognized exclusively by the case law of the Court of Justice but also includes a list of new rights, such as 'human dignity' (Art. 1 of the Charter)".*

Two consequences arise from the inviolability of human dignity: first of all, no right recognized by the Charter can prejudice the dignity of another person. Furthermore, human dignity cannot be balanced with other rights, because it must always be protected and cannot be limited by other rights.

II. The Kantian categorical imperative as the kernel of human dignity

Human dignity is a fundamental right that guides the interpretation of other rights. This is testified by judgments issued by many national and supranational judges, even if the meaning of dignity varies significantly from jurisdiction to jurisdiction[8].

Nevertheless, some examples can be mentioned.

The United States Supreme Court stated that *"the primary principle is that a punishment must not be so severe as to be degrading to the dignity of human beings"*[9].

The ECHR has established on several occasions that the detention regime must be such as to not violate human dignity[10]. Moreover, this Court ruled that human dignity and human freedom are the "very essence" of the Convention[11].

The CJEU also stated that human dignity imposes certain standards for the reception of applicants for international protection, in particular with regard to material conditions involving housing, food or clothing. The Court specified that a Member State cannot withdraw these standards even temporarily, not even in those cases where the person committed serious breaches of the rules of the accommodation centers or is characterized by seriously violent behavior[12].

These judgements are just a few examples involving the subject of human dignity, but they are more than enough to demonstrate how human dignity is a fundamental right underlying every other right. The fil rouge that connects these judgments seems to be the need to affirm that man can never be considered or treated as a thing.

---

[6] R.E. Kostoris, *The Protection of Fundamental Rights*. In Kostoris R.E. (Ed.) *Handbook of European Criminal Procedure,* Cham, Springer, 2018, p. 72.

[7] *Idem*, p. 73.

[8] C. McCrudden, *Human Dignity and Judicial Interpretation of Human Rights*, in *European Journal of International Law*, Volume 19, Issue 4, September 2008, pp. 655–724, https://doi.org/10.1093/ejil/chn043.

[9] Furman v. Georgia (1972), No. 69-5003.

[10] ECHR, Yaroslav Belousov v. Russia, No 2653/13 and 60980/14, 6 March 2017.

[11] ECHR, Christine Goodwin v. the The United Kingdom, No 28957/95, 11 July 2002.

[12] CJEU, Grand Chamber, 12 November 2019, Zubair Haqbin v. Federaal Agentschap voor de opvang van asielzoekers, Case C-233/18.

After all, any legal system should apply the Kantian categorical imperative, which states that "Handle so, daß du die Menschheit sowohl in deiner Person, als in der Person eines jeden andern jederzeit zugleich als Zweck, niemals bloß als Mittel brauchest" (Act in such a way that you treat humanity, whether in your own person or in the person of any other, never merely as a means to an end, but always at the same time as an end)[13].

III. Information technology and new challenges to human dignity: The case of judicial decision-making

The growing use of information technology (IT) poses new important challenges in terms of respect for fundamental rights and also for human dignity[14].

Technological development made possible the processing of a huge amount of personal data. However, there is the risk that the person is reified and considered a mere set of personal data to be marketed and exploited for the most varied purposes.

As a consequence, the protection of natural persons in relation to the processing of personal data is a fundamental right strictly connected to human dignity.

From a technological point of view, the processing of personal data is based on specific algorithms. In general, an algorithm is a set of instructions for carrying out a procedure or for solving a problem in a finite number of steps[15]. It is important to underline that some artificial intelligence (AI) techniques, in particular *Deep learning,* which is currently undergoing great development, require that the machine learn from data. Therefore, there are some elements of the algorithm actually used in the processing whose values have not been chosen by a programmer, but which are instead the result of automatic learning by the machine (machine learning)[16].

In the legal field, the use of AI algorithms poses significant problems[17]. For this reason, the European Commission for the efficiency of Justice (CEPEJ) tried to provide guidelines by adopting the European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment (Strasbourg, 3-4 December 2018).

AI applied to criminal proceedings and criminal procedures is already a reality in the most diverse fields. For example, there are algorithms that perform profiling of potential offenders or predict where a crime is likely to be committed. From this point of view, it has been noted that the use of algorithms can lead to an increase in proactive investigations[18].

---

[13] I. Kant, *Critik der practischen Vernunft,* 1788, AA IV, 429.

[14] See Z. Bauman, and D. Lyon, *Liquid surveillance: A conversation*. Melden: Polity Press, 2013, VIII – 152, and S. Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power,* New York: PublicAffairs, 2019, pp. 1-691.

[15] See e.g. https://www.merriam-webster.com/dictionary/algorithm.

[16] See M. Kubat, *An introduction to machine learning*, Switzerland, Springer, 2017, pp. 1-339.

[17] See J. Nieva Fenoll, *Inteligencia artificial y proceso judicial*, Madrid, Marcial Pons 2018, pp. 1-168; A. Garapon, J. Lassègue, *Justice digitale. Révolution graphique et rupture anthropologique*, Paris, Puf 2018, pp. 1-368; S. Quattrocolo, *Artificial Intelligence, Computational Modelling and Criminal Proceedings: A Framework for A European Legal Discussion*, Cham Springer, 2020, pp. 1-247; and L.M. Stănilă, *Inteligența artificială și sistemul de justiție penală – Instrumentele de evaluare a riscului penal*, București, Universul Juridic, 2020, pp. 1- 336.

[18] A.G. Ferguson, Predictive Prosecution, *Wake Forest Law Review*, Symposium 2016, Volume 51, May 2016 pp. 705-744, available at SSRN: https://ssrn.com/abstract=2777611, K. Ligeti, Artificial Intelligence and Criminal Justice, *Concepts paper for XX AIDP-IAPL International Congress of Penal Law*, Rome, 13-16 November 2019, p. 9, available at: http://www.penal.org/sites/default/files/Concept%20Paper_AI%20and%20Criminal%20Justice_Ligeti.pdf.

Moreover, other algorithms evaluate the reliability of a witness in a criminal trial. The use of algorithms aimed at assessing potential recidivism risk is currently widespread[19].

There are also algorithms that allow lawyers to reasonably predict what the judgment will be.

The use of algorithms can go even further. A machine can come to serve as a judge by issuing judgments. Robot judges are, for example, being tested in Estonia where they operate only in matters other than Criminal matters and for cases of low value. However, they decide.

At the European level, the use of such algorithms is only apparently prohibited by Directive (EU) 2016/680 (directive on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data), as well as by Regulation (EU) 2016/679 (regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data; cd. General Data Protection Regulation – GDPR).

Regarding the criminal trial, Article 11 of Directive (EU) 2016/680 provides that *"Member States shall provide for a decision based solely on automated data processing, including profiling, which produces an adverse legal effect concerning the data subject or significantly affects him or her, to be prohibited".* Therefore, any robotic decision would appear to be prohibited.

However, the same article establishes a relevant exception. In fact, it provides that the robotic decision is prohibited unless it is authorized by Union or Member State law to which the controller is the subject and which provides appropriate safeguards for the rights and freedoms of the data subject. In particular, at least the right to obtain human intervention on the part of the controller must be safeguarded in all cases.

However, it is necessary to ask ourselves what *"the right to obtain human intervention on the part of the controller"* consists of. The risk to be avoided is that the Judge becomes a mere ratifier of what the algorithm decides, on the basis of the alleged aura of infallibility that connotes IT.

In fact, IT is a human product and, therefore, it is fallible. Both programming and algorithm operating errors may occur. For example, recently two planes and more than 300 lives were lost due to a programming error which, combined with a sensor malfunction, caused the on-board computer to shut down the pilots' commands[20]. Furthermore, the learning process of a machine can lead to errors. It is important to underline that the goal of machine learning is not to obtain a machine that responds exactly in all cases, but a machine that responds correctly almost always based on reasonable requirements, taking into account the fact that a 100% accuracy rate is not achievable.

IV. The difficult relationship between the decision made by a machine and respect for human dignity

At the European level, both Directive (EU) 2016/680 and the GDPR allow exceptions to the prohibition of decision-making based solely on automated data processing,

[19] See e.g. Supreme Court of Wisconsin, State of Wisconsin v. Eric L. Loomis, Case No. 2015AP157-CR, 5 April – 13 July 2016.

[20] R.L. Sumwalt, J. Homendy, B. Landsberg, *Safety Recommendation Report 59582*, National Transportation Safety Bord, Washington, DC 2019, pp. 1-13.

including profiling. However, it is necessary to ask whether, in criminal matters, the exceptions to the prohibition of decision-making based solely on automated data processing are or are not compatible with respect for human dignity.

The problem to be faced is different from that of establishing whether an algorithm (or a set of algorithms) is capable of issuing a reliable judgment or not. This different problem, which was mentioned in § 3, is extremely important, but it is relevant from the point of view of the Right to a fair trial instead.

This question is faced here: Is human dignity violated or not by the fact that it is a machine and not a man who issues the judgement?

It is true that at the European level it is provided that "the right to obtain human intervention on the part of the controller" is respected. However, this does not solve the problem. This can be illustrated by means of an example. Suppose a person is undergoing inhuman or degrading treatment. There would be a clear violation of both the prohibition of torture and human dignity. If that person at a later stage is treated in full compliance of all the rules and rights, the previous violation of the prohibition of torture and of human dignity would not disappear.

Similarly, if the robotic decision involved a violation of human dignity, this violation would not be remedied by any subsequent human intervention.

It is therefore essential to understand whether, in criminal matters, a robotic decision causes a violation of human dignity or not. In my opinion the answer is affirmative.

A machine that issues a judgement on a person actually decides on the basis of current and past digital information. In essence, man is reduced to a set of data, that is, to a thing.

One could object to this reasoning saying that, even in an ordinary trial, the judge decides on the basis of a set of information. However, there is a difference. In the case of the robot judge, the person is reduced to information itself. In the case of the human judge, this is not the case. Even in the case of judgments in absentia, the person is something more than the information available to the judge.

If the robotic decision reduces man to a set of information, it follows that man is treated as a thing. Human dignity instead requires that man must always be considered and treated as a person and never as a thing. For this reason, the robotic decision violates human dignity.

Ultimately, human dignity seems to dictate that every man must be judged by another man. A machine could possibly assist a judge, a prosecutor or an investigator and could pick up on elements that would be difficult for a man to detect, especially in the case where a large amount of data needs to be processed, but any decision in a criminal trial must be made only by a man or a panel of men.

V. Conclusions

Human dignity is inviolable. Its kernel meaning dictates that man can never be reified. A robotic decision, on the other hand, reduces humans to a mere set of data and, therefore, to one thing. For this reason, such a type of decision seems to conflict with human dignity.

It follows that it is possible to doubt the legitimacy of Article 11 of Directive (EU) 2016/680, in the part in which it provides that the robotic decision can be authorized by Union or Member State law.

It is also possible to dispel the unfounded myth of the perfection of algorithms. An algorithm is not perfect, nor can it be. Furthermore, the algorithm does not consider the uniqueness of every human being but brings every man back into standard types. It would be interesting to wonder what the algorithm would decide if a person not attributable to typified categories, such as Beethoven, Einstein, Michelangelo, Leonardo da Vinci, were imputed.

It may also be mentioned that, as part of the update and enhancement of Israel's armored forces, a new tank is planned in which the two crew members are joined by an additional virtual member. This virtual member integrates all current and previous information provided by sensors and maps, as well as historical information that may not be available to the human crew, analyses the situation and, using AI techniques, shows to the crew possible solutions to the tactical problem. The decision to engage the target is only up to the human crew, i.e. the system is of the "man in the loop" type[21]. Anyway, AI in warfare, if not tempered by a "man in the loop" system, is believed to violate several principles, including the principle of human dignity[22].

If the concept of "man in the loop" is so important in war, where the decision time can be very short, is it not possible that it is at least as important in criminal procedure, where the decision time is not as short? AI can be useful to help the Judge reach a decision[23], but the decision must be only up to one or more human beings.

In conclusion, it seems necessary to recognize a new right: the right to non-automated judicial decision-making[24].

References

1. Barak, A., *Human dignity as a value and as a right in international documents,* in *Human Dignity: The Constitutional Value and the Constitutional Right,* Cambridge: Cambridge University Press, 2015, pp. 34-48, doi:10.1017/CB09781316106327.005.

2. Bauman, Z., Lyon D, *Liquid surveillance: A conversation*. Melden: Polity Press, 2013 VIII – 152.

3. Eshel, T., *Israel's Carmel Programme. Charting Future Concepts for Mounted Combat*, European Security & Defense, Volume 2020, Issue 1, February 2020, pp. 90-92.

4. European Commission for the efficiency of Justice (CEPEJ) *European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment*. Strasbourg, 3-4 December 2018.

5. European Parliament, *The ethics of artificial intelligence: Issues and initiatives*. Brussels: European Union, 2020, p. 64, doi: 10.2861/6644.

6. Ferguson, A.G., Predictive Prosecution. *Wake Forest Law Review, Symposium 2016*, Volume 51, May 2016, pp. 705-744, Available at SSRN: https://ssrn.com/abstract=2777611.

[21] T. Eshel, *Israel's Carmel Programme. Charting Future Concepts for Mounted Combat*, European Security & Defense, Volume February 2020, Issue 1, pp. 90-92.

[22] European Parliament, *The ethics of artificial intelligence: Issues and initiatives*, Brussels, European Union 2020, p. 64, doi: 10.2861/6644.

[23] The case of Beijing Internet Court is particularly interesting. Founded on 9 September 2018, Beijing Internet Court mainly deals with the first-instance of specific types of Internet cases within the jurisdiction of Beijing. The use of algorithms is aimed at giving support to the judge in relation only to the formal and procedural aspects. Consequently, the purpose of robots is not to replace humans or to arrive at algorithmic decisions, but to help the judge.

[24] S. Signorato, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Torino, Giappichelli, 2018 pp. 99-103.

7. Garapon, A. - Lassègue, J. *Justice digitale. Révolution graphique et rupture anthropologique*. Paris: Puf, 2018, pp.1-368.

8. Kant, I., *Critik der practischen Vernunft*, 1788, AA IV, 429.

9. Kostoris, R.E., *The Protection of Fundamental Rights*, in Kostoris R.E. (Ed.) *Handbook of European Criminal Procedure.* Cham: Springer, 2018, pp. 72-73.

10. Kubat, M., *An introduction to machine learning*. Switzerland: Springer, 2017, pp. 1-339.

11. Ligeti, K., *Artificial Intelligence and Criminal Justice*, *Concepts paper for XX AIDP-IAPL International Congress of Penal Law,* Rome, 13-16 November 2019*,* p. 9. Available at: http://www.penal.org/sites/default/files/Concept%20Paper_AI%20and%20Criminal%20Justice_Ligeti.pdf.

12. McCrudden, C., *Human Dignity and Judicial Interpretation of Human Rights*, European Journal of International Law, Volume 19, Issue 4, September 2008, pp. 655–724, https://doi.org/10.1093/ejil/chn043.

13. Nieva Fenoll, J., *Inteligencia artificial y proceso judicial*. Madrid: Marcial Pons, 2018, pp. 1-168.

14. Paşca, I.C., *Drept penal international.* Bucureşti: Universul Juridic, 2020, p. 116.

15. Quattrocolo, S., *Artificial Intelligence, Computational Modelling and Criminal Proceedings: A Framework for A European Legal Discussion,* Cham: Springer, 2020, pp. 1-247.

16. Signorato, S., *Le indagini digitali. Profili strutturali di una metamorfosi investigative*, Torino: Giappichelli, 2018, pp. 99-103.

17. Stănilă L.M., *Inteligenţa artificială şi sistemul de justiţie penală – Instrumentele de evaluare a riscului penal.* Bucureşti: Universul Juridic, 2020, pp. 1- 336.

18. Sumwalt R.L., Homendy J., Landsberg B., *Safety Recommendation Report 59582, National Transportation Safety Board*. Washington, DC, 2019, pp. 1-13.

19. Zuboff, S., *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power,* New York: PublicAffairs, 2019, pp. 1-691.

New Species of Criminal Phenomena: Organized Cybercrime

Laura Stanila*

Abstract

ICT (Information and Communication Technology) has spread to all dimensions of social life, including criminal phenomenon. Organized crime, as a rising type of crime, has gained new forms of manifestation since the members of criminal groups use ICT tools to commit crimes or moved to virtual space as this space offers them the ideal "work-field" providing anonymity, a large number of victims, and huge sources of profit.

In fact, the organized cybercriminal groups have become one of the most ascending criminal groups, very difficult to discover and combat.

In the present study, the author offers a presentation of cybercrime in its organized form, presents the cybercriminal groups, their types and characteristics and the types of cybercrimes that are to be committed by an organized criminal group online and offline.

Keywords: *cybercrime, organized crime, organized criminal group, organized cybercrime, cybercriminal group*

I. The Newest Challenge for the Criminal Investigators. Social context

In the recent years everyone may notice an increasing addiction of the society to technology, especially to ICT (Information and Communication Technology). This addiction turned dramatic as it has extended in the "criminal" area with criminals becoming specialized in committing online crimes and in using AI (artificial intelligence) as an important tool to achieve illegal goals. Organized crime was itself a devastating plague of the contemporary society, very difficult to discover, investigate and combat, but the new social realities seem to make it even more dangerous and even more difficult to fight with. Digital networks seem the perfect playground for criminals taking advantage of their features and advantages: privacy, secrecy, velocity, the possibility for dissimulation. Due to these features, the criminal goal is easier to achieve, while *modus operandi* is changed and adapted to the digitalization of the society. The result of this tendency is a sad one: a new type of organized crime – organized cybercrime.

As general Director of the FBI had stated *"transnational crime groups, sexual predators, fraudsters, and terrorists are all transforming the way they do business as technology evolves. Huge swaths of these crimes have a digital component or occur almost entirely online. And new technical trends are making the investigative environment a lot more complex"*[1].

---

* PhD, Associate Professor, West University of Timișoara (Romania). Contact: laura.stanila@e-uvt.ro.

[1] C. Wray, Director of Federal Bureau of Investigation (FBI), *Digital Transformation: Using Innovation to Combat the Cyber Threat*, Speech at the Boston College/FBI – Boston Conference on Cyber Security, March 7, 2018, https://www.fbi.gov/news/speeches/digital-transformation-using-innovation-to-combat-the-cyber-threat, accessed on 2.11.2020.

II. What is cybercrime? What is organized cybercrime? Distinctions

Cybercrime has evolved in parallel with society's use of digital networks, reacting to every development in legal sector with new approaches to committing offenses[2]. Scholars have noticed that, in the past decade, cybercrime has transformed itself from fragmented acts committed by individuals to increasingly sophisticated and highly professionalized activity[3].

It is obvious we are facing a new type of organized criminal groups operating solely in the cyberspace, tending to expand their activity at a global level.

From the very beginning one should notice that nowadays several terms and expressions are used in relation with the notion of crime in cyberspace and the notion of organization of crime. For example, would it be accurate to refer to organized cybercrime as organized crime in cyberspace? Or do these notions differ?

The answer key to this question is the cyberspace.

a) If we consider cyberspace as a medium for "traditional organized crime", a space where organized crime carries out its activity, then organized cybercrime is in fact a subdivision, a special type of organized crime.

In this case, the structure, purpose and operations of organized crime are the same in the case of organized cybercrime, while the area of carrying out criminal operations, the IT specializations of the members of the organized criminal group and a specific modus operandi implying specific techniques and methods (e.g. phishing, botnet trade) are features characterizing organized crime in cyberspace.

b) If we consider cyberspace as an enabler for organized crime, then organized cybercrime becomes a new distinct type of crime, which shares few features with traditional organized crime.

The debate on this distinction is not new. Actually, in the early 2000s, there were scholars affirming organized crime and cybercrime could not be one and the same because organized crime would be operated offline while most cybercrimes would be committed by individuals rather than organized groups[4]. Williams even identified five possible trends in the evolution of organized crime in the era of digitalization:

1. the use of the Internet for major fraud and theft activities by the organized crime groups;

2. the increased opportunities for profit stemming from the growth of electronic banking and electronic commerce for organized crime.

3.the growth of cyberextortion using complex extortion schemes, conducted anonymously and incurring modest risks, very efficient in money outputs.

4. the use of "nuisance tools", such as computer viruses, for more openly criminal activities.

5. jurisdictional arbitrage – cybercrimes will be committed by organized criminal groups in jurisdictions with poor legal framework and little capacity to enforce laws against cybercrime.

---

[2] T. Tropina, *The evolving structure of online criminality. How cybercrime is getting organized*, Eucrim, The European Criminal Law Associations' Forum, issue 4/2012, p. 158.

[3] *Idem*.

[4] P. Williams, *Organized Crime and Cybercrime: Synergies, Trends, and Responses*, Global Issues, Volume: 6, Issue: 2, August 2001, pp. 22-26, https://www.ncjrs.gov/App/Publications/abstract.aspx?ID=191389, accessed on 2.11.2020.

6. the increased use of the Internet for money laundering, as being a medium through which international trade takes place. Online auctions and online gambling offer similar opportunities to launder money through apparently legitimate purchases, and then lose the "clean" money through offshore financial centers. In addition, *"as e-money and electronic banking become more widespread, the opportunities to conceal the movement of the proceeds of crime in an increasing pool of illegal transactions are also likely to grow"*[5].

7. growing network connections between hackers or small-time criminals and organized crime. Network connections between the two kinds of groups are likely to deepen and widen.

Referring to all trends, it is worth to mention organized crime groups use the Internet for communications (usually encrypted) and for other purposes. Organized crime is proving as flexible and adaptable in its exploitation of cyber-opportunities as it is in any other opportunities for illegal activity.

These thoughts were expressed 18 years before and they appear accurate in the contemporary context.

In 2017 a study was conducted to investigate to what extent cybercriminals operating in phishing and malware attacks can be conceptualized as organized criminal groups. To answer this question, the authors analyzed 40 criminal networks investigated in four countries (Netherlands, UK, USA and Germany) and analyzed them through an organized crime analytical framework. The empirical analysis indicates that even if the criminal networks considered display the minimum set of characteristics to consider them as organized crime, if someone looks only at their structure and composition, they mostly fail to meet the existing definitions of organized crime when it comes to the characteristics of criminal activities carried out and social functions of these networks[6].

As a result of the study, the authors identified 39 networks and classified them into four types:

1. Completely through offline social contacts;
2. Offline social contacts as a base and online forums to recruit specialists;
3. Online forums as a base and offline social contacts to recruit local criminals;
4. Completely through online forums.

The analysis revealed specific features of traditional organized crime, such as use of Violence and Corruption and connections with the Legal Economy. Still, it was very difficult to declare cybercriminals operating in phishing and malware attacks, which were indeed acting in networks, as organized criminal groups.

Tropina distinguishes between two different phenomena, namely, migration of traditional organized crime in cyberspace and organized groups focused on committing cybercrimes[7]:

a) migration of traditional organized crime in cyberspace

The Internet has become a tool for facilitating all types of offline organized criminality (child abuse, drug trafficking, trafficking in human beings for sexual exploitation, illegal migration, different types of fraud, and counterfeiting) due to increased anonymity, money laundering schemes and possibilities of advertising.

---

[5] *Idem*.

[6] E.R. Leukfeldt, A. Lavorgna, E.R. Kleemans, *Organised Cybercrime or Cybercrime that is Organised? An Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime, European Journal of Criminal Policy Res* 23, 2017, pp. 287–300, https://doi.org/10.1007/s10610-016-9332-z, accessed on 2.11.2020.

[7] T. Tropina, *cited,* p. 159.

b)organized groups focused on committing cybercrimes.

This is a new form of organized crime characterized as organized structures operating solely in global information networks and committing only cybercrimes. This new type of organized crime is also characterized by different, constantly evolving structures and new ways of using hi-tech tools in order to obtain illegal profits.

These two types of organized crime coexist, with an increasing ascension of the latter.

The global security strategist and expert Marc Goodman, in an interview in 2015 said that the old image of a hacker was that of a "*17-year-old kids living in their parents' basements. Today, the average age of a cybercriminal is 35, and 80% of black-hat (e.g., criminal) hackers are affiliated with organized crime. (...) In other words, people are choosing this as a profession. (...)That's a radical shift, and it's led to the creation of increasingly sophisticated criminal organizations that operate with the professionalism, discipline, and structure of legitimate enterprises"*[8].

In order to illustrate the importance of the topic, we exemplify with a criminal organization known as Innovative Marketing that created a malware program it disguised as antivirus software. Using its crimeware tool to hijack Internet users' Web browsers, Innovative Marketing deceived hundreds of thousands of people into disclosing their credit card numbers and buying its fake antivirus software. This criminal enterprise operated for three years before being shut down by the FBI and Interpol, both of which calculated its fraudulent sales of malicious software at over 100 million dollars. Innovative Marketing maintained a headquarters in a three-story office building in the Ukraine and even had an org chart with a CEO, CFO, CIO, and head of HR. HR was responsible for hiring mules and bringing criminals into the organization. The CIO was responsible for the dark Web infrastructure that enabled the company to operate clandestinely on the Internet. Innovative Marketing also had a quality assurance team that tested its malicious code against over 200 legitimate antivirus programs before releasing it. At its height, the "company" had more than 600 employees and operated in more than 60 countries[9].

III. Types of organized cybercrime groups

In 2012, it was stated that about 80% of cybercrime could be the result of some form of organized activity[10].

The scholars have identified six basic organizational patterns of cybercrime, however noted that the typology of organized cybercrime groups is likely to change as the digital environment evolves[11].

---

[8] The Wall Street Journal, *Security Expert Marc Goodman on Cyber Crime*, May 12, 2015, https://deloitte.wsj.com/cio/2015/05/12/security-expert-marc-goodman-on-cyber-crime/, accessed on 2.11.2020.

[9] US Attorney's Office, *Northern District of Illinois, U.S. Indicts Ohio Man and Two Foreign Residents in Alleged Ukraine-Based "Scareware" Fraud Scheme That Caused $100 Million in Losses to Internet Victims Worldwide*, May 27, 2010, https://archives.fbi.gov/archives/chicago/press-releases/2010/cg052710-1.htm, accessed on 2.11.2020.

[10] M. McGuire, *Organised Crime in the Digital Age*, London, John Grieve Centre for Policing and Security, 2012.

[11] Idem. Also see M. Mazela, *Organizational structures of cybercrime groups: Overview of key characteristics*, European Cybersecurity Market, Volume 2, Issue 3-4, 2018, pp.18-23.

a) Type I groups operate solely online, being mostly "virtual" while trust is assessed via reputation in online illicit activities. This category includes two subtypes: swarms and hubs[12].

a.1. Swarms appear as "disorganized organizations with common purpose and without leadership". They are types of networks and have minimal chains of command, acting essentially online. Sworms *"may operate in viral forms in ways reminiscent of earlier 'hacktivist' groups"*[13]. They are most active in ideologically driven online activities (e.g. hate crimes, political resistance). The group Anonymous illustrates a typical swarm-type group[14].

a.2. Hubs are essentially active online also, however they have a command structure, being more organized than swarms. They involve a focal point (hub) of core criminals around which peripheral associates gather. Their activities are very diverse – phishing attacks, botnets, online sexual offending etc., all of them happening online. An example of hub-type cybercriminal group is Silk Road 2.0[15], which is an online market trading in illicit goods such as drugs.

b) Type II groups operate both online and offline and are described as "hybrids". This category could be also divided into two subtypes: clustered hybrids and extended hybrids.

b.1. the *clustered hybrid* is characterized by criminal acts committed by a small group of individuals using specific activities or methods. Clustered hybrids resemble with hubs in their structure, but oscillate between online and offline criminal acts. Their activities are driven by profit. An example of a sophisticated cybercriminal hub/ clustered hybrid and its organization was presented by Chabinsky, a representative of the US Federal Bureau of Investigation's Cyber Division, during his speech[16]: *"Coders create malware, exploits, and other tools necessary to commit the crime. Distributors trade/sell stolen data and vouch for the goods provided by the other specialties.*

---

[12] R. Broadhurst, P. Grabosky, M. Alazab, S. Chon, *Organizations and Cyber crime: An Analysis of the Nature of Groups engaged in Cyber Crime*, International Journal of Cyber Criminology, Vol 8, Issue 1, January – June 2014, p. 7.

[13] P.Olson, *We Are Anonymous: Inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency,* London: Little, Brown, 2012.

[14]*Anonymous* is a network of thousands of activists, a minority of them hackers, devoted to leftist-libertarian ideals of personal freedom and opposed to the consolidation of corporate and government power. *See* Dale Beran, The Return of Anonymous. The infamous hacker group reemerges from the shadows, The Atlantic, August 11, 2020, https://www.theatlantic.com/technology/ archive/2020/08/hacker-group-anonymous-returns/615058/, accessed on 3.11.2020.

[15] *Silk Road 2.0* is an underground website, lauched in 2013 and owned by Blake Benthall, aka "Defcon", being one of the most extensive, sophisticated, and widely used criminal marketplaces on the Internet today. The website has operated on the "Tor" network, a special network of computers on the Internet, distributed around the world, designed to conceal the true IP addresses of the computers on the network and thereby the identities of the network's users. Since its launch in November 2013, Silk Road 2.0 has been used by thousands of drug dealers and other unlawful vendors to distribute hundreds of kilograms of illegal drugs and other illicit goods and services to buyers throughout the world, as well as to launder millions of dollars generated by these unlawful transactions. As of September 2014, Silk Road 2.0 was generating sales of at least approximately $8 million per month and had approximately 150,000 active users. *See* J. Cook, *FBI Arrests Former SpaceX Employee, Alleging He Ran The 'Deep Web' Drug Marketplace Silk Road 2.0*, Business Insider, November 6, 2014, https://www.businessinsider.com/ fbi-silk-road-seized-arrests-2014-11, accessed on 3.11.2020.

[16] S. Chabinsky, *The Cyber Threat: Who's Doing What to Whom?* Federal Bureau of Investigation, 2010, Retrieved from https://archives.fbi.gov/ archives/news/speeches/the-cyber-threat-whos-doing-what-to-whom, accessed 5.11.2020.

Technicians maintain the criminal infrastructure and supporting technologies. Hackers search for and exploit vulnerabilities in applications, systems, and net- works in order to gain administrator or payroll access. Fraud specialists develop and employ social engineering schemes, including phishing, spamming, and domain squatting. Hosts provide "safe" facilities of illicit content servers and sites. Cashers control drop accounts and provide those names and accounts to other criminals for a fee; they also typically manage individual cash couriers, or "money mules." Money mules transfer the proceeds of frauds which they have committed to a third party for further transfer to a secure location. Tellers assist in transferring and laundering illicit proceeds through digital currency ser- vices and between different national currencies. Executives of the organization select the targets, and recruit and assign members to the above tasks, in addition to managing the distribution of criminal proceeds."

b.2. *extended hybrids* act similarly to clustered hybrids but are less centralized. They typically include many associates and subgroups and carry out a variety of criminal activities, but still retain a level of coordination sufficient to ensure the success of their operations. The level of coordination is based on the complexity of the operation. Their activities are also driven by profit.

c) Type III groups operate offline but use online technology and cyberspace to run their offline activities. They are increasingly contributing to digital crime and can be subdivided into "hierarchies" and "aggregates", due to their degree of organization and cohesion.

c.1. *Hierarchies* are traditional organized criminal groups which export some of their activities online, using the Internet to support/expand their offline activities. Examples include online gambling, blackmail, extortion, prostitution moved online (pornography, webcams) etc.

c.2. *Aggregates* are superficially organized, temporary, and often without clear purpose groups. They use digital technologies ad hoc. E.g. the use of Blackberry Messenger to coordinate public disorder during the 2011 UK riots[17]. The Sydney riots in September 2012[18] were conducted in the same way.

Also, organized cybercrime group could be classified regarding the purpose criteria in other two subtypes[19]:

a) enterprise or profit-oriented activities, and especially cybercrime committed by state actors, appear to require leadership, structure, and specialization.

b) protest activity tends to be less organized, with weak (if any) chain of command.

IV. Features of the organized cybercrime groups

The doctrine has noted that half of the cybercrime groups in his sample comprised six or more people, with one-quarter of groups comprising over 10 individuals. One-quarter of cybercrime groups had operated for less than 6 months. However, the size

[17] J. Halliday, *London riots: BlackBerry to help police probe Messenger looting 'role'*, The Guardian, August 8, 2011, retrieved from https://www.theguardian.com/uk/2011/aug/08/london-riots-blackberry-messenger-looting, accessed 5.11.2020.

[18] ABC News, *As it happened: Violence erupts in Sydney over anti-Islam film*, September 15, 2012, retrieved from https://www.abc.net.au/news/2012-09-15/anti-us-protests-hit-sydney/4263372, accessed 5.11.2020.

[19] R. Broadhurst et all., cited, p. 1.

of the group or the duration of their activities did not predict the scale of offending, as small groups can cause significant damage in a short time[20]. The scholars also noted a substantial functional specialization and divisions of labor as specific features of the organized cybergroups.

In fact, the main features identified by the doctrine for the organized cybercrime groups and the activity of their members are[21]:

- Coders or programmers write the malware, exploits, and other tools necessary to commit the crime.
- Distributors or vendors trade and sell stolen data, while vouch for the goods provided by the other specialties.
- Technicians maintain the criminal infrastructure and supporting technologies, such as servers, ISPs, and encryption.
- Hackers search for and exploit vulnerabilities in applications, systems, and networks in order to gain administrator or payroll access.
- Fraud specialists develop and employ social engineering schemes, including phishing, spamming, and domain squatting.
- Hosts provide "safe" facilities of illicit content servers and sites, often through elaborate botnet and proxy networks.
- Cashers control drop accounts and provide those names and accounts to other criminals for a fee; they also typically manage individual cash couriers, or "money mules."
- Money mules transfer the proceeds of frauds which they have committed to a third party for further transfer to a secure location.
- Tellers assist in transferring and laundering illicit proceeds through digital currency services and between different national currencies.
- Executives of the organization select the targets, and recruit and assign members to the above tasks, in addition to managing the distribution of criminal proceeds.

This ideal type is not necessarily limited to a formal, fixed organization. Some functions may be outsourced. The organization of cybercrime may also occur at a wider level involving networks of individuals who meet and interact within online discussion forums and chat rooms, some of them functioning as virtual black markets that advertise illicit goods or services.

According to Wall[22] cybercriminal groups share at least one of the following features:

- structure
- members have specific skill sets
- members exercise different responsibilities within the group;
- members are involved in the activity of two or more groups simultaneously;
- members worked with the same group on a regular basis, but on different occasions;
- members act together to commit the same type of crime, or share interests and/or common goals;
- members are self-contained;

---

[20] M. McGuire, cited.

[21] S. R. Chabinsky, *The Cyber Threat: Who's Doing What to Whom?* FBI, 2010, March 23, retrieved on 15th December 2013 from http://www.fbi.gov/news/speeches/the-cyber-threat-whos-doing-what-to-whom.

[22] D. Wall, *Dis-Organised Crime: Towards a Distributed Model of the Organization of Cybercrime*, The European Review of Organised Crime, 2(2), 2015, pp. 71-90.

- members usually driven by an individual or a very small group;
- adaptability – members are very reactive in response to circumstances;
- members are bound together by reputational economy.

According to Leukfeldt, Lavorgna and Kleemans[23] the cybercrime groups share the following features:

- there is no strict hierarchical structure per se.
- dependency relationships between their members
- different functional roles of their members
- three different structural layers: core members (stable group which commit crimes with the same team for a period of time, however, sometimes they simultaneously work with criminals from other groupings), enablers and money mules. In the absence of core members, cybercrime groups use online forums to identify and select suitable co-offenders. In these cases, the members of cybercrime groups have technical expertise, are active on online criminal forums and work together occasionally.
- the groups' structure is based on offline social contacts;
- offline social contacts are used to create the team of core members while online forums were used to recruit specialists.

The doctrine tried to classify the cybercrime groups in the following categories[24]:

- large size groups (more than 21 members)
- medium size groups (5–10 members) which are the most common.
- groups with 11–20 members
- small size groups (2–4 members)

A more complex classification of Cybercrime groups is presented in the Comprehensive Study on Cybercrime of UNDOC – United Nations Office on Drugs and Crime in 2013[25]: groups with 2 members, groups with 3-5 members, groups with 6-10 members, groups with 11-20 members, groups with over 20 members.

It is worth to mention that typology of cybercrime groups is continuously evolving, making it very difficult to identify and combat. The judicial bodies must monitor and analyze each group, focusing on the following elements[26]:

- size of the group;
- strength of association between the members;
- environment where the group operates;
- tools the group uses;
- group's financial resources;
- profile of the victim;
- members' responsibilities;
- hierarchy within the group;
- group's goal;
- using 'crime as a service';

---

[23] E.Leukfeldt, A.Lavorgna, E. Kleemans, *Organised Cybercrime or Cybercrime that is Organised? An Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime*, *European Journal on Criminal Policy and Research*, 23(3), 2016, pp.287-300.

[24] M. Mazela, cited, p. 22.

[25] Malby et. all, cited, p. 48; *Comprehensive Study on Cybercrime of UNDOC – United Nations Office on Drugs and Crime* p. 3.

[26] Malby, cited, p. 23.

- reactiveness in response to circumstances;
- importance of reputational economy;
- working with multiple groups at the same time;
- time frame of the cooperation;
- social relationships between the members.

V. Priorities of Europol: Organized Cybercrime

In its 2019 Internet Organized Crime Threat Assessment Report – IOCTA[27], Europol's European Cybercrime Centre (EC3) provides key recommendations to law enforcement, policy makers and regulators to allow them to respond to cybercrime in an effective and concerted manner. The IOCTA Report focuses on cybercrime priorities, which are determined by the EU Policy Cycle – EMPACT, are currently: Cyber-dependent crime, online child sexual exploitation and payment fraud. Further, the preoccupation of the EUROPOL also focuses on the criminal abuse of the dark web, the convergence of cyber and terrorism and on cross-cutting crime factors.

a) Cyber-dependent crime

While ransomware remains the top threat in this report, the overall volume of ransomware attacks has declined as attackers focus on fewer but more profitable targets and greater economic damage. Also, the report speaks about *phishing* and *vulnerable remote desktop protocols (RDPs)* being the key primary malware infection vectors. In addition data remains a key target, commodity and enabler for cybercrime. Following the increase of destructive ransomware, such as the German wiper attacks of 2019, the report states there is a growing concern within organizations over attacks of sabotage making continuous efforts needed to further synergize the network and information security sector and the cyber law enforcement authorities improving the overall cyber resilience and cybersecurity.

b) online child sexual exploitation

The 2019 IOCTA Report states the amount of child sexual exploitation detected online by law enforcement and the private sector had continued to increase, putting considerable strain on law enforcement resources. There is an increased online solicitation of children for sexual purposes with a largely unchanged modus operandi, facilitated by growing access of minors to high quality smartphones and a lack of awareness of the risks.

c) payment fraud

Skimming continues to evolve with criminals continuously adapting to new security measures while jackpotting attacks are becoming more accessible and successful.

d) criminal abuse of the dark web

The dark web remains the key online enabler for trade in an extensive range of criminal products and services and a priority threat for law enforcement. The coordinated law enforcement activities, combined with extensive Distributed Denial of Service (DDoS) attacks have generated distrust in The onion router (Tor) environment. There is strong evidence administrators are exploring alternatives, but a full

[27] EUROPOL, *Internet Organized Crime Threat Assessment 2019* (IOCTA 2019), https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2019, accessed on 5.11.2020.

migration to new platforms is unlikely just yet, due to the user-friendliness, existing market variety and customer-base on Tor. Some organized crime groups are also fragmenting their business over a range of online marketplaces, while encrypted communication applications enhance single-vendor trade on the dark web, helping direct users to illegal services and enabling closed communications.

e) the convergence of cyber and terrorism

Terrorist groups adopt new technologies, exploit emerging platforms for their online communication and distribution strategies and other online service providers also. Online medium offers perfect conditions for planning and recruiting new members, terrorist attacks can rapidly turn viral, making law enforcement difficult to quickly respond.

f) cross-cutting crime factors

Phishing remains an important tool in the arsenal of cybercriminals for both cyber-dependent crime and non-cash payment fraud, while cryptocurrencies continue to facilitate cybercrime.

Previously, in 2010, the EU set up a four-year policy cycle in order to create a greater measure of continuity for the fight against serious international and organized crime. EU Policy Cycle – EMPACT priorities for the fight against organized and serious international crime between 2018 and 2021 were adopted by the Council of the EU at its meeting on 18 May 2017, and among them stands the fight against cybercrime. In order to achieve this goal, several directions were established[28]:

a. disrupting the criminal activities related to attacks against information systems, particularly those following a Crime-as-a-Service business model and working as enablers for online crime;
b. combating child sexual abuse and child sexual exploitation, including the production and dissemination of child abuse material, *and*
c. targeting criminals involved in fraud and counterfeiting of non-cash means of payment, including large-scale payment card fraud (especially card-not-present fraud), emerging threats to other non-cash means of payment and enabling criminal activities.

Europol's European Cybercrime Centre (EC3) defines cyber-dependent crime as *"any crime that can only be committed using computers, computer networks or other forms of information communication technology (ICT)".*

The 2019 Europol Report reveals the top European cybercrime treats, trends and areas for law enforcement improvement.

Finally, Internet Organized Crime Threat Assessment Report – IOCTA 2020[29] has emphasized a new cross-cutting crime facilitator – COVID 19 pandemic: *"the outbreak of COVID-19 has demonstrated the unfortunate impact potential of such crises on our daily lives across the globe. As physical lockdowns became the norm, cybercrime became more popular than before. There is no denying that the arrival of COVID-19 was a crucial factor in any development discussed with respect to 2020. However, COVID-19 in connection to cybercrime needs to be placed within its context. If anything, COVID-19 demonstrated how cybercrime – at its core – remains largely the same but criminals*

[28] Europol – EU Policy Cycle – EMPACT, https://www.europol.europa.eu/crime-areas-and-trends/eu-policy-cycle-empact, accessed on 6.06.2020.

[29] Europol, *Internet Organized Crime Threat Assessment 2020* (IOCTA), https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020, accessed on 5.11.2020.

change the narrative. They adapt the specifics of their approach to fit the societal context as a means to enhance their rate of success."[30] At the same time, the pandemic *"also gave rise to disinformation campaigns and activities. Disinformation efforts are often associated with hybrid threats, which are defined as threats combining conventional and unconventional, military and non-military activities which may be used by non-state or state actors to achieve political aims. A wide range of measures applied in hybrid campaigns include cyber-attacks and disinformation, disruption of critical services, undermining of public trust in governmental institutions and exploiting social vulnerabilities. The presence of disinformation became a crucial feature in the overall threat landscape during the crisis"*[31].

V. Types of tools and methods used by organized cybercrime groups

Organized cybercrime uses specific tools and methods applied by specialized members who act mainly online. The most common of these tools and methods were reported the following[32]:

a) Ransomware

Ransomware maintained as the top cyber threat in Europe in the 2019 and 2018. The primary methods used by malicious cyber actors to compromise networks include social engineering and highly targeted phishing emails (*spear-phishing*), the use of vulnerable remote desktop protocols (RDPs) – either through hacking or buying access to the network through a criminal forum and destructive cyber acts of sabotage, designed to cause permanent destruction of the victim's data, such as the *GermanWiper*[33] malware which surfaced in 2019.

b) Data compromise

Data compromise refers to illegally obtained financial or personal data through means such as malware or phishing. After ransomware, the compromise of data represents the second most prominent cyber threat in Europe. This data may be used directly to commit fraud or sold to other criminals on the dark web. Whilst compromised financial data may allow for immediate financial gains by cyber criminals, personal data may be used to enable targeted attacks such as spear-phishing or Business Email Compromise (BEC) fraud, which in the longer term may yield more significant criminal proceeds.

There is also a growing threat of malicious insider activity in compromising data, where the insider works directly for a company or for a third-party service provider.

---

[30] IOCTA 2020 p. 13.

[31] IOCTA 2020 p. 13.

[32] N.G. Miralis, *What were the greatest organised cybercrime threats in 2019?*, Lexology, February 14, 2020, https://www.lexology.com/library/detail.aspx?g=8ca91844-7c49-4542-9a7a-f78530b616dc, accessed on 5.11.2020.

[33] *GermanWiper* was a ransomware which didn't encrypt files but instead it rewrote their content with zeroes, permanently destroying users' data. As a result, any users who got infected by this ransomware should have been aware that paying the ransom demand would not helped them recover their files. Unless users had had created offline backups of their data, their files were gone and unrecoverable. *See* C. Cimpanu, *GermanWiper ransomware hits Germany hard, destroys files, asks for ransom*, ZD Net, 2 August 2019, retrieved from

https://www.zdnet.com/article/germanwiper-ransomware-hits-germany-hard-destroys-files-asks- for-ransom/, acessed on 10.03.2020.

c) DDoS attacks

Distributed Denial of Service (DDoS) attacks occur where multiple compromised systems work together to deny others access to an entity's data or services, critically disrupting the operations of an organization. DDoS attacks were identified as the third most significant threat in the Report. Whilst attacks were most commonly motivated by financial gain through extortion, other attacks were of an ideological/political nature or purely malicious.

d) Attacks on critical infrastructure

These attacks may involve the use of some of the previously covered attack tools such as DDoS, however they are distinguished by the primary motive focusing on attacking the infrastructure itself and disrupting its functions.

e) Website defacement

The number of website defacement cases still requires the allocation of limited law enforcement resources. Investigation of these offences may help to catch potential future cybercriminals testing out their capabilities and prevent them from developing a career in cyber crime.

f) Lower priority threats

This category includes data stealing malware, cryptomining by exploiting a victim's processing power without their permission to mine cryptocurrencies and mobile malware.

g) Future threats and developments

In the future there will likely be a growth in supply chain attacks, financially motivated cybercrime focused on cryptocurrency assets and significant ongoing risk to the Domain Name System (DNS) infrastructure allowing malicious actors to see data in transit, redirecting traffic or spoofing[34] specific websites.

VI. Types of cybercrime committed by organized groups

Cybercrime was defined as computer-related crime, its development being closely related and influenced by the global connectivity. Cybercrime activities are characterized by the use of globalized information communication technology (ICT) for committing criminal acts. Another important feature is its transnational spread and its transnational outcome.

Still, some scholars[35] do not use the term "computer crime" because its narrowness, using instead only the term "cybercrime", the prefix "cyber" emphasizing that both computers *and* the Internet are inextricably linked with the crime. Thus Cybercrime is defined as *"criminal acts committed using electronic communication networks and information systems or against such networks and systems"*[36]. Based on this definition, cybercrimes can be distinguished as:

1. target cybercrimes: crimes in which a computer is the target of the offense; and
2. tool cybercrimes: crimes in which a computer is used to facilitate a traditional crime.

---

[34] *Spoofing* a website means creating a website as a hoax, with the intention of misleading readers that the website has been created by a different person or organization.

[35] J.-J.Oerlemans, *Investigating Cybercrime*, Thesis, SIKS – The Dutch Research School for Information and Knowledge Systems, Amsterdam University Press, 2017, p. 20, DOI: 10.13140/RG.2.2.19060.55686.

[36] *Ibidem*.

The scholars have tried to identify the types of cybercrime committed by organized groups, even if there is lack of a general definition of cybercrime itself[37].

a) Acts against the confidentiality, integrity and availability of computer data or systems, including:
   - Illegal access to a computer system;
   - Illegal access, interception or acquisition of computer data;
   - Illegal interference with a computer system or computer data;
   - Production, distribution or possession of computer misuse tools
   - Breach of privacy or data protection measures;

b) Computer-related acts for personal or financial gain or harm, including:
   - Computer-related fraud or forgery;
   - Computer-related identity offences;
   - Computer-related copyright or trademark offences;
   - Sending or controlling sending of Spam;
   - Computer-related acts causing personal harm;
   - Computer-related solicitation or 'grooming' of children;

c) Computer content-related acts, including
   - Computer-related acts involving hate speech;
   - Computer-related production, distribution or possession of child pornography;
   - Computer-related acts in support of terrorism offences;

However, this list is not exhaustive and could be detailed, including in the first category the following[38]: *illegal access to a computer system; illegal access, interception or acquisition of computer data;illegal data interference or system interference; production, distribution, or possession of computer misuse tools; breach of privacy or data protection measures*; *computer-related fraud or forgery;computer-related identity offences; computer-related copyright and trademark offences; sending or controlling sending of spam; computer-related acts causing personal harm; computer-related acts involving racism or xenophobia; computer-related production, distribution, or possession of child pornography; computer-related solicitation or 'grooming' of children; computer-related acts in support of terrorism offences.*

VII. Predictions on cybercrime

The so called "crime's movement into cyberspace" affected the structure of organized criminal activity. Cyberspace frees individuals from many of the constraints that apply to activities in the real world, thus many forms of criminal organizations have made the transition to online crime. In the cyberworld, acts and processes are mostly automated, real-world physical force being unlikely to play a significant role in online criminal activities. As Brenner stated, "situational concentrations of effort are far more easily achieved in cyberspace than in the real world. Activity in cyberspace is not constrained by geography or other temporal limitations. Indeed, even time is less of a constraint in cyberspace, where processes can be automated and monitored only sporadically". At the same time, hierarchical structure of a traditional organized criminal group evolved to allow criminal groups to carry out large-scale, complicated

[37] Malby et. all, cited, p. 16.
[38] Malby et. all, cited, *Annex 1 – Act descriptions*, p. 257-258.

entrepreneurial activities both in the real world and cyberspace. However, in cyberspace, the rigid hierarchical structures of traditional organized criminal groups do not fit, since online criminal activity emphasizes lateral relationships and networks instead of hierarchies. Swarms, hubs or hybrid organizational models of cybercrime groups prove to be more adaptable, yet very difficult to identify and combat by judicial bodies. The cybercrime groups may constitute and act ad hoc, only for a short period of time and to complete a specific criminal activity, making them very difficult to include in the traditional organized criminal group, since their features do not fit the features of the latter.

As the doctrine pointed out, "in the real-world, the stability and consistency of organized criminal groups gives law enforcement a fixed target upon which to focus its efforts. Police concentrate on identifying a permanent group of participants who engage in a set of routine illicit activities. This predictability, in itself, enhances law enforcement's ability to combat organized crime making police to lose this advantage, which will only contribute to the success of organized cybercrime"[39].

The efforts and struggle of the judicial bodies in their fight with this new type of organized crime is once more emphasized by the Director of FBI in 2018: "As cyber threats evolve, we need to evolve as well. This means evolving both our day-to-day operational strategies and our broader approach to handling global digital challenges. To combat these blended threats and worldwide computer intrusions, we can no longer just investigate individual parts of a criminal scheme occurring in one jurisdiction. We need to focus our efforts on dismantling the entire cyber enterprise. We're prosecuting the actors, burning their infrastructure, and seizing their illicit proceeds. We're taking down the groups running malware campaigns and the criminals who support them—those who operate the dark markets, compromise networks and servers, and the people who buy and sell stolen data. Think of it as going after the distribution ring and the manufacturer rather than simply taking out the drug dealer on the corner. And we need to have a global perspective. We need to delegate roles and responsibilities across multiple field offices and to international partners—so that we can share information in real time, as we target and dismantle the most significant cyber enterprises"[40].

References

1. ABC News, *As it happened: Violence erupts in Sydney over anti-Islam film*, September 15, 2012, retrieved from https://www.abc.net.au/news/2012-09-15/anti-us-protests-hit-sydney/4263372, accessed 5.11.2020.

2. Beran, D., *The Return of Anonymous. The infamous hacker group reemerges from the shadows*, The Atlantic, August 11, 2020, https://www.theatlantic.com/technology/archive/2020/08/hacker-group-anonymous-returns/615058/, accessed on 3.11.2020.

3. Brenner, S., *Organized Cybercrime? How Cyberspace May Affect the Structure of Criminal Relationships*, North Carolina Journal of Law & Technology, Volume 4(1): 1-51, Fall 2002, https://www.researchgate.net/publication/228198960_Organized_

[39] S.Brenner, *Organized Cybercrime? How Cyberspace May Affect the Structure of Criminal Relationships*, North Carolina Journal of Law & Technology, Volume 4(1):1-51, Fall 2002, pp.47-51, https://www.researchgate.net/publication/228198960_Organized_Cybercrime_How_Cyberspace_May_Affect_the_Structure_of_Criminal_Relationships, accessed on 5.11.2020.

[40] C. Wray, cited.

Cybercrime_How_Cyberspace_May_Affect_the_Structure_of_Criminal_Relationship, accessed on 5.11.2020.

4. Broadhurst, R., Grabosky, P., Alazab, M., Chon, S., *Organizations and Cyber crime: An Analysis of the Nature of Groups engaged in Cyber Crime*, International Journal of Cyber Criminology, Vol. 8, Issue 1: 1-20, ianuarie-iunie 2014.

5. Chabinsky, S., *The Cyber Threat: Who's Doing What to Whom?* Federal Bureau of Investigation, 2010, Retrieved from https://archives.fbi.gov/archives/news/speeches/the-cyber-threat-whos-doing-what-to-whom, accessed 5.11.2020.

6. C. Cimpanu, *GermanWiper ransomware hits Germany hard, destroys files, asks for ransom*, ZD Net, 2 August 2019, retrieved from https://www.zdnet.com/article/germanwiper-ransomware-hits-germany-hard-destroys-files-asks-for-ransom/, acessed on 10.03.2020.

7. Cook, J., *FBI Arrests Former SpaceX Employee, Alleging He Ran The 'Deep Web' Drug Marketplace Silk Road 2.0*, Business Insider, November 6, 2014, https://www.businessinsider.com/fbi-silk-road-seized-arrests-2014-11, accessed on 3.11.2020.

8. EU Organized Crime Threat Assessment 2007; www.europol.europa.eu.

9. Europol – EU Policy Cycle – EMPACT, https://www.europol.europa.eu/crime-areas-and-trends/eu-policy-cycle-empact, accessed on 6.06.2020.

10. EUROPOL, *Internet Organized Crime Threat Assessment 2019* (IOCTA 2019), https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2019, accessed on 5.11.2020.

11. Falcone, G., *Mafia*, Ed.Danubius, Bucureşti, 1994.

12. Halliday, J., *London riots: BlackBerry to help police probe Messenger looting 'role'*, The Guardian, August 8, 2011, retrieved from https://www.theguardian.com/uk/2011/aug/08/london-riots-blackberry-messenger-looting, accessed 5.11.2020.

13. https://deloitte.wsj.com/cio/2015/05/12/security-expert-marc-goodman-on-cyber-crime/, accessed on 2.11.2020.

14. Kerr, P., *Mafia Rusească,* Ed. Aldo Press, 1997.

15. Leukfeldt, E.R., Lavorgna, A., Kleemans, E.R., *Organised Cybercrime or Cybercrime that is Organised? An Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime, European Journal of Criminal Policy Res* 23, 2017, https://doi.org/10.1007/s10610-016-9332-z, accessed on 2.11.2020.

16. Longo, F., *Discoursing organized crime. Towards a two-level analysis,* în Felia Allum, Francesca Longo, F., Irrera, D., Kostakos P.A. (editors), *Defining and Defying Organized Crime. Discourse, perceptions and reality,* Part I, Routledge advances in international relations and global politics, Rutledge, New York, 2010.

17. Mazela, M., *Organizational structures of cybercrime groups: Overview of key characteristics*, European Cybersecurity Market, Vol. 2, Issue 3-4: 18-23, 2018.

18. McGuire, M., *Organised Crime in the Digital Age*, London, John Grieve Centre for Policing and Security, 2012.

19. Miralis, N.G., *What were the greatest organised cybercrime threats in 2019?*, Lexology, February 14, 2020, https://www.lexology.com/library/detail.aspx?g= 8ca91844-7c49-4542-9a7a-f78530b616dc, accessed on 5.11.2020.

20. Obokata, T., *Transnational Organized Crime in International Law,* Hart Publishing, Oxford and Portland Oregon, USA, 2010.

21. Oerlemans, J.-J., *Investigating Cybercrime*, Thesis, SIKS – The Dutch Research School for Information and Knowledge Systems, Amsterdam University Press, 2017, p. 20, DOI: 10.13140/RG.2.2.19060.55686.

22. Olson, P., *We Are Anonymous: Inside the Hacker World of LulzSec*, Anonymous, and the Global Cyber Insurgency, 2012, London: Little, Brown.

23. Pitulescu, I., *Crima Organizată*, Ed. Naţional, 1996.

24. Puzo, M., *Sicilianul,* Ed. Politică, Bucureşti, 1997.

25. Sutherland, E.H., *White Collar Crime: The Uncut Version*, Yale University Press, 1983, Business & Economics.

26. The Wall Street Journal, *Security Expert Marc Goodman on Cyber Crime*, May 12, 2015,

27. Tropina, T., *The evolving structure of online criminality. How cybercrime is getting organized*, Eucrim, The European Criminal Law Associations' Forum, issue 4/2012.

28. UN Convention against Transnational Organized Crime, 2000.

29. Ursa, V., *Criminologie*, Ed. Didactico-Ştiinţifică, Bucureşti, 1996.

30. US Attorney's Office, *Northern District of Illinois, U.S. Indicts Ohio Man and Two Foreign Residents in Alleged Ukraine-Based "Scareware" Fraud Scheme That Caused $100 Million in Losses to Internet Victims Worldwide*, May 27, 2010, https://archives.fbi.gov/archives/chicago/press-releases/2010/cg052710-1.htm, accessed on 2.11.2020.

31. Wall, D., *Dis-Organised Crime: Towards a Distributed Model of the Organization of Cybercrime*, The European Review of Organised Crime, 2(2), 2015.

32. Williams, P., *Organized Crime and Cybercrime: Synergies, Trends, and Responses*, Global Issues, Volume: 6, Issue: 2, August 2001, https://www.ncjrs.gov/App/ Publications/abstract.aspx?ID=191389, accessed on 2.11.2020.

33. Wray, C., Director of Federal Bureau of Investigation (FBI), *Digital Transformation: Using Innovation to Combat the Cyber Threat*, Speech at the Boston College/FBI – Boston Conference on Cyber Security, March 7, 2018, https://www.fbi.gov/news/speeches/digital-transformation-using-innovation-to-combat-the-cyber-threat, accessed on 2.11.2020.

About Legality of *On Line* Trials in Criminal Procedure

Zoran S. Pavlović *

Abstract

Online trials and human rights standards cover various aspects of the right to a fair trial contained in Article 6 of the European Convention on Human Rights (ECHR) and / or the prohibition of torture and torture in Article 3 of the ECHR, in particular how to ensure the principle of legality and procedural guarantees in criminal court proceedings during an unprecedented health crisis in modern times. The status of subjects in criminal proceedings may depend on their ability to express themselves clearly and to represent their interests. A virus pandemic Covid-19 has posed unprecedented challenges when it comes to many human rights, including the area of justice in the context of a new reality, from the principle of publicity, the right to defense or the right to a fair trial. The use of IT solutions could not necessarily replace physical presence in the absence of clear regulations and proper enforcement by courts. An additional issue has become the availability of reliable software that would enable a secure and stable connection. Numerous problems could suddenly open up issues related to the ECHR: poor sound system in the courtroom, internet connection, concerns regarding personal data, confidential communication with counsel, and public access to the trial. Provision in law, standards and pro futuro procedures can prevent such situations in the future.

Keywords: *right to a fair trial, prohibition of torture, principle of publicity, principle of legality.*

I. Instead of an introduction

One of the biggest challenges of today is certainly a life during the pandemic caused by the COVID19 virus and its consequences, but also the organization for the day after, having in mind the consequences of the disease and the appropriate response to this global problem. At the same time, the consequences in the field of criminal law and more broadly in the field of human rights are obvious. In modern times, the Republic of Serbia has twice encountered the suspension of certain rights and freedoms, during 1999 and 2020, during the aggression of the COVID19 virus, as an epidemic of world proportions. This certainly affected the exercise (restriction) of the rights provided by international and domestic standards in criminal proceedings. The question is, whether these restrictions are necessary, and only for criminal offenses, non-compliance with health regulations during the epidemic and transmission of infectious diseases. The introduction of a trial using the *online Skype* platform, for these two crimes (violation of self-isolation measures), as a form of participation of a detained defendant in criminal proceedings, is extremely debatable. While it is

* PhD, Full Professor, University of Business Academy Novi Sad, Law Faculty (Serbia). Contact: zoran.pav@hotmail.com.

important to sanction individuals who do not comply with health regulations during a pandemic, as a measure of general and special prevention, this must in no way prejudice the rights guaranteed in international and domestic law.

The use of the *Skype* application or some other computer program for trials is not problematic *only* if as such it is provided by procedural legislation, which is still not the case so far. This conduct of the executive and the judiciary regarding and this form of judicial decision-making was not only a characteristic of Serbian criminal procedural law, but also of other countries of the same or similar model of judicial organization during the pandemic. Therefore, we cite here only as an example the invalid verdict of the Basic Court in Dimitrovgrad from March 2020, where the defendant was found guilty of the criminal offense of failing to comply with health regulations during the epidemic under Article 248 of the Criminal Code. The defendant was sentenced to three years in prison, the maximum sentence, which includes the time the defendant spent in custody[1].

Such a verdict passed after the *Skype* trial opened several questions, among which are the basic ones: non-respect of the principle of immediacy and the principle of publicity. Such an open question of legality of work and decision-making of courts is certainly not with the aim of giving a message whether to sanction all those who do not respect health measures adopted and in order to prevent the spread of corona virus, but that such an important topic should be regulated by positive regulations, even during a state of emergency. The answer therefore cannot be simple, so let us move on in following order.

II. The use of technical means for the transmission of image and sound in criminal proceedings in international and community law

Technological achievements of the new age and the use of technical means for the transmission of sound and images have brought a whole series of changes in criminal matters in traditional criminal law, which not only accelerate them but also change the manner and concept of conducting proceedings. Following the practice of the ICTY, we noticed that they were among the first in Europe to start using the trial via video link or Skype trial. The court established by the decision of the UN Security Council was thus a pioneer in this area. Thus, the 1994 Rules of Procedure and Evidence of the *Ad Hoc* Tribunal were amended[2] Rule 71 point A provides that the Trial Chamber may order, in the interests of justice, that an out-of-trial testimony be taken, specifying in point D that such testimony may be given both in court and out of court, by videoconference. A similar solution provides for the EU Directive 2012/29[3] as the possibility of giving testimony to victims and witnesses using communication technologies. The Directive stipulates in its standards that national legislation will regulate the use of technical means for the transmission of images and sound – video links, as an option for additional protection of victims and witnesses.

---

[1] http://rs.n1info.com/Vesti/a584070/Odrzana-prva-Skajp-sudjenja-struka-upozorava-krse-se-prava-okrivljenih.html.

[2] https://www.icty.org/bcs/documents/pravilnik-o-postupku-i-dokazima.

[3] Directive 2012/29EU of the European Parliament and of the Council of October, 25 2012 establishing minimum standards on the rights, support and protection of victims of crime.

In France and Great Britain, even before the measures of imprisonment due to the pandemic caused by the COVID 19 virus, videoconferencing was used during the trial, while in Russia; this model of working on long-distance hearings was introduced as the so-called *hybrid* trial. These are trials that are conducted mainly before the Commercial Court, and the judges are in the court building – in the courtroom, and the parties are in their premises. This is a great practical solution in the administration of justice in the largest country with a veto, having in mind the existence of great distances between the regions.

The French right the shape of the hearing leaves as discretionary BC and in the judges, but still not completely defined who should be in charge (of the court or the parties) for a choice between *on-line* trials or traditional leadership concussion among those present. Trials in the UK are a small problem with *online* jury trials.

Doctrine and jurisprudence in the United States have been largely against pleading guilty through the use of videoconferencing in proceedings leading to a pandemic caused by COVID 19. That's right, following Hillman's allegations[4] The U.S. Supreme Court gave an interpretation of the relevant provisions of the Federal Rules of Criminal Procedure, in the context of protecting the defendant's right to a trial in presence, Part VI of the Amendment to the USA Constitution. The presence of the accused implies physical presence, and personal contact and interaction with the judge is irreplaceable, so that virtual reality is inadequate to the actual presence. The right to a fair trial and a fair trial cannot be held against Judge Brennan (in the case of *Bruton v. USA*) if the defendant is not directly present, if there is a forced atmosphere generated by detention, without adequate support from counsel as counsel.

On the other hand, at the time of the pandemic in the USA, a verdict based on plea bargaining was passed in 2020 in the Federal Court in St. Louis. The defendant was in custody, and housed in one room, the judge in another, and the prosecutor and defense counsel were in their offices. The comment that could otherwise be given on concluding an agreement between the prosecutor and the defendant in such specific conditions is even more difficult, because it (the agreement) is part of the pressure on the defendants to plead guilty in order to avoid imprisonment. The absence of the public and the principle of immediacy were not legally justified in this particular case[5].

The relative surprise of the judiciary with the emerging situation related to the dangers and challenges of COVID 19 does not obviously mean that there has been no consideration of these issues in relation to standards of conduct. The case law of the European Court of Human Rights, similar to the American judge Brennan, stated that the rules of the European Convention on Human Rights apply equally to distance hearings. So is the Grand Chamber in *Sakhnovskiy v. Russia*[6] ruled that the use of videoconferencing was neither an advantage nor a disadvantage over the standard of the right to a fair trial under Article 6 of the Convention, as a technology that could be used in court proceedings. However, this does not relieve the national authorities of their obligations under Article 6 of the ECHR and the principle of fairness. It is the court that must ensure the legality of the proceedings and ensure a fair balance of all interests.

---

[4] Hillman, Z.M., (2007) Pleading Guilty and Video Teleconference: Is a Defendant Constitutionally "Present" when Pleading Guilty by Video Teleconference?", Journal of High Technology Law, Vol.VII, No.1.

[5] https://www.stltoday.com/news/local/crime-and-courts/federal-court-in-st-louis-holds-first-guilty-plea-by-videoconference/article_fd5f6525-fbff-5316-9e79-f8624d768.

[6] https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-101568%22]}.

Such legal reasoning indicates the only possible solution, i.e. that the use of videoconferencing and related practical means is feasible only if as such, it is provided for in the national procedural legislation.

One of the unresolved issues in *online* trials is information security and party identification. The technical quality of videoconferencing is a prerequisite for the effective participation of all parties to the proceedings. If no courts May own platform with the information system that allows identification of the parties, to use an open s communication s platform s, such as *Skype*. The limbs in Serbia used *Skype,* and the security of this communication platform for court hearings is problematic. Russian commercial courts do not have these problems; they already have their own video platforms built. For the correct use of these IT platforms, it would also mean introducing the participants to the procedure of use.

In the UK, special guidelines have been developed for distance hearings – online hearings, which must comply with the rules of conduct as in the courts. However, in the case of persons with a communication disability, these instructions may not be particularly useful. The fairness of the procedure is further complicated by cross-examination in the online format, because there is no solution here for now, and this will have to be worked on separately. The possibility of equal participation of subjects in the proceedings, the efficiency of the judiciary and the fairness of the proceedings remain the most important aspects when a judge makes a decision on the use of videoconferencing, regardless of its format.

Insight into the files from the earliest stage of the proceedings is a special issue, especially in online trials. While access and exchange of documents electronically has been a common practice in the UK for many years, this could not be said for trials in some other countries. Even without special research, we can claim that in the criminal proceedings that were conducted in Serbia, there was no such interaction between the parties and the court.

This in fact jeopardizes the reaction of one of the parties to new evidence that could emerge during the trial. This has to do with the moment until which new evidence can be submitted and the decision of the national legislation accordingly. Such issues do not arise in the UK, as the parties are required to disclose their direction of defence during the pre-trial proceedings.

The principle of publicity, as an indisputable value of modern criminal procedure by applying online trials, has at least two problems. On the one hand, there is the need to protect the parties from conducting court proceedings in secret without any public control, and the desire to maintain trust in the courts, on the other. Skype trials are certainly not available to the general public and there is no need to discuss the issue of their compliance with one of the requirements of Article 6 of the ECHR. Monitoring of court prosecutions can do the courts open and accessible regardless of distance, and whether the case when the information about the trial online publicly available. Such an objection can be remedied by timely informing the public and the media about the place and model of the discussion and the ways for an effective approach. But ... in the case of applying the principle of publicity in real-time online trials, the question of the privacy of the participants in the procedure and the risks to their privacy arises. Although the sessions of the appellate and highest courts are mostly public, the question is how safe it is in the first instance chambers, due to the so-called zoom bombing or the possibility of unauthorized shooting and privacy violations.

While all sessions of the Supreme Court of the UK are public, one of the solutions can already be seen in, for example, the Serbian legislator, because in organized crime

proceedings it provided for the possibility of recording the entire procedure, which then allows subsequent public insight into the course and credibility of the entire procedure.

For a trial to be fair, it would be extremely important to be able to see the entire courtroom, not just the faces of those speaking at a given moment. This detail, although not conventionally provided for, is implied as such.

Article 6 of the ECHR provides for the guarantee of discretion in communication between the defendant and the lawyers of defence during the criminal proceedings. The right to effective legal aid includes the right of the accused to communicate privately with his lawyer. If a lawyer is unable to meet with his client and receive confidential instructions from him without supervision, his assistance is not in line with the standard of the right to a defence. In online trials, there must be all the technical possibilities to avoid any pressure or influence on the accused (especially the detainee) that may not be visible in the regular proceedings. In criminal proceedings conducted online, and especially if the defendant is in custody, as long as he is not provided with a secure line of communication with counsel, his right to defence is not fully exercised. In France, it is not regulated where the defence counsel is in online trials, so this is certainly something that is left to court practice, and that is not the best solution.

These are just some of the problems and solutions in online trials that we have given as an example. From those that are purely technical in nature, but as such are still regulated by procedural legislation, not technical instructions, at trials, to those that violate basic principles of criminal procedural law, such as the principle of immediacy, publicity, the right to counsel and confidentiality. conversation, prohibition of torture and other torture, all of which together can call into question the need for efficient resolution of court proceedings, but also with the right to a fair trial. Justice is not a matter of technique and a matter of compromise, but a principle from which it cannot be an exception, regardless of all the difficulties that accompany the time of the pandemic. The fact is that such situations caused by the COVID 19 pandemic must be foreseen in the future, which indicates the possible need for a unified regulation of online trials.

III. The right to a fair trial and online procedure in the jurisprudence and legislation of Serbia

The current Code of Criminal Procedure does not currently provide the possibility of trial through using of technical means for the transmission of sound and images, only in the proceedings before the first instance court, leaving that possibility (the court may) only in the procedure of deciding on a legal remedy. As an exception to the principle of immediacy in criminal proceedings, this is the case here:

1. Where there are certain exceptions, such as securing the presence of the accused for security or other reasons, and

2. When the condition is met that there are appropriate technical conditions for that, so the accused may appear at the hearing by technical means for the transmission of sound and images (Article 449, paragraph 4 in fine of the CPC). This possibility can also be applied at a hearing held before a court that decides on an appeal against a second-instance judgment (Article 464, paragraph 1 of the CPC).

In the context of the right to justice according to the case law of the European Court of Human Rights, the direct presence of the defendant before a court of law is not as decisive as when it comes to a trial before a court of first instance. However, this does not exclude the exceptional possibility that the first-instance trial in which the participation of the defendant is secured via video link will be assessed as in accordance with the guarantees contained in the right to a fair trial.

The rule is that the direct presence of the defendant in the first-instance procedure implies, in principle, his/her ability to participate in the hearing. This undoubtedly follows from the subject-matter and purpose of paragraph 1 of Article 6 of the ECHR. In addition, the provisions of paragraph 3 of Article 6 of the ECHR, which guarantee every accused one the right to defend himself/herself, to examine or request the examination of a witness and to be provided with a free interpreter if he/she does not understand or speak the language of the trial, are unfeasible without his/her presence at trial.

Ensuring the presence of the defendant via video link before the court of legal remedy is not necessarily incompatible with the right to a fair trial, provided that the defendant is able to follow the procedure and be heard without technical difficulties, and to have an effective and confidential conversation with the defense counsel/person.

Guided by this analogy, and at the time of the COVID19 pandemic, which did not only affect our country and countries in the region, the question of the legality of the Decree brought on April 1st, 2020 was raised, which prescribes the possibility for a defendant in custody to participate in the main trial assistance of technical means and to refer to any criminal proceedings (therefore, for any criminal offense) conducted before the first instance court. The decision on that is made by the president of the panel, i.e. the single judge, provided that he/she considers that securing the presence of the accused at the main trial is difficult due to the danger of spreading a contagious disease. This provision shall apply during a state of emergency, provided that there are appropriate technical possibilities.

Pursuant to the provisions of Article 32 of the Constitution of the Republic of Serbia and Article 6 of the ECHR, the right of access to a court and a reasoned decision are part of the right to a fair trial, which means that in no case can there be deviations from human and minority rights, it should be also in accordance with legislative solutions.

This means that trials via video link or Skype application are then in contrary to the principle of immediacy, but also in contrary to the principle of publicity.

However, having in mind the fact that the Decree of the Government of Serbia of April 1st, 2020 has brought the right to hold such trials, which was just introduced in 2020, needs to be explained why the participation of the defendant in the main trial via video link does not diminish the guarantees contained in the right to a fair trial.

According to the cited Decree, during the state of emergency declared on March 15th, 2020, in criminal proceedings before the first instance court, when the presiding judge or single judge finds that securing the presence of the accused in custody is difficult, or at the main trial, due to the danger of spreading a contagious disease, he/she may decide to ensure the participation of the defendant in the main trial through technical means for the transmission of sound and images, if this is possible given the technical conditions.

This Decree came after the initiative of the courts for such a way of working, which was accepted by the Ministry of Justice by instructing the courts to act in a uniform manner, so that such a Decree would be adopted soon.

Skype trials in special courtrooms were therefore recommended by the Ministry of Justice, in order to ensure the safety of defendants and court employees, and to prevent the spread of the corona virus.

The trial via the Skype application, i.e. online, also opens up problems in the light of the absolute prohibition of torture, inhuman or degrading treatment or punishment.

In the light of the basic principles of criminal procedure, starting from the principle of legality, conducting main trials in this way, may reduce the guarantees for protection against maltreatment, which arise from Article 25 of the Constitution of the Republic of Serbia and from Article 3 of the Convention for the Protection of Human Rights and Fundamental Freedoms that must not be deviated even during a state of emergency.

A defendant who was a victim of abuse/maltreatment and who is physically under the control of officials who abused him/her or who are in close hierarchical or organizational connection with the perpetrators of the abuse during the main trial, and not in the court building, may be discouraged from taking out the allegations of abuse he/she suffered to the court because of fear of retaliation.

The situation in which the defendant does not have personal contact with his defense counsel/person but communicates through technical means for the transmission of images and sound, can significantly contribute to discouraging the defendant from presenting allegations of abuse to the court or defense counsel/person.

In order to avoid this situation, the text of the Criminal Procedure Code should include this possibility for the first instance procedure, for special cases, of course, with guarantees that it would provide the defendant not only the right to a fair trial, the principle of immediacy, but also guarantees protection from maltreatment or torture, which all mentioned would be a violation of Article 3 of the ECHR.

In the function of justice and respect for the protection of human rights, which are listed as rights from which there are no deviations, this could be ensured through the activities of the NPM mechanism in which the fourth branch of government participates, i.e. the Protector of Serbian Citizens with the Provincial Ombudsman and civil society organizations.

The legality of the trial, which takes place partly in an online form, would be then strengthened by good organization and explanation, by the participation of the ombudsman and other institutions and in this way, it would be reduced to a minimum the doubts about its validity (legality).

The current imperfections of the state of emergency solutions on online trials should not discourage us from conducting them, but to use them in such a way, and when we introduce them in the CPC, of course, in accordance with the Constitution of Serbia and the ECHR, to allow them to contribute to preserving the rule of law and respect for human rights of all citizens.

V. Conclusion or where are we and where to go next

The holding of a remote trial – online in criminal proceedings in Serbia and in the world was imposed by the COVID19 pandemic. In order to protect the application of the principle of immediacy in criminal proceedings and the legitimate interests of a democratic society – security and safety risks, public health, harm reduction to the participants in the procedure, but also to the staff in the court and the prosecutor's

office, holding hearings and not their postponement, when undertaking procedural actions through online trials, technical means for image and sound transmission must still be applied restrictively. The decision to conduct such a trial modality should be in court and the basis in the Law.

This requires judges to have special technical skills, pre-trial logistical arrangements and additional management responsibilities. At the same time, it is necessary to establish the existence of a legitimate interest in *an online* trial, i.e. for a virtual trial among those present instead of the physical presence of the trial subject before the court.

In order to be able to approach an online trial, the principle of equality of arms between the parties as an aspect of the principle of fairness through the assessment of effective virtual participation must not be violated either.

Technical resources in terms of applying the highest standards in image and sound transmission must be adjusted in terms of a high standard of image, sound and opportunities for effective participation of the defendant in the examination of witnesses and presentation of other evidence, as parties equal to the prosecutor.

And while in the real world we mainly focus on the legal status and protection of the rights of the accused, which are discussed in this paper, the fact is that exactly the same conditions must be provided to the victim of a crime, as a condition *sine qaua non* for a fair trial.

The question arises, assuming that an online form of trial is envisaged in procedural law, to what extent are legally binding rules necessary or would guidelines representing soft law be sufficient? The rapid and continuous development of communication technology provides for the right to some experts come to the formulation of soft regulation, by means of a guideline, rather than legally binding regulations. However, the type of regulation should depend and of the legal system in each country. In the country of continental legal tradition, that is certainly the Code of Criminal Procedure. In any case, it is important to have appropriate guidelines (in any form). In addition to regulations, two other elements are important for a successful distance trial:

(1) Cooperation of all subjects in remote proceedings and online trials and

(2) Taking into account the experience gained in remote procedures during the pandemic caused by the COVID-19 virus.

This means that it will be necessary to amend the existing procedural legislation in order to bring it into line with new forms of trials via videoconferencing. Some problems could be related to the strict legal determination of cases and situations in which remote proceedings are allowed, without leaving room for discretionary decision-making by judges, especially in critical situations, such as the health crisis caused by the COVID-19 pandemic.

Relativization of criminal procedural solutions or freer interpretation of certain criminal procedural principles through deviation from the usual rules is not a good solution, but the determination of online trials only when the legal conditions are met. In criminal procedural law, there is no possibility to apply the analogy in criminal proceedings. And there can be no deviations through parallels with some other proceedings, without a legal basis (parallels with administrative proceedings, for example).

It is this analogy in online trials that could be linked to a document adopted almost 10 years ago regarding the position of the victim in criminal proceedings, but Directive 2012/29 / EU and its solutions have not yet been fully implemented in

domestic legislation and courts. This is not only due to the increased caution of case law, but more as a reflection of the lack of technical possibilities for the same. Namely, it is not possible to talk about the application of modern criminal procedure possibilities that provide technical means for image and sound transmission as a substitution of direct presence of subjects in criminal proceedings when such technical possibilities are still not provided in all courts. If we have not succeeded in the field of protection of victims' rights, then we should fully consider the issue of online trials without the presence of the defendant and see how we could implement it in courts of all levels, for all proceedings and for all subjects.

The revision of existing procedural legislation is something that is necessary to bring regulations into line with the new form of trial now unquestionably imposed by the pandemic. Some of the problems could be solved by making this a strict exception, without leaving the discretionary power of the acting president of the panel – the judge, especially in situations such as the health crisis.

Critics of *online* trials in Serbia gave less attention even to solutions that are in these procedures applied; paid less attention even to the solutions applied in those proceedings and paid more attention to the lack of regulation due to the lack of solutions in the law.

So, some problems with the trial via video conference connections can be attached to the decision regarding the non-fortification procedures and solutions. Without effective safeguards in terms of ensuring the principles of publicity, privacy in communication with counsel, protection from torture and torture through the national preventive mechanism against torture, the principle of immediacy – active participation in court decisions on detention, are just some of the aspects to consider, ensuring a lawful and proper online trial.

To conclude, the effective participation of any subject in criminal proceedings online depends on their ability to express themselves clearly and to represent their interests. This principle is an integral part of the right guaranteed by Article 6 of the ECHR in civil and criminal proceedings. The COVID-19 online trials and pandemic have posed unprecedented challenges to many human rights, including the administration of justice in the face of a new, virtual reality: trials have had to continue, while the rules of physical distance and barriers; along with travel restrictions did not always allow the parties to be present at the hearing. The use of IT solutions could not necessarily replace physical presence in the absence of clear regulations and established approaches by courts. Without clearly legally defined conditions for online trials, they would call into question the meaning of legality and legal security of citizens. This would violate the values envisaged by the Universal Declaration of Human Rights, the ECHR and public order.

Long-term changes and improvements in the work of national courts, following experience in COVID-19 online trials, can contribute to legal certainty and the full application and respect of the rule of law in a society. This would confirm the rule that the level of protection of human rights in criminal procedure legislation is a reflection of the state of human rights in society as a whole, regardless of whether this protection takes place directly before the court in physical presence, or in an online format.

References

Directive 2012/29 EU of the European Parliament and of the Council of October, 25 2012 establishing minimum standards on the rights, support and protection of victims of crime.

1. Hillman, Z.M., *Pleading Guilty and Video Teleconference: Is a Defendant Constitutionally "Present" when Pleading Guilty by Video Teleconference?"*, Journal of High Technology Law, Vol.VII, No.1, 2007.
2. http://rs.n1info.com/Vesti/a584070/Odrzana-prva-Skajp-sudjenja-struka-upozorava-krse-se-prava-okrivljenih.html.
3. https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-101568%22]}.
4. https://www.icty.org/bcs/documents/pravilnik-o-postupku-i-dokazima.
5. https://www.stltoday.com/news/local/crime-and-courts/federal-court-in-st-louis-holds-first-guilty-plea-by-videoconference/article_fd5f6525-fbff-5316-9e79-f8624d768.

Fake News and the Challenges of Criminal Law

Giulia Lanza*

Abstract

The spread of fake news online is a global and complex phenomenon. It can be considered a "virus" that must be actively fought at several levels (i.e., supranational level and domestic level) and by different actors (i.e., private and public). This phenomenon is challenging for both social media companies and states, and they are called on to work in a synergy to address it. Many mechanisms and legislative measures have been proposed and adopted in order to counter the diffusion of fake news online. Some countries have also relied on criminal law. However, due to the complexity of the phenomenon, the specificity of each domestic legal order and the variety of fake news, it is not an easy task and it is difficult to adopt a unique solution that applies in all circumstances. The situation in Italy reflects such a difficulty. Therefore, particular attention will be paid to the different approaches proposed in Italy in order to address the spread of fake news online. Can we be sure that criminal law is the only (or the best) solution to deal with such a growing phenomenon? I conclude that criminal law may be invoked only in exceptional circumstances and when non-criminal measures prove inadequate to protect legal goods (Rechtsgüter) of paramount importance. Nevertheless, criminal law and the fight against the diffusion of fake news cannot be used – as has been done in certain countries – neither as an excuse nor as a tool to violate the right to freedom of expression, and to limit pluralism and participatory democracy.

Keywords: *Fake news, global phenomenon, social media, criminal law, human rights, freedom of expression.*

I. Fake news as a global phenomenon

The problem of fake news is not a contemporary one. History has always witnessed the diffusion of "false stories"[1]. The only new factor is the means of communication (the Internet) used in the "digital era" to spread false or misleading

---

* Postdoctoral researcher at the Department of Law, University of Verona. This is an elaborated version of the paper presented on 6 November 2020 at the *International Biennial Conference, 13th Edition*, organized by the Faculty of Law of the West University of Timisoara. The fake news phenomenon is very complex and presents several problematic issues that cannot be addressed here. The paper offers an updated overview of the measures adopted at supranational level to fight against this growing phenomenon, further increased during the Covid-19 pandemic. Moreover, it focuses on the different approaches developed at domestic level to address it and on the possibility of relying on criminal law to counter the diffusion of fake news.

[1] F. Safieddine, *History of Fake News*, in F. Safieddine, Y. Ibrahim (eds.), *Fake News in an Era of Social Media: Tracking Viral Contagion*, Rowman & Littlefield International, London, New York, 2020, p. 18 ff.; F. Sciacchitano, A. Panza, *Fake News e disinformazione online: misure internazionali*, in *Rivista di diritto dei media*, 1/2020, p. 104; L. Canfora, *La storia falsa*, Rizzoli, Milano, 2008. See also: S. Casillo, F. Di Trocchio, S. Sica, *Falsi giornalistici. Finti scoop e bufale quotidiane*, Alfredo Guida Editore, Napoli, 1997.

information, accompanied by the speed and the low cost of its diffusion in cyberspace[2]. The global emergence of the Internet, the uncontrolled access to information available on it and the increasing usage of social media[3] in several countries – including less economically developed countries (LEDCs) – determined a massive wave of false and misleading information in several contexts. Consider, for example: the US presidential elections of 2016; the Brexit referendum that had taken place in the same year; the new pandemic disease (Covid-19) that plagued (and is still plaguing) the entire word and has been accompanied by an unprecedented 'infodemic'[4]; the humanitarian crisis that afflicted Myanmar[5]. In all these scenarios, very different from each other, the spread of fake news had (and continues to have) a very negative impact.

Mass online disinformation campaigns are very frequent and sometimes may have a transnational character. They can be considered a "new weapon" of the "digital era"[6]. They take advantage of social media and are used in order to cause harm or social unrest, as well as to manipulate public opinion, jeopardizing the democratic principle[7]. They are among the most dangerous and subtle forms of aggression against

---

[2] P. Guercia, *I progetti di legge sulle fake news e la disciplina tedesca a confronto*, in A. Cadoppi, S. Canestrari, A. Manna, M. Papa (eds.), *Cybercrime*, Utet, Milan, 2019, pp. 1257-1258; M. Bassini, G.E. Vigevani, *Primi appunti su fake news e dintorni*, in *Rivista di diritto dei media*, 1/2017, p. 15. On the specificity of *cyberspace*, *ex multis*: L. Picotti, *Diritto penale e tecnologie informatiche: una visione d'insieme*, in A. Cadoppi, S. Canestrari, A. Manna, M. Papa (eds.), *Cybercrime*, Utet, Milano, 2019, pp. 57-58.

[3] M. Monti, *Fake news e social network: la verità ai tempi di Facebook*, in *Rivista di diritto dei media*, 1/2017, p. 80 ff.; C.E. Paliero, *La maschera e il volto. (Percezione sociale del crimine ed 'effetti penali' dei media)*, in *Rivista italiana di diritto e procedura penale*, 2/2006, p. 470.

[4] This term was used by the World Health Organization (WHO) to target the proliferation of an excessive amount of information about Covid-19. It further specified that infodemics "can spread misinformation, disinformation and rumors during a health emergency […] can hamper an effective public health response and create confusion and distrust among people", https://www.un.org/en/un-coronavirus-communications-team/un-tackling-'infodemic'-misinformation-and-cybercrime-covid-19, accessed on 29 November 2020. The WHO considered such a phenomenon as one of the greatest threats to public health. On the impact of Facebook on the diffusion of fake news related to the pandemic: T. Guerini, *La tutela penale della libertà di manifestazione del pensiero nell'epoca delle fake news e delle infodemie*, in *discrimen.it*, 14 June 2020, pp. 14-15. Fake news also has a strong impact on the vaccination campaign, increasing hesitancy to vaccinate. On the impact of fake news on public health more recently, see: K. Mamak, *Do we need the criminalization of medical fake news?*, in *Medicine, Health Care and Philosophy*, 2021, p. 1 ff.

[5] As highlighted in the *Report of the detailed Findings on the Independent International Fact-Finding mission on Myanmar*, "Facebook has also widely been used to spread misinformation, including by government officials and the Tatmadaw", A/HRC/39/CRP.2, 17 September 2018, para. 1346.

[6] M. Monti, *Italian Populism and Fake News on the Internet: A New Political Weapon in the Public Discourse*, in G. Delledonne, G. Martinico, M. Monti, F. Pacini (eds.), *Italian Populism and Constitutional Law. Challanges to Democracy in the 21th Century*, Palgrave, Macmillan, London, 2020, p. 177 ff. (the author refers in particular to the use of fake news in politics); E. Perucchietti, *Fake news. Dalla manipolazione dell'opinione pubblica alla post-verità. Come il potere controlla i media e fabbrica l'informazione per ottenere consenso*, Arianna Editrice, Bologna, 2018. See also: T. Nagasako, *Global disinformation campaigns and legal challenges*, in *International Cybersecurity Law Review*, 1/2020, p. 127 (the author refers to disinformation as a "new form of warfare created by the information society").

[7] E. Van Wie Davis, *Shadow Warfare: Cyberwar Policy in the United States, Russia, and China*, Rowman & Littlefield, London, 2021, pp. 19-20; T. Nagasako, *Global disinformation campaigns and legal challenges*, in *International Cybersecurity Law Review*, 1/2020, pp. 126-127 (the author stated that disinformation "is a severe challenge to democracy, since it is executed by combining the leakage of information stolen by cyberattacks with information warfare in media and SNS to transform public opinion in individual countries and to influence democratic processes, such as the outcome of elections and demonstrations").

individual and collective legal goods of primary rank, such as reputation, honour, public order, safety and health[8].

The online word is a fertile ground for the propagation of all types of information[9] and debunking fake news is challenging. Most of the individual's life is spent online. This aspect has been further intensified by the Covid-19 pandemic. Social media platforms, such as Facebook, Instagram and Twitter, are the most common instruments used to spread both "false" and "truthful" information. Social media algorithms[10], as well as mechanisms of sharing, reposting and retweeting, can contribute to the proliferation of fake news. In the "digital era", users are no longer mere consumers of online services, but they play an active role, sharing and producing content[11]. The use of bots and fakes profiles[12] further accelerates the diffusion of such news[13]. A role is also played by "filter bubbles"[14] and "echo chambers"[15] that may

---

[8] S. De Flammineis, *Diritto penale, beni giuridici collettivi nella sfida delle fake news: principio di offensività ed emergenze*, in *Sistema penale*, 6/2020, p. 131 ff.; T. Guerini, *La tutela penale della libertà di manifestazione del pensiero nell'epoca delle fake news e delle infodemie*, in *discrimen.it*, 15 June 2020, p. 4.

[9] F. Sciacchitano, A. Panza, *Fake News e disinformazione online: misure internazionali*, in *Rivista di diritto dei media*, 1/2020, pp. 104-105; S. De Flammineis, *Diritto penale, beni giuridici collettivi nella sfida delle fake news: principio di offensività ed emergenze*, in *Sistema penale*, 6/2020, pp. 141-142; G. Pitruzzella, *La libertà di informazione nell'era di Internet*, in *Rivista di diritto dei media*, 1/2018, p. 30 ff.

[10] On the relationship between algorithms and fake news: G. Marchetti, *Le fake news e il ruolo degli algoritmi*, in *Rivista di diritto dei media*, 1/2020, pp. 29-36. The author examines the role of algorithms both as an instrument to create and spread fake news, and as an instrument to counter their diffusion. For example, Project Fandango, funded by the European Union's H2020 EU research and innovation program, is aimed at using artificial intelligence and, in particular, algorithms to counter fake news, for more details see: https://fandango-project.eu/the-project/what-is-fandango/, accessed on 15 January 2020.

[11] L. Picotti, *Diritto penale e tecnologie informatiche: una visione d'insieme*, in A. Cadoppi, S. Canestrari, A. Manna, M. Papa (eds.), *Cybercrime*, Utet, Milano, 2019, p. 43; F. Sciacchitano, A. Panza, *Fake News e disinformazione online: misure internazionali*, in *Rivista di diritto dei media*, 1/2020, p. 104; P. Caretti, A. Cardone, *Diritto dell'informazione e della comunicazione nell'era della convergenza*, Il Mulino, Bologna, 2019, p. 254 ff. This aspect has been emphasized also by the Council of Europe in Resolution 2143 (2017), *Online media and Journalism: Challenges and Accountability*, https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=23455&lang=en, accessed on 20 November 2020.

[12] On the impact of fake profiles and bots in the diffusion of fake news: A. Mazziotti di Celso, *Dal primo emendamento al bavaglio malese. Fake news, libertà di espressione e il rovesciamento delle categorie politiche tradizionali*, in *Rivista di Diritto dei Media*, 3/2018, p. 93 ff.

[13] F. Donati, *Fake News e libertà d'informazione*, in *Rivista di Diritto dei Media*, 2/2018, p. 440.

[14] The term "*filter bubble*" is used to describe a phenomenon that limits the exposure of the individual to a full range of information on the Internet by algorithmically prioritizing content that matches the user's profile, his or her online history, excluding content that does not. This term was coined in the following book: E. Pariser, *The Filter Bubble: What the Internet is Hiding from You*, Penguin Group, London, 2011. For further details: Sumpter D., *Outnumbered: From Facebook and Google to Fake News and Filter-bubbles. The Algorithms that Control our Lives*, Bloomsbury, Londra, 2018; F.J. Zuiderveen Borgesius, D. Trilling, J. Möller, B. Bodó, C.H. De Vreese, N. Helberg, *Should we worry about filter bubbles?*, in *Internet Policy Review*, 2016, p. 1 ff.

[15] The term online or social media "*echo chamber*" is used to describe an "environment" in which the same opinions are repeatedly promoted and voiced. As a result, users are not exposed to opposing views. G. Marchetti, *Le fake news e il ruolo degli algoritmi*, in *Rivista di diritto dei media*, 1/2020, p. 31; G. Ziccardi, *Tecnologie per il potere. Come usare i social network in politica*, Raffaello Cortina Editore, Milano, 2019, p. 78; G. Pitruzzella, *La libertà di informazione nell'era di Internet*, in *Rivista di diritto dei media*, 1/2018, p. 31 ff.; W. Quattrociocchi, A. Scala, C.R. Sustein, *Echo Chambers on Facebook*, in *ssrn.com*, 13 June 2016; W. Quattrociocchi, A. Vicini, *Misinformation: guida alla società dell'informazione e della credulità*, Franco Angeli, Milano, 2016, pp. 66-67.

contribute to the propagation of fake news. These phenomena have an increased impact on vulnerable users or on users with a low level of media literacy, and in regions where social media constitutes the sole (or principal) source of information. This is clear, for example, in the case of Myanmar.

II. Defining fake news

Defining fake news is not an easy task[16]. The term "fake news" became particularly common during the Presidency of Donald Trump[17]. The former President of the United States is the first politician to have deployed it very often, also using it as a slur to counter his opponents[18]. In 2017, it became the term of the year[19].

However, the term "fake news" is generally used to refer to a growing and widespread phenomenon, characterized by the circulation of news with a misleading or outright false content[20]. Therefore, it reflects a vast category, which includes different types of information.

In the context of this work, the term "fake news" is used in a broad sense and includes misinformation, disinformation and mal-information[21]. Nevertheless, it must

---

[16] Emphasizing the difficulty for institutions to define the concept of "fake news": F. Sciacchitano, A. Panza, *Fake News e disinformazione online: misure internazionali*, in *Rivista di diritto dei media*, 1/2020, p. 105.

[17] In the press there are those who refer to the "Trump's era of 'fake news'": B. Stelter, *Analysis: Election Day is also a Referendum on Trump's era of 'fake news'*, 30 October 2020, https://edition.cnn.com/2020/10/30/media/fake-news-age/, accessed 29 November 2020.

[18] For example, the Parliamentary Assembly of the Council of Europe in Resolution 2255 (2019) recommended to member states to "avoid the term "fake news", which has been excessively politicized and frequently used to negatively label independent critical journalists or media outlets", but to use instead "the concept of "information disorder" to describe the content, the purpose and the extent of dissemination of misleading information", http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-EN.asp?fileid=25406&lang=en, accessed on 20 November 2020. Similarly, the High-Level Expert Group (HLEG) set up by the European Commission to advise on policy initiatives to counter fake news and disinformation spread online issued a report where it stated that the term "fake news" "has been appropriated and used misleadingly by powerful actors to dismiss coverage that is simply found disagreeable": *A multi-dimensional approach to disinformation. Report of the Independent High Level Group on fake news and online disinformation*, Publication office of the European Union, Luxemburg, 2018, p. 5, https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation, accessed on 20 November 2020.

[19] S. Meza, *"Fake News" Named Word of the Year*, in newsweek.com, 11 February 2017 https://www.newsweek.com/fake-news-word-year-collins-dictionary-699740, accessed on 20 November 2020.

[20] F. De Simone, *'Fake news', 'post truth', 'hate speech': nuovi fenomeni sociali alla prova del diritto penale*, in *Archivio penale*, 1/2018, p. 3.

[21] For example, for a different meaning assigned to these terms, see the Report of the Council of Europe DGI(2017)09: C. Wardle, H. Derakhshan, *Information Disorder: Toward an Interdisciplinary Framework for Research and Policy making*, Council of Europe, Strasbourg, 2017. The authors differentiate between: "mis-information: when the news spread is false but no harm is meant"; "dis-information, when news is false and shared to cause harm"; and, "mal-information, when genuine information is spread to cause harm" (p. 5), https://edoc.coe.int/en/media/7495-information-disorder-toward-an-interdisciplinary-framework-for-research-and-policy-making.html, accessed on 20 November 2020. See also the HLEG's Report, where disinformation is defined "as false, inaccurate, or misleading information designed, presented and promoted to intentionally cause public harm or for profit. The risk of harm includes threats to democratic political processes and values, which can specifically target a variety of sectors, such as health, science, education, finance and more" and misinformation "as misleading or inaccurate information shared by people who do not recognize it as

be noted that there is not a uniform definition of these terms and they may be used and interpreted in different ways, in relation to the context in which they are considered[22]. Not all types of false or misleading information require the same treatment and the tools with which they need to be addressed may vary. This holds true in particular with regards to the feasibility of relying on criminal law. Therefore, in order to limit the scope of a possible intervention of criminal law to counter the phenomenon under examination, it is important to make a preliminary specification. Particular attention will be paid to fake news that may threaten or harm legal goods of paramount importance, such as public order, safety and health. Indeed, false information per se, as well as its diffusion, does not necessarily fall within the sphere of criminal law, except for where it harms or threatens a legal good, such as those previously mentioned[23].

Before focusing on the possibility of relying on criminal law to address this specific type of fake news, it is important to examine the measures proposed and/or adopted at both supranational level and domestic level to combat the phenomenon under examination.

III. The response of the United Nations

The continuous growth of the fake news phenomenon and its global dimension constitute one of the major problems of the modern, connected word and requires a global answer. This became particularly manifest in the face of the Covid-19 pandemic. The World Health Organization (WHO) defined the proliferation and the overabundance of information – including false information – as an "infodemic" and one of the greatest threats to public health. Consequently, it predisposed a reporting mechanism aimed at countering the spread of false and potentially harmful

such", *A multi-dimensional approach to disinformation. Report of the Independent High-Level Group on fake news and online disinformation*, Publication office of the European Union, Luxemburg, 2018, p. 10. On the different types of "fake news" in academic literature, *ex multis*: T. Nagasako, *Global disinformation campaigns and legal challenges*, in *International Cybersecurity Law Review*, 1/2020, p. 125 ff.; F. Safieddine, *History of Fake News*, in F. Safieddine, Y. Ibrahim (eds.), *Fake News in an Era of Social Media: Tracking Viral Contagion*, Rowman & Littlefield International, London, New York, 2020, p. 1 ff. In Italian academic literature: T. Guerini, *La tutela penale della libertà di manifestazione del pensiero nell'epoca delle fake news e delle infodemie*, in *discrimen.it*, 15 June 2020, p. 11 ff.; M. Bassini, G.E. Vigevani, *Primi appunti su fake news e dintorni*, in *Rivista di diritto dei media*, 1/2017, pp. 11 ff. More specifically related to the different interpretation of false information in the Italian criminal legislation and case law: C. Perini, *Fake news e post-verità tra diritto penale e politica criminale*, in *archiviodpc.dirittopenaleuomo.org*, 20 December 2017, pp. 2-3.

[22] In this vein: F. Sciacchitano, A. Panza, *Fake News e disinformazione online: misure internazionali*, in *Rivista di diritto dei media*, 1/2020, p. 105.

[23] In Italian academic literature: P. Guercia, *I progetti di legge sulle fake news e la disciplina tedesca a confronto*, in A. Cadoppi, S. Canestrari, A. Manna, M. Papa (eds.), *Cybercrime*, Utet, Milano, 2019, p. 1256; A. Costantini, *Istanze di criminalizzazione delle fake news al confine tra tutela penale della verità e repressione del dissenso: verso un nuovo simbolismo penale?*, in *Rivista trimestrale di diritto penale contemporaneo*, 2/2019, p. 68; C. Perini, *Fake news e post-verità tra diritto penale e politica criminale*, in *archiviodpc.dirittopenaleuomo.org*, 20 December 2017, p. 3. See also: A. Pace, in A. Pace, M. Manetti (eds.), *La libertà di manifestazione del proprio pensiero (commento all'Art. 21 Cost.),* in *Commentario della Costituzione,* Bologna – Roma, 2006, p. 89; P. Barile, *Diritti dell'uomo e libertà fondamentali*, Il mulino, Bologna, 1984, p. 229; C. Esposito, *La libertà di manifestazione del pensiero nell' ordinamento italiano,* Milano, 1958, p. 36.

information online[24]. Moreover, a team of the WHO "mythbusters" started to collaborate with social media platforms to limit the spread of fake news related to the virus[25]. Regardless of the mechanisms adopted, it is important to respect individual fundamental rights: in particular, the right to freedom of expression. Indeed, as stressed by the Special Rapporteur on Freedom of Opinion and Expression, Robert Kaye, in 2017, "fake news has emerged as a global topic of concern and there is a risk that efforts to counter it could lead to censorship, the suppression of critical thinking and other approaches contrary to human rights law"[26].

The Joint Declaration on Freedom of Expression and "Fake News", Disinformation and Propaganda signed on 3 March 2017 by the United Nations (UN) Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media, the Organization of American States (OAS) Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information, contains the principles that should be aimed at balancing the different interests involved[27]. More precisely, the Declaration encouraged the promotion of pluralism in the media, identified the applicable human rights standards and highlighted the specific roles of the intermediaries, journalists and all stakeholders.

IV. The response of the European Union

One of the major challenges for the European Union is that of combatting fake news and online disinformation[28]. The European Commission has taken several actions in order to address the relevant actors, methods, tools and targets to give a prompt response and put an end to this growing phenomenon.

The first attempt of the European Commission to counter this phenomenon dates back to March 2015, with the establishment of the Task Force East StratCom in the European External Action Service (EEAS), following the disinformation campaign in Russia[29].

---

[24] For more details on the mechanism developed by the WHO "How to report misinformation online": https://www.who.int/campaigns/connecting-the-world-to-combat-coronavirus/how-to-report-misinformation-online?gclid=EAIaIQobChMI6ZKfy7_x7gIVvSB7Ch2i6gD4EAAYASAAEgJ46vD_BwE, accessed on 3 December 2020. See also: J. Zarocostas, *How to Fight an Infodemic*, in *The Lancet*, Vol. 395, February 2020, p. 676.

[25] For more details: https://www.un.org/en/un-coronavirus-communications-team/un-tackling-'infodemic'-misinformation-and-cybercrime-covid-19, accessed on 20 November 2020.

[26] See: https://www.ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=21287&LangID=E, accessed on 20 November 2020.

[27] The text of the Declaration is available at the following link: https://www.osce.org/fom/302796, accessed on 3 December 2020.

[28] For an overview of EU joint and coordinated action against disinformation: https://ec.europa.eu/digital-single-market/en/tackling-online-disinformation, accessed on 3 December 2020. For a detailed analysis of the EU joint and coordinated action against disinformation: F. Sciacchitano, A. Panza, *Fake News e disinformazione online: misure internazionali*, in *Rivista di diritto dei media*, 1/2020, p. 106 ff. This was an important issue not only for the European Union, but also for the Council of Europe, see in particular: Resolution 2143 (2017), Online media and journalism: challenges and accountability, https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=23455&lang=en, accessed on 3 December 2020.

[29] For further details on the Task Force East StratCom: https://eeas.europa.eu/headquarters/headquarters-homepage_en/2116/, accessed on 3 December 2020.

In 2018, the European Commission established a High-Level Expert Group (HLEG) on fake news and online disinformation with the aim of proposing initiatives to counter fake news and disinformation spread online[30]. The responses proposed by the HLEG were expressed in five pillars: 1) enhancing transparency of online news; 2) promoting media and information literacy; 3) developing tools for empowering users and journalists; 4) safeguarding the diversity and the sustainability of the European news media ecosystems; 5) promoting continued research on the impact of disinformation in Europe[31].

In the Communication "Tackling Online Disinformation: a European Approach" of 26 April 2018, the Commission emphasized the importance of the private sector, and therefore of social media platforms, in tackling the problem of online disinformation[32].

In an attempt to regulate the expansion of the phenomenon under examination and in view of the 2019 European elections, the European Commission published the "Code of Practice on Disinformation"[33]. It constitutes an important step in the fight against the spread of online fake news within the EU. It is the first time that players within the industry (i.e., Facebook, Twitter, Google, Mozilla, advertisers) agreed, on a voluntary basis, to adopt self-regulatory standards to fight against fake news online[34]. The aim of the Code is to achieve the objectives delineated in the Commission's Communication "Tackling Online Disinformation: a European Approach". In particular, it contributes to ensuring greater transparency on platforms' policies against fake profiles and disinformation. However, all measures adopted must respect and guarantee freedom of expression. Throughout the entire text, particular attention is paid to this fundamental right[35]. Specifically, the Code reads that "the Signatories are mindful of the fundamental right to freedom of expression and to an open Internet, and the delicate balance which any efforts to limit the spread and impact of otherwise

---

[30] The work of the HLEG results in the following report: *A multi-dimensional approach to disinformation. Report of the Independent High-Level Group on fake news and online disinformation*, Publication office of the European Union, Luxemburg, 2018, p. 5.

[31] *Ibid*., p. 35.

[32] European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Tackling Online Disinformation: a European Approach, 26 April 2018, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018DC0236, accessed on 3 December 2020.

[33] The text of the Code is available at the following link: https://ec.europa.eu/digital-single-market/en/code-practice-disinformation, accessed on 3 December 2020. In 2019, Facebook, Google, Mozilla, Twitter and trade associations representing the advertising sectors submitted their first reports on the measures taken to comply with the Code: *First results of the EU Code of Practice against disinformation*: https://ec.europa.eu/digital-single-market/en/news/first-results-eu-code-practice-against-disinformation?fbclid=IwAR3WQmydZDdMH6uiUGQPDyERTC_4oTik7dI3H31rDO7WsYq9-jKyBwYff4I, accessed on 3 December 2020.

[34] Self-regulation is defined as follows: "Self-regulation constitutes a type of voluntary initiative which enables economic operators, social partners, non-governmental organizations or associations to adopt common guidelines amongst themselves and for themselves. They are responsible for development, monitoring, compliance with and enforcement of those guidelines", in *The Sounding Board's Unanimous Final Opinion on the so-called Code of Practice*, 24 September 2018, https://www.beuc.eu/documents/files/3OpinionoftheSoundingboard.pdf, accessed on 3 December 2020.

[35] The right to freedom of expression is enshrined both in the Constitutions of democratic legal systems (e.g., art. 21 of the Italian Constitution) and in other supranational legal instruments, such as the Charter of Fundamental Rights of the European Union (art. 11), the European Convention on Human Rights (art. 10), the International Covenant on Civil and Political Rights (art. 19) and the Universal Declaration of Human Rights (art. 19).

lawful content must strike"[36]. The signatories of the Code also have to produce on a regular basis reports regarding the program for the monitoring and reporting of Covid-19, as well as, more recently, reports on the measures adopted to combat the spread of disinformation regarding Covid-19 vaccines.

In the context of the efforts made by the EU to combat online disinformation, we also find "The Action Plan Against Disinformation", published in December 2019[37]. The Action Plan is also aimed at monitoring the actions of the *big players* of the information market, such as Google, Facebook and Twitter[38] and to urge platforms to implement the self-regulatory Code of Practice and Disinformation. As set out in the Action Plan, the response to disinformation is based on four pillars: i) improving the capacities of European Union institutions to detect, analyze and expose disinformation; ii) strengthening coordinated and joint responses to disinformation; iii) mobilizing the private sector to tackle disinformation; iv) raising awareness and improving societal resilience[39]. It emphasizes the requirement for a coordinated response in the fight against fake news, as well as for increased international cooperation and the involvement of society as a whole to cooperate in such a fight (i.e., online platforms, fact checkers, public authorities, researchers and social society). The approach adopted in the Action Plan was also followed to counter the disinformation wave during the Covid-19 pandemic[40]. Indeed, it had harmful consequences for public health and effective crisis communications. The same still holds true with regards to the vaccination campaigns.

---

[36] This aspect was previously stressed in the Joint Declaration on Freedom of Expression and "Fake News", Disinformation and Propaganda signed on 3 March 2017 by the United Nations (UN) Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media, the Organization of American States (OAS) Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information.

[37] Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions. Action Plan Against Disinformation, 5 December 2018, https://ec.europa.eu/info/publications/action-plan-disinformation-commission-contribution-european-council-13-14-december-2018_en, accessed on 3 December 2020.

[38] The European Regulators Group for Audiovisual Medial Service (ERGA) plays a fundamental role in the monitoring activities related to the implementation of the commitments by the signatories of the Code of Practice Signatories. At the same time, it has to guarantee the media pluralism. For a detailed analysis of the role played by the ERGA: F. Sciacchitano, A. Panza, *Fake News e disinformazione online: misure internazionali*, in *Rivista di diritto dei media*, 1/2020, p. 118 ff.

[39] In the context of the Action plan against disinformation the European Digital Media Observatory (EDMO) was established. It was aimed at creating a European center for fact-checkers, academics and other relevant stakeholders with the purpose to: 1) map fact-checking organisations; 2) support and coordinate research activities; 3) build a public portal; 4) ensure secure and privacy-protected access to platforms' data; 5) support public authorities. It started its activities on 1 June 2020. For more information on its activities: https://edmo.eu, accessed on 3 December 2020.

[40] Joint Communication of the European Commission and the High Representative the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions. Tackling COVID-19 disinformation – getting the facts right (JOIN(2020) 8 final), 10 June 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020JC0008, accessed on 3 December 2020. This Communication focuses on the immediate response to disinformation around the coronavirus pandemic, responding to the Joint Statement of the Members of the European Council to resolutely counter disinformation of 26 March 2020, https://www.consilium.europa.eu/en/press/press-releases/2020/03/26/joint-statement-of-the-members-of-the-european-council-26-march-2020/, accessed on 3 December 2020.

The Commission particularly recalled the importance of combatting disinformation in the context of elections and in the democratic process in the European Democracy Action Plan (2 December 2020), which is built on three pillars: i) free and fair elections; ii) media freedom and pluralism; iii) fighting against disinformation[41].

Finally, the appeal for online intermediaries and platforms to take more responsibility for the content they host, as set out in the Digital Service Act[42], may also impact positively on the fight against the spread of fake news online.

V. The response of domestic legal systems

Measures aimed at countering the phenomenon under examination are widely debated throughout the world[43]. At domestic level, three different approaches can be identified.

The first approach is that of relying on existing law which regulates the use of traditional media, anti-defamation and elections in order to address the phenomenon. The problem of this approach is that relying on existing law, as it may be based on rules adopted in the pre-Internet era (e.g., Italy), may not be adequate. The second approach is that of adopting specific legislation which imposes sanctions on individuals and social media platforms who spread fake news. The countries that have adopted this approach relying on criminal law[44] include China[45], Malaysia[46],

---

[41] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. On the European Democracy Action Plan, 3 December 2020: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A 2020 %3A790%3AFIN&qid=1607079662423, accessed on 20 December 2021.

[42] The Digital Service Act and the Digital Markets Act are two legislative measures proposed by the European Commission and part of the European Digital Strategy, aimed also at creating a safer digital place where users' fundamental rights of digital services are protected. For more details: https://ec.europa.eu/digital-single-market/en/digital-services-act-package, accessed on 20 December 2020.

[43] For an overview: Report of the Library Congress Law, *Initiatives to counter fake news in selected countries*, April 2019, https://www.loc.gov/law/help/fake-news/index.php, accessed on 20 December 2020.

[44] For an overview: R.K. Helm, H. Nasu, *Regulatory Responses to 'Fake News' and Freedom of Expression: Normative and Empirical Evaluation*, in *Human Rights Law Review*, 2021, p. 21.

[45] In China the media environment is rigidly controlled. In 2015, art. 291 of the Penal Code of the People's Republic of China (PRC) was amended by the introduction of a criminal offense that punishes anyone who fabricates false information on dangerous situations, epidemics, disasters or alert situations, or intentionally disseminates such information by means of information networks or any other media, knowing that it is fabricated, and thereby seriously disturbing public order, with a penalty of up to three years of imprisonment. If the consequences are serious, the penalty varies from three to up to seven years imprisonment. The PRC Cybersecurity Law approved on 7 November 2016, which entered into force on 1 June 2017, further provides for the prohibition of fabricating or disseminating false information that may disrupt the economic or social order, also by means of social media. It also imposes several obligations on network operators (e.g., they have to monitor the content and, if it is found to be false, they have to record and report the information to the authority). For more details on the Chinese legislation, see: https://www.loc.gov/law/help/social-media-disinformation/china.php#_ftnref13, accessed on 20 December 2020. In August 2018, the Illegal and Unhealthy Information Reporting Centre, affiliated to the Cyberspace Administration of China, set up a platform that refutes rumors at national level. This platform relies on artificial intelligence to identify misinformation (http://www.piyao.org.cn/). For more details on the measures adopted by the Chinese government to reduce and minimize fake news during the Covid-19 pandemic: U.M.

Singapore[47] and Burkina Faso[48]. These countries have been criticized for having used such an instrument in order to control information and suppress freedom of expression[49]. During the Covid-19 pandemic, several States have also adopted criminal measures to counter the diffusion of fake news (e.g., Russia[50]).

The third approach is that of addressing the issue in a more general way by educating citizens about the danger of fake news and thus emphasizing the importance of media literacy (e.g., Finland[51]).

In Europe, the first European States that have adopted legislation against fake news are Germany and France. Therefore, the following sections will focus on these countries. Particular attention will be paid to the situation in Italy as it represents an important example on the difficulty of finding the ideal solution to countering the fake news phenomenon.

V.1. Germany

The Network Enforcement Act (in German *Netzwerkdurchsetzungsgesetz*, NetzDG)[52], also known as the Facebook Act, entered into force on 1 October 2017. The

---

Rodrigues, J. Xu, *Regulation of COVID-19 Fake News Infodemic in China and India*, in *Media International Australia*, 2020, p. 127 ff.

[46] The Anti-Fake News Act was published in the Federal Gazette of Malaysia on 11 April 2018, https://perma.cc/Y5H3-D6G8, accessed on 20 December 2020. However, it was repealed in 2019 https://perma.cc/VMT7-GAN4, accessed on 20 December 2020. The Act provided for the punishment with the imprisonment of up to six years and/or with a fine of up to five hundred thousand ringgit for anyone "who, by any means, knowingly creates, offers, publishes, prints, distributes, circulates or disseminates any fake news or publication containing fake news". For further details: A. Mazziotti di Celso, *Dal primo emendamento al bavaglio malese. Fake news, libertà di espressione e il rovesciamento delle categorie politiche tradizionali*, in *Rivista di Diritto dei Media*, 3/2018, p. 105 ff.; M. Monti, *Cronaca dell'emanazione e dell'abrogazione dell'Anti-Fake News Act malaysiano*, in *Rivista di Diritto dei Media*, 3/2018, p. 435 ff. The possibility of reviving the Anti-Fake News Act is under discussion of the Malaysia's Parliament: https://www.straitstimes.com/asia/se-asia/malaysia-to-discuss-the-revival-of-anti-fake-news-act-at-parliament, accessed on 20 December 2020.

[47] The Parliament passed the Protection from Online Falsehoods and Manipulation Act (POFMA) on 8 May 2019, which came into force on 2 October 2019, https://www.pofmaoffice.gov.sg/resources/, accessed on 20 December 2020. In particular, Part II relates to the "Prohibition of Communication of False Statement of Fact in Singapore". It provides for strict penalties. The text of the Act is available at the following link: https://sso.agc.gov.sg/Act/POFMA2019#pr7-, accessed on 20 December 2020.

[48] The Burkina Faso's Parliament with Loi N° 044-2019 amended the Penal Code (in particular artt. 313-12 ff.) by introducing specific offences related to the fight of fake news. For further details: https://www.assembleenationale.bf/IMG/pdf/loi_044_portant_modification_du_code_penal.pdf, accessed on 20 December 2020.

[49] T. Nagasako, *Global disinformation campaigns and legal challenges*, in *International Cybersecurity Law Review*, 1/2020, p. 135.

[50] In 2019, Russia passed two laws banning fake news and disrespects of authorities, providing for administrative sanctions. However, on 31 March 2020, art. 207 of the Russian Penal Code was amended in order to counter false information related to serious issues of public safety, such as Covid-19, https://ipi.media/new-fake-news-law-stifles-independent-reporting-in-russia-on-covid-19/, accessed on 20 December 2020.

[51] *Finland's Secret Weapon in the Fight against Fake News: its kindergarten children*, 16 February 2021, https://www.telegraph.co.uk/global-health/climate-and-people/finlands-secret-weapon-fight-against-fake-news-kindergarten/, accessed on 17 February 2021.

[52] Act to Improve Enforcement of the Law in Social Networks (Networks Enforcement Act), Bundestag, 17 July 2017. The text of the law is available in English at the following link: https://www.bmjv.de/

inadequacy of the self-regulatory mechanisms adopted by social media to counter illegal content online led to the establishment of this Act[53]. In order to define what must be considered "illegal content", more strictly related to fake news, the Act explicitly refers to some of the offenses endorsed in the penal code, which include defamation (§ 187 StGB), treasonous forgery (§ 100 a StGB) and the forgery of data of probative value (§ 269 StGB).

According to § 1 of the Act only applies "to telemedia service providers which, for profit-making purposes, operate Internet platforms which are designed to enable users to share any content with other users or to make such content available to the public", with more than two million registered users in Germany.

The Act imposes two types of obligations. Firstly, according to § 2, the provider of a social network that has received more than 100 complaints in a calendar year has to report, on a bi-annual basis, the complaints and the measures adopted in order to counter the illegal content on the platforms. This is required for reasons regarding public transparency and in order to determine whether the NetzDG is effective. Furthermore, on the basis of § 3, the provider of a social network has to handle complaints about unlawful content and follow the procedure provided by the provision (i.e., take note of and examine the complaint, remove or block access to unlawful content within a certain amount of time after receiving the complaint).

The violation of the obligations imposed by the NetzDG on social networks constitutes administrative offenses, punishable with a regulatory fine of up to five million euros (§ 4(2)). The peculiarity of the Act is that it can be applied even if the offense is not committed in the territory of the Federal Republic of Germany (§ 4(3)).

The NetzDG is not exempt from criticism[54]. The legal concerns relate in particular to the alleged limitation of the constitutional freedom of expression, the violation of the legality principle[55] and the contrast with the limits imposed by the E-Commerce Directive. The Act attributes excessive power to the platforms. The absence of an independent entity (e.g., a State authority) to control the content of information that is likely to be false could lead to private censorship, and thus jeopardize the right to freedom of expression. Moreover, the threat of applying such strict sanctions would lead to the risk that "suspicious" content would be removed if its reviewers had doubts about its veracity. The severity of the sanction poses some doubts also with regard to its effectivity administrative nature, as, substantially, it could be considered *matière pénale* as defined by the European Court of Human Rights (ECtHR)[56].

SharedDocs/Gesetzgebungsverfahren/Dokumente/NetzDG_engl.pdf;jsessionid=E54C7EC36D9B604A237AFF2CF2965C9C.2_cid289?__blob=publicationFile&v=2, accessed on 20 December 2020.

[53] V. Claussen, *Fighting Hate Speech and Fake News. The Network Enforcement Act (NetzDG) in Germany in the context of the European Legislation*, in *Rivista di diritto dei media*, 3/2018, p. 117.

[54] V. Claussen, *Fighting Hate Speech and Fake News. The Network Enforcement Act (NetzDG) in Germany in the context of the European Legislation*, in *Rivista di Diritto dei Media*, 3/2018, p. 119 ff.; M. Liesching, *Die Durchsetzung von Verfassungs- und Europarecht gegen das NetzDG: Überblick über die wesentlichen Kritikpunkte*, in *Multimedia und Recht*, 1/2018, p. 27; G. Spindler, *Der Regierungsentwurf zum Netzwerkdurchsetzungsgesetz – europarechtswidrig?*, in *Zeitschrift für Urheber- und Medienrecht*, 2017, p. 481.

[55] Claussen V., *Fighting Hate Speech and Fake News. The Network Enforcement Act (NetzDG) in Germany in the context of the European Legislation*, in *Rivista di Diritto dei Media*, 3/2018, p. 119 ff.

[56] T. Guerini T., *La tutela penale della libertà di manfestazione del pensiero nell'epoca delle fake news e delle infodemie*, in *discrimen.it*, 15 June 2020, fn. 73.

V.2. France

So far, France is the only European State to have adopted a penal legislation in order to combat fake news online. In 2018, France enacted the "Loi organique n° 2018-1201 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information" and the "Loi n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information", both related to the fight against the manipulation of information[57]. These laws were developed in order to better protect democracy and to adopt stricter rules to be applied to the media during the electoral campaigns, specifically in the three months before any election. Indeed, this period is considered especially delicate for the democracy of the country. According to Art. L163-1 of the Electoral Code, as modified by Loi n° 2018-1202, in the three months before the elections, platform operators have particular obligations concerning transparency, among which is the duty to provide users with "honest, clear and transparent content" regarding the identity of the natural person or the name of the company, the registered office and the purpose of the juridical person who pays to promote content related to a "debate of national interest". Violation of the provision is punishable with the penalty of up to one year of imprisonment and a fine of 75.000 euros[58].

Moreover, in the abovementioned period, a judge, upon request of a prosecutor, a candidate, a party, a political movement of anyone with an interest to act, may order "any proportional and necessary measure" to block the "deliberate, artificial and massive" dissemination of inexact allegations or imputations, or news that falsely report facts, with the intention of changing the genuineness of a vote[59]. The judge is required to decide within 48 hours. This aspect was criticized as such an evaluation would require more time and a deeper analysis, and would jeopardize the right to freedom of expression[60]. The legislative intervention is further criticized as it relates to specific circumstances and to a limited time frame. It only involves the political sphere and does not explore the broader context of the phenomenon examined.

V.3. Italy

In Italy, the debate related to the introduction of measures aimed at countering the creation, sharing and spreading of fake news on the Internet is a burning

---

[57] The text of the laws are respectively available at the following links: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000037847556 and https://www.legifrance.gouv.fr/jorf/id/ JORFTEXT000037847559/, accessed on 20 December 2021. For a detailed analysis: C. Magnani C., *Libertà d'informazione online e fake news: vera emergenza? Appunti sul contrasto alla disinformazione tra legislatori statali e politiche europee*, in *Forum di Quaderni Costituzionali*, 4 April 2019, p. 16 ff. It is also important to call attention to the 1881 Law on Freedom of the Press ("Loi du 29 juillet 1881 sur la liberté de la presse"), particularly art. 27 which punishes the publication, dissemination or reproduction of fake news in bad faith. Moreover, art. L.97 of the Electoral Code prohibits the dissemination of "fake news, defamatory rumors or other fraudulent schemes" that affect the result of an election. Another measure developed in France to address the phenomenon under evaluations is the Cross Check fact-checking project. For further details on the project: F. Sciacchitano, A. Panza, *Fake News e disinformazione online: misure internazionali*, in *Rivista di diritto dei media*, 1/2020, p. 128 ff.

[58] Art. L112 of the Electoral Code as modified by Loi n° 2018-1202.

[59] Art. L163-2 of the Electoral Code as modified by Loi n° 2018-1202.

[60] In this vein, the Syndacat National des Journalistes (SNJ) in the press release entitled: *"Fake news": un project de loi liberticide*: https://www.snj.fr/article/«-fake-news-»-un-projet-de-loi-liberticide-60222644, accessed on 20 December 2020. See also the decision of the Conseil constitutional: Decision n. 2018-773 DC 20 decembre 2018. In academic literature: E. Lehner, *Fake news e democrazia*, in *Rivista dei Media*, 1/2019, pp. 6-7.

issue[61]. The Italian legal order does not have specific legislation related to the fight against fake news online[62]. However, it does provide for several provisions dealing with, or which are in some way related to, fake news. Examples include: false corporate communications ("*false comunicazioni sociali*", art. 2621 of the Italian Civil Code), market manipulation ("*manipolazione del mercato*", art. 185 of the Consolidated Law on Financial Intermediation), which refers to "anyone who spreads false news"; political defeatism ("*disfattismo politico*", art. 265 of the Penal Code, hereinafter referred to as c.p.); fraudulent price fluctuation on the public market or on the stock exchange ("*rialzo e ribasso fraudolento di prezzi sul pubblico mercato o nelle borse di commercio*", art. 501 of the Penal Code, i.e. agiotage); publication or dissemination of false, exaggerated or biased news, likely to disrupt public order ("*pubblicazione o diffusione di notizie false, esagerate o tendenziose, atte a turbare l'ordine pubblico*", art. 656 c.p.)[63]; raising false alarm for authority ("*procurato allarme presso l'Autorità*", art. 658 c.p.)[64].

During the XVII Legislature, a number of legislative proposals were presented in order to address the fake news phenomenon[65]. Particular attention will be paid to the most relevant bills; the other initiatives will be only mentioned.

Before getting into the core of the analysis, it is important to recall what is stated in the Preamble of the Declaration of Internet Rights, elaborated by the Commission

---

[61] A bill (ddl n. 1900) on the establishment of a parliamentary committee of inquiry on the massive diffusion of fake news is under examination by the Senate. For more details see: http://www.senato.it/leg/18/BGT/Schede/Ddliter/53197.htm, accessed on 21 December 2020. A role in the fight against fake news is also played by the AGCOM ("*Autorità per le garanzie nelle comunicazioni*"). On the role played by the latter, see in particular: F. Sciacchitano, A. Panza, *Fake News e disinformazione online: misure internazionali*, in *Rivista di diritto dei media*, 1/2020, p. 102 ff. See also the task force set up by the Prime minister's office to counter the spread of fake news on Covid-19 on the web and social networks ("Unità di monitoraggio per il contrasto della diffusione delle fake news relative al Covid-19 sul web e sui social network"), https://informazioneeditoria.gov.it/it/notizie/unita-di-monitoraggio-per-il-contrasto-della-diffusione-di-fake-news-relative-al-covid-19-sul-web-e-sui-social-network-adottato-il-4-aprile-il-decreto-di-istituzione-presso-il-dipartimento/, accessed on 21 December 2020.

[62] Pointing out the inadequacy of our legal system to face the technological evolution and the phenomenon under examination: T. Guerini, *La tutela penale della libertà di manifestazione del pensiero nell'epoca delle fake news e delle infodemie*, in *discrimen.it*, 15 June 2020, p. 50; S. De Flammineis, *Diritto penale, beni giuridici collettivi nella sfida delle fake news: principio di offensività ed emergenze*, in *Sistema penale*, 6/2020, p. 137. In a broader perspective: L. Picotti, *Diritto penale e tecnologie informatiche: una visione d'insieme*, in A. Cadoppi, S. Canestrari, A. Manna, M. Papa (eds.), *Cybercrime*, Utet, Milano, 2019, p. 42; L. Picotti, *La tutela penale della persona e le nuove tecnologie dell'informazione*, in L. Picotti (ed.), *Tutela penale della persona e nuove tecnologie*, Cedam, Padova, 2013, p. 29 ff.

[63] A similar provision is contained also in art. 440 of the Romanian Penal Code.

[64] For a more detailed analysis of art. 656 c.p.: S. De Flammineis, *Diritto penale, beni giuridici collettivi nella sfida delle fake news: principio di offensività ed emergenze*, in *Sistema penale*, 6/2020, p. 134 ff. (according to the author, art. 656 c.p. represents the main criminal law instrument against this phenomenon in the protection of collective legal goods, p. 136).

[65] For an analysis of the different bills on the topic: T. Guerini, *Fake news e diritto penale. La manipolazione digitale del consenso nelle democrazie liberali*, Giappichelli, Torino, 2020, p. 168 ff.; P. Guercia, *I progetti di legge sulle fake news e la disciplina tedesca a confronto*, in A. Cadoppi, S. Canestrari, A. Manna, M. Papa (eds.), *Cybercrime*, Utet, Milano, 2019, pp. 1253-1271; A. Costantini, *Istanze di criminalizzazione delle fake news al confine tra tutela penale della verità e repressione del dissenso: verso un nuovo simbolismo penale?*, in *Rivista trimestrale di diritto penale contemporaneo*, 2/2019, p. 60 ff.; F. De Simone, *'Fake news', 'post truth', 'hate speech': nuovi fenomeni sociali alla prova del diritto penale*, in *Archivio penale*, 1/2018, p. 1 ff.

for Internet Rights and Duties and published in 2015. It reads that the Declaration "is founded on the full recognition of the liberty, equality, dignity and unique diversity of each individual. Preserving these rights is crucial to ensuring the democratic functioning of institutions and avoiding the domination of public and private powers that may lead to a society of surveillance, control and social selection. The Internet is an increasingly important space for the self-organization of individuals and groups, and it is a vital tool for promoting individual and collective participation in democratic processes as well as substantive equality"[66]. Such a Declaration is particularly important also with regards to the topic under examination as, whatever the means used to counter the fake news phenomenon – including criminal law – it is not possible to limit the right of the individual to freedom of expression, which constitutes a cornerstone of our democratic system.

V.3.1. The Gambaro bill

The Gambaro bill ("ddl Gambaro"), sponsored by senator Adele Gambaro, at the time a member of the Five Star Movement (M5S), was presented on 7 December 2017 ("Provisions to prevent the manipulation of online information, to ensure transparency on the web and to encourage media literacy")[67]. It represents the first attempt aimed at countering fake news and followed the Resolution 2143 (2017) "Online media and journalism: challenges and accountability", adopted by the Parliamentary Assembly of the Council of Europe on 25 January 2017[68]. The bill stems from the need to face the challenges presented by the technological developments and to regulate the individual's online life with the same guarantees ensured in the offline life[69]. Its aim was to make online platforms liable for the dissemination of news which is false, exaggerated, biased or which has a propensity to disrupt public order, as well as to introduce specific offenses for the authors of such news and for the dissemination of hate campaigns[70].

The bill under examination included three new offences in the Penal Code. More precisely, art. 1 of the ddl Gambaro provided for the introduction – after art. 656 c.p. – of art. 656 *bis* c.p. "Publication or dissemination of false, exaggerated or biased news likely to disrupt public order through IT platforms", ("*Pubblicazione o diffusione di*

---

[66] The text in English of the Declaration of Internet Rights is available at the following link: https://www.camera.it/application/xmanager/projects/leg17/commissione_internet/testo_definitivo_inglese.pdf, accessed on 21 December 2020. The Declaration is particularly important as it contains a number of provisions recognizing several rights to the users, such as the right to Internet access (art. 2), the right to online knowledge and education (art. 3), the right to one's identity (art. 9), the right to be forgotten (art. 11), the rights and safeguards of people on platforms (art. 12).

[67] Atto Senato n. 2688, XVII legislature (ddl Gambaro) "Disposizioni per prevenire la manipolazione dell'informazione online, garantire la trasparenza sul web ed incentivare l'alfabetizzazione mediatica". The text is available at the following link: http://www.senato.it/japp/bgt/showdoc/17/DDLPRES/0/1006504/index.html?part=ddlpres_ddlpres1-articolato_articolato1, accessed on 21 December 2020. The bill remained a "dead letter" as it was never discussed and it did not proceed in the parliamentary procedure.

[68] The text of the Resolution is available at the following link: https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=23455&lang=en, accessed on 21 December 2020.

[69] T. Guerini, *Fake news e diritto penale. La manipolazione digitale del consenso nelle democrazie liberali*, Giappichelli, Torino, 2020, p. 169. More in general: L. Picotti, *Diritto penale e tecnologie informatiche: una visione d'insieme*, in A. Cadoppi, S. Canestrari, A. Manna, M. Papa (eds.), *Cybercrime*, Utet, Milano, 2019, p. 42.

[70] M. Bassini, G.E. Vigevani, *Primi appunti su fake news e dintorni*, in *Rivista di diritto dei media*, 1/2017, p. 13.

notizie false, esagerate o tendenziose, atte a turbare l'ordine pubblico, attraverso piattaforme informatiche"), punishable with a fine of up to 5.000 euros[71]. This provision would not have been applied to professional journalism.

Art. 2 of the ddl Gambaro provided for the introduction respectively of art. 265 *bis* c.p. "Dissemination of false news that can raise public alarm or mislead sectors of public opinion", ("*Diffusione di notizie false che possono destare pubblico allarme o fuorviare settori dell'opinione pubblica*"), punishable with at least twelve months of imprisonment or a fine of up to 5.000 euros, and art. 265 *ter* c.p. "Dissemination of hate campaigns or campaigns aimed at undermining the democratic process", ("*Diffusione di campagne d'odio o volte a minare il processo democratico*"), punishable with at least two years of imprisonment or a fine of up to 10.000 euros[72]. However, the second part of art. 2 is more related to hate speech.

The bill further imposed a series of measures on IT platforms, such as registration requirements (art. 3), the obligation to rectify detrimental or fake content (art. 4) and the obligation to monitor online activity, determining the liability of the providers in the event that they did not remove unreliable and fake news (art. 7).

Finally, but equally importantly, the bill highlighted the importance of media literacy and the role played by schools within their functions of education and of encouraging public awareness (art. 6).

The bill faced fierce criticism for several reasons. It was criticized for violating the "principle of legality" (*principio di legalità*) and the "principle of offensivity" (*principio di offensività*)[73]. It jeopardized the right to freedom of expression as, for fear of punishment, the private individual would, firstly, have been discouraged from sharing his or her opinion and, furthermore, the platform would have further increased the controlling power[74]. This would have resulted in forms of private censorship. Such a

---

[71] With regard to the conduct, the offense endorsed in art. 656 *bis* c.p. seems to be very similar to the one contained in art. 656 c.p. with the exception of the means (IT platforms) required to carry out the conduct.

[72] These criminal offenses would have been introduced among the crimes against the personality of the State.

[73] T. Guerini, *Fake news e diritto penale. La manipolazione digitale del consenso nelle democrazie liberali*, Giappichelli, Torino, 2020, p. 172; E. Lehner, *Fake news e democrazia*, in *Rivista di diritto dei media*, 1/2019, p. 100; M. Fumo, *Bufale elettroniche, repressione penale e democrazia*, in *Rivista di diritto dei media*, 1/2018, p. 89; Cuniberti M., *Il contrasto alla disinformazione in rete tra logiche del mercato e (vecchie e nuove) velleità di controllo*, in *Rivista di diritto dei media*, 1/2017, p. 31. The bill lacks of a clear definition of "fake news".

[74] The "interventionist" spirit of the bill is highlighted by Guercia, in particular where he highlights the use of the term "control", adopted already in the bill's presentation report: P. Guercia, *I progetti di legge sulle fake news e la disciplina tedesca a confronto*, in A. Cadoppi, S. Canestrari, A. Manna, M. Papa (eds.), *Cybercrime*, Utet, Milan, 2019, p. 1258. Moreover, on p. 1259, the author points out the significance of the "chilling effect" according to which the ISP, for fear of incurring sanctions, could implement private censorship strategies and thus limit the circulation of information). More specifically on the "chilling effect": J. Townend, *Freedom of Expression and the Chilling Effect*, in H. Tumber, S. Waisbord (eds.), *The Routledge Companion to Media and Human Rights*, Routledge, 2017, pp. 73 ff. In the same vein: M. Bassini, G.E. Vigevani, *Primi appunti su fake news e dintorni*, in *Rivista di diritto dei media*, 1/2017, p. 20, the authors refer to the "collateral censorship" effect. More generally, on the "collateral censorship" effect: J. Balkin, *Free Speech and Hostile Environment*, in *Columbia Law Review*, 99/1999, p. 2295 ff. In the case law, *inter alia*: dissenting opinion of judge Sajó and judge Tsotsoria appended to the judgment of the Grand Chamber of the European Court for Human Rights (ECtHR) in the *Delfi v. Estonia* case, App. 64569/09, 16 June 2015. According to the judges, if the ISPs were obliged to remove content or were considered

strong duty of control would have been in contrast with the law provided at European Union level and, more particularly, with the E-Commerce directive[75]. The bill was further criticized for being a selective and partial legislation (e.g., it was not applicable to the journalists)[76] and for mixing problems related to the spreading of fake news and to hate speech[77].

V.3.2. The Zanda and Filippin bill

The Zanda and Filippin bill ("ddl Zanda and Filippin"), sponsored by senator Luigi Zanda and Rossana Filippin, members of the Democratic Party[78] "General rules on social networks and combatting the dissemination of illegal content and fake news on the Internet" ("Norme generali in materia di social network e per il contrasto della diffusione su internet di contenuti illeciti e delle fake news") was presented on 14 December 2017.

The bill was inspired by the model adopted in Germany ("NetzDG")[79]. It targeted only social networks with an elevated number of users, more than one million (art. 1(2)). In contrast to the ddl Gambaro, it did not introduce new criminal offenses, but relied on the existing provisions contained in the Penal Code. As pointed out in the bill's presentation, the aim of the law was to limit the publication and spread of content that constitutes crimes against the individual and crimes against the republic. Alongside the authors' criminal liability for the illicit content constituting one of the criminal offenses listed in art. 1 (e.g., stalking, defamation), the bill provided for the administrative liability (of an omissive nature) of the social network providers for not fulfilling the obligations endorsed in the bill's provisions. More precisely, art. 2 required the social network providers to adopt a very complex procedure with the

---

responsible for the content, for conditioned reflex they could implement strategies of private censorship for fear of penalties, which would probably have a negative effect on the circulation of information on the web.

[75] C. Magnani, *Libertà d'informazione online e fake news: vera emergenza? Appunti sul contrasto alla disinformazione tra legislatori statali e politiche europee*, in *Forum di quaderni costituzionali*, 4 April 2019, p. 4; F. Donati F., *Fake News e libertà d'informazione*, in *Rivista di diritto dei media*, 2/2018, p. 443 (the author goes even further stating that the bill constitutes a "surreptitious form of censorship"). In particular, art. 15 of the E-Commerce Directive 2001/31/EC does not impose a general obligation to monitor on ISPs. At domestic level, the legislative decree 70/2003 of 9 April 2003, implementing the EU E-Commerce Directive 2001/31/EC, establishes that the ISP does not have a general obligation to monitor information which is transmitted or stored, nor a general obligation to actively seek facts or circumstances indicating illegal activity (art. 16).

[76] C. Melzi D'Eril, *Fake news e responsabilità: paradigmi classici e tendenze incriminatrici*, in *Rivista di diritto dei media*, 1/2017, p. 62 (according to the author, if the aim of the bill is that of punishing the manipulation of the public opinion, the fact that the provision does not apply in the field of professional journalists seems inconsistent with the premise); M. Cuniberti M., *Il contrasto alla disinformazione in rete tra logiche del mercato e (vecchie e nuove) velleità di controllo*, in *Rivista di diritto dei media*, 1/2017, pp. 30-31.

[77] M. Bassini, G.E. Vigevani, *Primi appunti su fake news e dintorni*, in *Rivista di diritto dei media*, 1/2017, fn. 20.

[78] Atto Senato n. 3001, XVII legislature (ddl Zanda-Fillipin) "Norme generali in materia di social network e per il contrasto della diffusione su internet di contenuti illeciti e delle fake news". The text is available at the following link: http://www.senato.it/leg/17/BGT/Schede/Ddliter/48538.htm, accessed on 21 December 2020. For an analysis in academic literature: P. Guercia, *I progetti di legge sulle fake news e la disciplina tedesca a confronto*, in A. Cadoppi, S. Canestrari, A. Manna, M. Papa (eds.), *Cybercrime*, Utet, Milan, 2019, p. 1263 ff.

[79] *Supra*, para. 5.2.

aim of handling complaints and removing illicit content within a certain amount of time[80]. In case of violation of the obligations required by the bill, social network providers would have been sanctioned with a fine of up to five millions euros (art. 7).

This bill has also been the subject of criticism. More particularly, the quantitative requirement was criticized for at least two reasons: firstly, it is difficult to determine the exact number of users; secondly, the number of users does not seem to constitute a fundamental requirement as content could be shared and relaunched, and could jump from one platform to another, thus obtaining a level of dissemination with the potential to influence public opinion[81]. The bill was further criticized for leaving private subjects to determine whether a specific piece of content may constitute a crime[82]. This could have led to the implementation of private censorship strategies, which may have resulted in the limitation of the circulation of information[83]. This also holds true in light of the sanctions set out in the bill. It is notable how criticism that emerged against this bill is similar to the criticism of the Facebook act[84].

V.3.3. The De Girolamo bill

Although it does not strictly refer to fake news, it is important to at least mention bill n. 4692, "Introduction of the ban on the anonymous use of the Internet and provisions on the right to be forgotten" ("*Introduzione del divieto dell'uso anonimo della rete internet e disposizioni in materia di tutela del diritto all'oblio*")[85] presented by Nunzia De Girolamo and other parliamentarians of Forza Italia on 10 October 2017. The bill was aimed at adopting measures to combat online anonymity. It was composed of only two articles. The first article prohibited the uploading of online content of any kind anonymously and obliged all IT platforms to register users via username, password and e-mail address. The second was strictly related to the right to be forgotten, to its exercise and to the obligations imposed on the operators of search engines and websites related to the removal of certain content.

V.3.4. The red button

In 2018, around the time of the elections, the Italian Government launched an online service (named "red button") aimed at repressing and combatting the spread of

---

[80] The social network provider, which received more than 100 complaints in a calendar year, should have reported it on a bi-annual basis. Moreover, such a report should have been published in the official gazette and in the social network's homepage. See art. 4.

[81] F. De Simone, *'Fake news', 'post truth', 'hate speech': nuovi fenomeni sociali alla prova del diritto penale*, in *Archivio penale*, 1/2018, p. 18.

[82] T. Guerini, *Fake news e diritto penale. La manipolazione digitale del consenso nelle democrazie liberali*, Giappichelli, Torino, 2020, p. 175.

[83] P. Guercia, *I progetti di legge sulle fake news e la disciplina tedesca a confronto*, in A. Cadoppi, S. Canestrari, A. Manna, M. Papa (eds.), *Cybercrime*, Utet, Milano, 2019, p. 1263 ff. In this vein, see also: M. Monti, *La proposta del ddl Zanda-Filippin sul contrasto alle fake news sui social network: profili problematici*, in *diritticomparati.it*, 7 December 2017, https://www.diritticomparati.it/la-proposta-del-ddl-zanda-filippin-sul-contrasto-alle-fake-news-sui-social-network-profili-problematici/, accessed on 10 January 2021.

[84] *Supra*, para. 5.2.

[85] Camera dei deputati n. 4692, XVII legislature (ddl De Girolamo et al.) "*Introduzione del divieto dell'uso anonimo della rete internet e disposizioni in materia di tutela del diritto all'oblio*", the text of the bill is available at the following link: https://www.camera.it/leg17/126?tab=2&leg=17&idDocumento=4692&sede=&tipo= For a deep analysis: F. De Simone F., *'Fake news', 'post truth', 'hate speech': nuovi fenomeni sociali alla prova del diritto penale*, in *Archivio penale*, 1/2018, pp. 35 ff.

fake news[86]. This initiative was aimed at countering the proliferation of fake news, particularly during the electoral period. Indeed, as mentioned above, the spread of fake news is particularly common in periods such as this one.

This service allowed people to report the alleged fake news through the use of a red button on the website of the Postal and Communication Police. The task of verifying the warnings received through the reporting mechanism was assigned to a team of experts from the National Anti-Computer Crime Centre for Critical Infrastructure Protection" ("*Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche*", Cnaipic), within the Postal and Communications Police. In order to verify the information, the experts made use of specific fact-checking software and techniques[87]. If the information was found to be fake, the Postal and Communications Police would have had to demand that the platform withheld such content and give prominence to the denial on the website of the Postal and Communications Police, as well as on other institutional channels.

The criticism raised against the red button mechanism led to the closure of the page on the portal shortly after it had been activated. One point of criticism made against this mechanism related to the power attributed to the police and the adoption of such a simplistic solution to face a very thorny issue, which requires the balancing of different protected rights, one of which is the right to freedom of expression[88].

VI. The role of criminal law in the fight against the fake news phenomenon

Criminal law has a subsidiary character. It should be invoked as a last resort and thus when non-criminal measures have proven inadequate in tackling a specific phenomenon. The same holds true with regard to the fake news phenomenon.

The role of criminal law in the context under examination would not be that of safeguarding the truth of information itself, since false information and its spread per se are not relevant under criminal law[89]. In contrast, it would intervene to prevent the potential harm that false information and its diffusion may cause to protected legal goods of paramount importance, such as public order, safety and health[90].

---

[86] More information is available on the Government's website: https://www.interno.gov.it/it/notizie/progetto-red-button-contro-fake-news, accessed on 15 January 2021.

[87] Belonging in particular to the "Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche" (Cnaipic). For further details: P. Guercia, *I progetti di legge sulle fake news e la disciplina tedesca a confronto*, in A. Cadoppi, S. Canestrari, A. Manna, M. Papa (eds.), *Cybercrime*, Utet, Milano, 2019, p. 1268 ff.

[88] P. Guercia, *I progetti di legge sulle fake news e la disciplina tedesca a confronto*, in A. Cadoppi, S. Canestrari, A. Manna, M. Papa (eds.), *Cybercrime*, Utet, Milan, 2019, pp. 1269-1270; Magnani C., *Libertà d'informazione online e fake news: vera emergenza? Appunti sul contrasto alla disinformazione tra legislatori statali e politiche europee*, in *Forum di quaderni costituzionali*, 4 April 2019, p. 6. See also the Communication of the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression on the red button protocol, Mr. David Kaye, of 20 March 2018.

[89] *Supra*, para. 2.

[90] In this vein: P. Guercia, *I progetti di legge sulle fake news e la disciplina tedesca a confronto*, in A. Cadoppi, S. Canestrari, A. Manna, M. Papa (eds.), *Cybercrime*, Utet, Milano, 2019, p. 1256. Similarly: Melzi D'Eril C., *Fake news e responsabilità: paradigmi classici e tendenze incriminatrici*, in *Rivista di diritto dei media*, 1/2017, p. 64.

Criminal regulation should not be used widely. A regulation that is too strict would determine the chilling effect[91] and thus excessively limit the free flow of information. Moreover, the reliance on criminal law to counter the diffusion of fake news can be used neither as an excuse nor as a tool to violate the right to freedom of expression[92]. The choice to criminalize conduct inevitably requires a balance between fundamental rights and protected legal goods. However, when the spread of false information jeopardizes protected legal goods such as public order or public health, it seems likely that freedom of expression may (proportionately) be limited[93].

In the fight against the phenomenon of fake news, it is important to avoid using criminal law in a way that is merely symbolic[94] and that may weaken the specific function of this branch of law. This risk is particularly high in light of the fact that the fake news phenomenon is among the most widespread problems faced by the entire world, further increased by the spread of fake news about Covid-19 and, more recently, on vaccination campaigns. Criminal law could, therefore, be used inappropriately[95], as a tool to placate the widespread concerns of the majority, flowing into the so-called "penal populism"[96].

Another risk is that of anticipating excessively the intervention of criminal law[97]. This approach, for example, would have the effect of determining a merely symbolic intervention of criminal law[98].

What is of fundamental importance is to establish whether the spread of false or misleading information has a negative impact on the aforementioned legal goods. This

---

[91] *Supra*, fn. 74.

[92] This aspect is highlighted in: A. Costantini, *Istanze di criminalizzazione delle fake news al confine tra tutela penale della verità e repressione del dissenso: verso un nuovo simbolismo penale?*, in *Rivista trimestrale di diritto penale contemporaneo*, 2/2019, p. 76.

[93] This is particularly manifest with regard to the criminal offense provided in art. 656 of the Italian penal code. The prevalence of the protection of public order respect to the exercise of the right to freedom of expression has been highlighted also by the Italian Constitutional Court: Corte Cost., n. 19/1962, in *Giurisprudenza costituzionale*, 1962, p. 189 ff., annotated by Esposito, *La libertà di manifestazione del pensiero e l'ordine pubblico*. See also Corte Cost. n. 199/1972 and n. 210/1976. For a further analysis: S. De Flammineis, *Diritto penale, beni giuridici collettivi nella sfida delle fake news: principio di offensività ed emergenze*, in *Sistema penale*, 6/2020, p. 135 ff.

[94] On the symbolic use of criminal law: A. Manna, *Alcuni recenti esempi di legislazione penale compulsiva e di ricorrenti tentazioni circa l'utilizzazione di un diritto penale simbolico*, in *archiviodpc. dirittopenaleuomo.it*, 21 December 2016, pp. 7-13; S. Bonini, *Funzione "strumentale" e funzione "simbolica" del diritto penale, fra discorsività "critica" e discorsività "dialogica"*, in *archiviodpc. dirittopenaleuomo.it*, 21 December 2016, pp. 27-31.

[95] On the use of criminal law during the emergency period: S. De Flammineis, *Diritto penale, beni giuridici collettivi nella sfida delle fake news: principio di offensività ed emergenze*, in *Sistema penale*, 6/2020, pp. 138-139; R. Bartoli, *Il diritto penale dell'emergenza "a contrasto del coronavirus": problematiche e prospettive*, in *sistemapenale.it*, 24 April 2020, p. 1 ff.

[96] On this concept, *ex multis*: N. Selvaggi, *Populism and Criminal Justice in Italy*, in G. Delledonne, G. Martinico, M. Monti, F. Pacini (eds.), *Italian Populism and Constitutional Law. Challenges to Democracy in the 21th Century*, Palgrave, Macmillan, London, 2020, p. 291 ff.; M. Donini, *Populismo penale e ruolo del giurista*, in *sistemapenale.it*, 7 September 2020, p. 1 ff.; M. Donini, *Populismo e ragione pubblica. Il post-illuminismo penale tra lex e ius*, Mucchi, Modena, 2019; E. Amati, *Insorgenze populiste e diritto penale*, in *discrimen.it*, 3 June 2019, p. 1 ff.; G. Fiandaca, *Populismo politico e populismo giudiziario*, in *Criminalia*, 2013, p. 95 ff.; D. Pulitanò, *Populismi e penale. Sull'attuale situazione spirituale della giustizia penale*, in *Criminalia*, 2013, pp. 123-148; J. Pratt, *Penal populism*, 1st ed., Routledge, London, 2006.

[97] De Flammineis S., *Diritto penale, beni giuridici collettivi nella sfida delle fake news: principio di offensività ed emergenze*, in *Sistema penale*, 6/2020, p. 132 ff., p. 138.

[98] *Ibid*., pp. 144-145.

approach would contribute to further determining which fake news warrants intervention by means of criminal law and which does not. Particular attention must be paid to the threshold of harm and to the proportionality of the reaction. Indeed, the high level of interference determined by criminal law must be proportionate to the levels of threat and harm to the protected legal good[99]. Only in this case is the intervention of criminal law justifiable. For example, it appears reasonable to criminally punish an individual who intentionally or knowingly creates and spreads fake news that results in a public health crisis or in the incitement of violence that disrupts the legal order[100]. In this case, it is manifest how the diffusion of such information could provoke collective reactions, as well as distorted or even violent behavior. Furthermore, particular attention must be paid to the subjective element, as it is less plausible to assume that the unconscious spreading or sharing of false information should fall within criminal law.

In conclusion, in limited cases and circumstances, it would be possible to rely on criminal law. However, it cannot be ignored that this approach may pose some difficulties with regards to particular aspects, some of which are specifically related to the domestic legal system in which a criminal offense related to the creation and diffusion of fake news online has to be introduced. Firstly, it has to be coherent with the legal system in which the proposition is introduced. Moreover, the criminal offense should be determined with specific precision and, as mentioned above, the criminal sanction should be proportionate to both the legitimate aims pursued and the legal goods protected by the provision.

Criminal law is one of the instruments that could help to fight against the diffusion of fake news, but alone it is not sufficient to counter the phenomenon. Prevention plays a fundamental role in this battle. As was recently demonstrated in Finland, the educational aspect is fundamental to countering the spread of fake news. This aspect was emphasized at both supranational and national levels (e.g., Finland, ddl Gambaro). The promotion of critical media literacy is a key factor. It is a tool to empower citizens, to help them to critically understand and assess information divulgated by all types of media. This holds true in particular in an era characterized by the predominance of social media and the crisis of traditional media. Furthermore, it cannot be ignored that, in spite of being the principle means by which fake news is spread, social media plays a central role in both the prevention and repression of fake news. In light of this, given that the harmful consequences of fake news warrant multi-level action with the objective of limiting or reducing its negative impact on society –

---

[99] R.K. Helm, H. Nasu, *Regulatory Responses to 'Fake News' and Freedom of Expression: Normative and Empirical Evaluation*, in *Human Rights Law Review*, 2021, p. 23.

[100] In this vein: R.K. Helm, H. Nasu, *Regulatory Responses to 'Fake News' and Freedom of Expression: Normative and Empirical Evaluation*, in *Human Rights Law Review*, 2021, p. 23 ff. Similarly, but more specifically related to medical fake news: Mamak K., *Do we need the criminalization of medical fake news?*, in *Medicine, Health Care and Philosophy*, 2021, pp. 1-11. More specifically related to the Italian system: M. Fumo, *Bufale elettroniche, repressione penale e democrazia*, in *Rivista dei Media*, 1/2018, p. 90. Open to the possibility of relying on criminal law: De Flammineis S., *Diritto penale, beni giuridici collettivi nella sfida delle fake news: principio di offensività ed emergenze*, in *Sistema penale*, 6/2020, p. 144. *Contra:* A. Costantini, *Istanze di criminalizzazione delle fake news al confine tra tutela penale della verità e repressione del dissenso: verso un nuovo simbolismo penale?*, in *Rivista trimestrale di diritto penale contemporaneo*, 2/2019, pp. 76-77 (the author rejects the possibility of relying on criminal law mainly for two reasons: the potential limitation of the right to freedom of expression and the lack of effect of the reliance on criminal law in the limitation of the diffusion of fake news online).

including democratic political processes and values – social media is one of the indispensable players involved in such a fight.

References

1. Adinolfi M., *Hanno tutti ragione? Post-verità, fake news, big data e democrazia*, Salerno Editrice, Roma, 2019.

2. Amati E., *Insorgenze populiste e diritto penale*, in *discrimen.it*, 3 June 2019, pp. 1-34.

3. Balkin J., *Free Speech and Hostile Environment*, in *Columbia Law Review,* 1999, pp.2295-2320.

4. Bartoli R., *Il diritto penale dell'emergenza "a contrasto del coronavirus": problematiche e prospettive*, in *sistemapenale.it*, 24 April 2020, pp. 1-15.

5. Bassini M., Vigevani G.E., *Primi appunti su fake news e dintorni*, in *Rivista di diritto dei media*, 1/2017, pp. 11-22.

6. Bonini S., *Funzione "strumentale" e funzione "simbolica" del diritto penale, fra discorsività "critica" e discorsività "dialogica"*, in *archiviodpc.dirittopenaleuomo.it*, 21 December 2016, pp. 27-31.

7. Canfora L., *La storia falsa*, Rizzoli, Milano, 2008.

8. Caretti P., Cardone A., *Diritto dell'informazione e della comunicazione nell'era della convergenza*, Il Mulino, Bologna, 2019.

9. Casillo S., Di Trocchio F., Sica S., *Falsi giornalistici. Finti scoop e bufale quotidiane*, Alfredo Guida Editore, Napoli, 1997.

10. Claussen V., *Fighting Hate Speech and Fake News. The Network Enforcement Act (NetzDG) in Germany in the context of the European Legislation*, in *Rivista di diritto dei media*, 3/2018, pp. 110-136.

11. Costantini A., *Istanze di criminalizzazione delle fake news al confine tra tutela penale della verità e repressione del dissenso: verso un nuovo simbolismo penale?*, in *Rivista trimestrale di diritto penale contemporaneo*, 2/2019, pp. 60-80.

12. Cuniberti M., *Il contrasto alla disinformazione in rete tra logiche del mercato e (vecchie e nuove) velleità di controllo*, in *Rivista di diritto dei media*, 1/2017, pp. 26-40.

13. De Flammineis S., *Diritto penale, beni giuridici collettivi nella sfida delle fake news: principio di offensività ed emergenze*, in *Sistema penale*, 6/2020, pp. 131-146.

14. De Simone F., *'Fake news', 'post truth', 'hate speech': nuovi fenomeni sociali alla prova del diritto penale*, in *Archivio penale*, 1/2018, pp. 1-49.

15. Donati F., *Fake News e libertà d'informazione*, in *Rivista di diritto dei media*, 2/2018, pp. 440-446.

16. Donini M., *Populismo e ragione pubblica. Il post-illuminismo penale tra lex e ius*, Mucchi, Modena, 2019.

17. Donini M., *Populismo penale e ruolo del giurista*, in *sistemapenale.it*, 7 September 2020, pp. 1-22.

18. Fiandaca G., *Populismo politico e populismo giudiziario*, in *Criminalia*, 2013, pp. 95-121.

19. Fumo M., *Bufale elettroniche, repressione penale e democrazia*, in *Rivista di diritto dei media*, 1/2018, pp. 83-91.

20. Giusti S., Piras E. (eds.), *Democracy and Fake News: Information Manipulation and Post-Truth Politics*, Routledge, London, 2021.

21. Guercia P., *I progetti di legge sulle fake news e la disciplina tedesca a confronto*, in A. Cadoppi, S. Canestrari, A. Manna, M. Papa (eds.), *Cybercrime*, Utet, Milano, 2019, pp. 1253-1271.

22. Guerini T., *Fake news e diritto penale. La manipolazione digitale del consenso nelle democrazie liberali*, Giappichelli, Torino, 2020.

23. Guerini T., *La tutela penale della libertà di manifestazione del pensiero nell'epoca delle fake news e delle infodemie*, in *discrimen.it*, 15 June 2020, pp. 1-66

24. Helm R.K., Nasu H., *Regulatory Responses to 'Fake News' and Freedom of Expression: Noramative and Empirical Evaluation*, in *Human Rights Law Review*, 2021, pp. 1-21.

25. Lehner E., *Fake news e democrazia*, in *Rivista di diritto dei media*, 1/2019, pp. 93-122.

26. Liesching M., *Die Durchsetzung von Verfassungs- und Europarecht gegen das NetzDG: Überblick über die wesentlichen Kritikpunkte*, in *Multimedia und Recht*, 1/2018, pp. 26-30.

27. Magnani C., *Libertà d'informazione online e fake news: vera emergenza? Appunti sul contrasto alla disinformazione tra legislatori statali e politiche europee*, in *Forum di quaderni costituzionali*, 4 April 2019, pp. 1-29.

28. Mamak K., *Do we need the criminalization of medical fake news?*, in *Medicine, Health Care and Philosophy*, 2021, pp. 1-11.

29. Manna A., *Alcuni recenti esempi di legislazione penale compulsiva e di ricorrenti tentazioni circa l'utilizzazione di un diritto penale simbolico*, in *archiviodpc. dirittopenaleuomo.it*, 21 December 2016, pp. 7-13.

30. Marchetti G., *Le fake news e il ruolo degli algoritmi*, in *Rivista di diritto dei media*, 1/2020, pp. 29-36.

31. Mazziotti di Celso A., *Dal primo emendamento al bavaglio malese. Fake news, libertà di espressione e il rovesciamento delle categorie politiche tradizionali*, in *Rivista di diritto dei media*, 3/2018, pp. 90-109.

32. Melzi D'Eril C., *Fake news e responsabilità: paradigmi classici e tendenze incriminatrici*, in *Rivista di diritto dei media*, 1/2017, pp. 60-67.

33. Monti M., *Fake news e social network: la verità ai tempi di Facebook*, in *Rivista di diritto dei media*, 1/2017, pp. 79-90.

34. Monti M., *La proposta del ddl Zanda-Filippin sul contrasto alle fake news sui social network: profili problematici*, in *diritticomparati.it*, 7 December 2017.

35. Monti M., *Cronaca dell'emanazione e dell'abrogazione dell'Anti-Fake News Act malaysiano*, in *Rivista di diritto dei media*, 3/2018, pp. 435-438.

36. Monti M., *Italian Populism and Fake News on the Internet: A New Political Weapon in the Public Discourse*, in G. Delledonne, G. Martinico, M. Monti, F. Pacini (eds.), *Italian Populism and Constitutional Law. Challenges to Democracy in the 21th Century*, Palgrave, Macmillan, London, 2020, pp. 177-197.

37. Nagasako T., *Global disinformation campaigns and legal challenges*, in *International Cybersecurity Law Review*, 1/2020, pp. 125-136.

38. Paliero C.E., *La maschera e il volto. (Percezione sociale del crimine ed 'effetti penali' dei media)*, in *Rivista italiana di diritto e procedura penale*, 2/2006, pp. 467-538.

39. Pariser E., *The Filter Bubble: What the Internet is Hiding from You*, Penguin Group, London, 2011.

40. Perini C., *Fake news e post-verità tra diritto penale e politica criminale*, in *archiviodpc.dirittopenaleuomo.org*, 20 December 2017, pp. 1-14.

41. Perucchietti E., *Fake news. Dalla manipolazione dell'opinione pubblica alla post-verità. Come il potere controlla i media e fabbrica l'informazione per ottenere consenso*, Arianna Editrice, Bologna, 2018.

42. Picotti L., *La tutela penale della persona e le nuove tecnologie dell'informazione*, in L. Picotti (ed.), *Tutela penale della persona e nuove tecnologie*, Cedam, Padova, 2013, p. 29-75.

43. Picotti L., *Diritto penale e tecnologie informatiche: una visione d'insieme*, in A. Cadoppi, S. Canestrari, A. Manna, M. Papa (eds.), *Cybercrime*, Utet, Milano, 2019, pp. 33-95.

44. Pitruzzella G., Pollicino O., Quintarelli S., *Parole e potere. Libertà di espressione, hate speech e fake news*, Egea, Milano, 2017.

45. Pitruzzella G., *La libertà di informazione nell'era di Internet*, in *Rivista di diritto dei media*, 1/2018, pp. 19-47.

46. Pitruzzella G., Pollicino O., *Disinformation and Hate Speech: A European Constitutional Perspective*, Bocconi University Press, Milan, 2020.

47. Pratt J., *Penal populism*, 1st ed, Routledge, London, 2006.

48. Pulitanò D., *Populismi e penale. Sull'attuale situazione spirituale della giustizia penale*, in *Criminalia*, 2013, pp. 123-148.

49. Quattrociocchi W., Scala A., Sustein C. R., *Echo Chambers on Facebook*, in *papers.ssrn.com*, 13 June 2016.

50. Quattrociocchi W., Vicini A., *Misinformation: guida alla società dell'informazione e della credulità*, Franco Angeli, Milano, 2016.

51. Rodrigues U.M., Xu J., *Regulation of COVID-19 Fake News Infodemic in China and India*, in *Media International Australia*, 2020, pp. 125-131.

52. Safieddine F., *History of Fake News*, in F. Safieddine, Y. Ibrahim (eds.), *Fake News in an Era of Social Media: Tracking Viral Contagion*, Rowman & Littlefield International, London, New York, 2020.

53. Sciacchitano F., Panza A., *Fake News e disinformazione online: misure internazionali*, in *Rivista di diritto dei media*, 1/2020, pp. 104-105.

54. Selvaggi N., *Populism and Criminal Justice in Italy*, in G. Delledonne, G. Martinico, M. Monti, F. Pacini (eds.), *Italian Populism and Constitutional Law. Challenges to Democracy in the 21th Century*, Palgrave, Macmillan, London, 2020, pp. 291-310.

55. Spindler G., *Der Regierungsentwurf zum Netzwerkdurchsetzungsgesetz – europarechtswidrig?*, in *Zeitschrift für Urheber- und Medienrecht*, 2017, pp. 473-487.

56. Sumpter D., *Outnumbered: From Facebook and Google to Fake News and Filter-bubbles. The Algorithms that Control our Lives*, Bloomsbury, London, 2018.

57. Townend J., *Freedom of Expression and the Chilling Effect*, in H. Tumber, S. Waisbord (eds.), *The Routledge Companion to Media and Human Rights*, Routledge, London, 2017, pp. 73-82.

58. Van Wie Davis E., *Shadow Warfare: Cyberwar Policy in the United States, Russia, and China*, Rowman & Littlefield, London, 2021.

59. Zarocostas J., *How to Fight an Infodemic*, The Lancet, Vol. 395, February 2020.

60. Zhuk D., Tretiakov A., Gordeichuk A., Puchkovskaia A., *Methods to Identify Fake News in Social Media Using Artificial Intelligence Technologies*, in D.A. Alexandrov et al. (eds.) *Digital Transformation and Global Society*, Springer, 2018, pp. 446-454.

61. Ziccardi G., *Tecnologie per il potere. Come usare i social network in politica*, Raffaello Cortina Editore, Milano, 2019.

62. Zuiderveen Borgesius F.J., Trilling D., Möller J., Bodó B., De Vreese C.H., Helberg N., *Should we worry about filter bubbles?*, in *Internet Policy Review*, 2016, pp. 1-16.

New Technologies and Freedom of Expression with the Reference to the Case Law of European Court of Human Rights

Nikola Paunovic*

Abstract

The right to freedom of expression is one of the basic human rights guaranteed by the European Convention on Human Rights. However, it should be borne in mind that the inviolability of this right is not understood in an absolute sense. This Convention prescribes several grounds for restricting the right to freedom of expression, among which the interest in conducting criminal proceedings stands out. This is especially important in the context of new technologies, the Internet and accompanying social networks, where the right to freedom of expression is massively abused through the commission of criminal acts. Therefore, the paper starts from the basic presumption that the need to conduct criminal proceedings is a legitimate basis for restricting the right to freedom of expression. In this sense, the paper considers the case law of the European Court of Human Rights in cases related to Article 10 of the European Convention on Fundamental Rights and Freedoms, where the legitimacy of restrictions of the right to freedom of expression is raised. In the concluding remarks, it is pointed out that the restrictions of the right to freedom of expression for the purposes of conducting criminal proceedings may represent legitimate ground only with respect to the principles of necessity, proportionality and restrictiveness.

Keywords: *freedom of expression, human rights, new technologies, proportionality*

I. Introduction

Everyday use of information technology and the establishment of a lot of different social networks have created new opportunities for exercising freedom of expression in a virtual environment. Although the primary function of establishing social networks is useful and necessary in modern society as it encourages the exercise of freedom of expression and exchange of opinions among people around the world, in many cases it can be observed that individuals abuse this freedom by endangering the human rights of others. Bearing in mind that such conduct often leads to the criminal liability of individuals for actions taken in a virtual environment, it was necessary to establish limits on freedom of expression. In this sense, the main task is to establish a balance between freedom of expression and the interests of national security, which in certain cases requires the restriction of this freedom in order to conduct criminal proceedings. Freedom of expression and its restrictions in certain cases are

* Research Assistant, University of Belgrade, Faculty of law. Contact: dzoni925@gmail.com.

provided in the European Convention on Human Rights in Article 10 (hereinafter: the Convention)[1].

According to Article 10 of the Convention, everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. However, the exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary. Therefore, in the following lines, the cases from the practise of the European Court of Human Rights (hereinafter: the Court) concerning the application of Article 10 will be analyzed in order to examine the conditions under which the Court finds that the conditions for restricting freedom of expression are met[2].

II. Freedom of expression and electronic data

In the context of freedom of expression and electronic data evidence, a particularly interesting issue is the position of the Court in the case of balancing the interest of the investigation in providing evidence and the right of journalists to freedom of expression, especially in situations where evidence is collected and stored electronically. The following case deals with the abovementioned issue.

In Nagla v. Latvia case concerned the search by the police of a well-known broadcast journalist's home and seizure of data storage devices. The applicant's home was searched following a broadcast she had aired in February 2010 informing the public of an information leak from the State Revenue Service database. The applicant complained that the search of her home meant that she had been compelled to disclose information that had enabled a journalistic source to be identified, violating her right to receive and impart information. The Court held that there had been a violation of Article 10 of the Convention. It emphasised that the right of journalist's not to disclose their sources could not be considered a privilege, dependent on the lawfulness or unlawfulness of their sources, but rather as an intrinsic part of the right to information that should be treated with the utmost caution. In this case, the investigating authorities had failed to properly balance the interest of the investigation in securing evidence against the public interest in protecting the journalist's freedom of expression[3].

III. Freedom of expression and the use of internet as well as social networks

In the context of freedom of expression and the use of the Internet, a key issue concerns the credibility of information downloaded online. The question is whether

[1] European Convention on Human Rights, Council of Europe, 1950.

[2] European Court of Human Rights, Factsheet – New technologies, European Court of Human Rights, Strasbourg, 2020.

[3] Nagla v. Latvia, application no. 73469/10, Judgement 16 July 2013.

this type of information provides legal possibilities for further permitted distribution or it is not the case. On the other hand, when it comes to the relationship between the right to freedom of expression and the use of social networks, the basic issue concerns making a difference between posting and sharing content electronically that meets all requirements and distribution of offensive nature content. The following cases provide solutions to raised dilemmas.

The applicant company, owner and publisher of the Times newspaper, in the Times Newspapers Ltd v. the United Kingdom case alleged that the rule under United Kingdom law, whereby a new cause of action in libel proceedings accrues each time defamatory material on the Internet is accessed, constituted an unjustifiable and disproportionate restriction on its right to freedom of expression. In December 1999 the applicant newspaper published two articles that were allegedly defamatory of a private individual. Both articles were uploaded onto The Times' website on the same day as they were published in the paper version of the newspaper. During the subsequent libel proceedings against the applicant newspaper, it was required to add a notice to both articles in the Internet archive announcing that they were subject to libel litigation and were not to be reproduced or relied on without reference to the applicant company's legal department. In the judgment the Court underlined that, in the light of its accessibility and its capacity to store and communicate vast amounts of information, the Internet plays an important role in enhancing the public's access to news and facilitating the dissemination of information in general. In the present case, it found that there had been no violation of Article 10 of the Convention. Since the archives were managed by the newspaper itself and the domestic courts had not suggested that the articles be removed altogether, the requirement to add an appropriate qualification to the Internet version had not been disproportionate[4].

Editorial Board of Pravoye Delo and Shtekel v. Ukraine case mainly concerned the lack of adequate safeguards in Ukrainian law for journalists' use of information obtained from the Internet. In particular, defamation proceedings had been brought against a local newspaper and its editor-in-chief following their publication of a letter downloaded from the Internet alleging that senior local officials were corrupt and involved with the leaders of an organised criminal gang. The domestic courts ruled against the applicants and ordered them to publish an apology and pay 15,000 Ukrainian hryvnias, eventually waived via a friendly settlement. The Court held that the order to the editor-in-chief to apologise had not been done in accordance with the law, and had, therefore, been in violation of Article 10 of the Convention. It further held that there had been a violation of Article 10 because of the lack of adequate safeguards for journalists using information obtained from the Internet. Notably, "having regard to the role the Internet plays in the context of professional media activities ... and its importance for the exercise of the right to freedom of expression generally ..., the Court considered that the absence of a sufficient legal framework at the domestic level allowing journalists to use information obtained from the Internet without fear of incurring sanctions seriously hinders the exercise of the vital function of the press[5].

Delfi AS v. Estonia was the first case in which the Court had been called upon to examine a complaint about liability for user-generated comments on an Internet news

---

[4] Times Newspapers Ltd v. the United Kingdom (nos. 1 & 2), application *nos* 3002/03 and 23676/03, Judgement 10 March 2009.

[5] Editorial Board of Pravoye Delo and Shtekel v. Ukraine, application no.33014/05, Judgement 5 May 2011.

portal. The applicant company, which runs a news portal run on a commercial basis, complained that it had been held liable by the national courts for the offensive comments posted by its readers below one of its online news articles about a ferry company. At the request of the lawyers of the owner of the ferry company, the applicant company removed the offensive comments about six weeks after their publication. The Court held that there had been no violation of Article 10 of the Convention, finding that the Estonian courts' understanding of liability against the applicant company had been a justified and proportionate restriction on the portal's freedom of expression, in particular, because the comments in question had been extreme and had been posted in reaction to an article published by the applicant on its professionally managed news portal run on a commercial basis. The steps taken by the applicant to remove the offensive comments without delay after their publication had been insufficient and the 320 euro fine had by no means been excessive for the applicant, one of the largest Internet portals in Estonia[6].

Cengiz and Others v. Turkey case concerned the blocking of access to YouTube, a website enabling users to send, view and share videos. The applicants complained in particular of an infringement of their right to freedom to receive and impart information and ideas. The Court held that there had been a violation of Article 10 of the Convention, finding in particular that the applicants, all academics in different universities, had been prevented from accessing YouTube for a lengthy period of time and that, as active users, and having regard to the circumstances of the case, they could legitimately claim that the blocking order in question had affected their right to receive and impart information and ideas. The Court also observed that YouTube was a single platform which enabled information of specific interest, particularly on political and social matters. The Court further found that there was no provision in the law allowing the domestic courts to impose a blanket blocking order on access to the Internet, and in the present case to YouTube, on account of one of its contents[7].

Kalda v. Estonia case concerned a prisoner's complaint about the authorities' refusal to grant him access to three Internet websites, containing legal information, run by the State and by the Council of Europe. The applicant complained in particular that the ban under Estonian law on his accessing these specific websites had breached his right to receive information via the Internet and prevented him from carrying out legal research for court proceedings in which he was engaged. The Court held that there had been a violation of Article 10 of the Convention. It found in particular that contracting States are not obliged to grant prisoners access to Internet. However, if a State is willing to allow prisoners access, as is the case in Estonia, it has to give reasons for refusing access to specific sites. In the specific circumstances of the applicant's case, the reasons, namely the security and costs implications, for not allowing him access to the Internet sites in question had not been sufficient to justify the interference with his right to receive information. Notably, the authorities had already made security arrangements for prisoners' use of Internet via computers specially adapted for that purpose and under the supervision of the prison authorities and had borne the related costs. Indeed, the domestic courts had undertaken no detailed analysis as to the possible security risks of access to the three additional

[6] Delfi AS v. Estonia, application no. 64569/09 Judgement 16 June 2015.

[7] Cengiz and Others v. Turkey, application nos. 48226/10 and 14027/11, Judgement 1 December 2015.

websites in question, bearing in mind that they were run by an international organisation and by the State itself[8].

Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v. Hungary case concerned the liability of a self-regulatory body of Internet content providers and an Internet news portal for vulgar and offensive online comments posted on their websites following the publication of an opinion criticising the misleading business practices of two real estate websites. The applicants complained about the Hungarian courts' rulings against them, which had effectively obliged them to moderate the contents of comments made by readers on their websites, arguing that that had gone against the essence of free expression on the Internet.The Court held that there had been a violation of Article 10 of the Convention. It reiterated in particular that, although not publishers of comments in the traditional sense, Internet news portals had to, in principle, assume duties and responsibilities. However, the Court considered that the Hungarian courts, when deciding on the notion of liability in the applicants' case, had not carried out a proper balancing exercise between the competing rights involved, namely between the applicants' right to freedom of expression and the real estate websites' right to respect for its commercial reputation. Notably, the Hungarian authorities accepted at face value that the comments had been unlawful as being injurious to the reputation of the real estate websites[9].

Savva Terentyev v. Russia case concerned the applicant's conviction for inciting hatred after making insulting remarks about police officers in a comment under a blog post. The Court held that there had been a violation of Article 10 of the Convention. It found in particular that while the applicant's language had been offensive and shocking that alone was not enough to justify interfering with his right to freedom of expression. The domestic courts should have looked at the overall context of his comments, which had been a provocative attempt to express his anger at what he perceived to be police interference, rather than an actual call to physical violence against the police[10].

Magyar Jeti Zrt v. Hungary case concerned the applicant company being found liable for posting a hyperlink to an interview on YouTube which was later found to contain defamatory content. The applicant company complained that by finding it liable for posting the hyperlink onits website the domestic courts had unduly restricted its rights. The Court held that there had been a violation of Article 10 of the Convention. It underscored in particular the importance of hyperlinking for the smooth operation of the Internet and distinguished the use of hyperlinks from traditional publishing – hyperlinks directed people to available material rather than provided content. Updating its case-law on these issues, the Court set down elements which need to be considered under Article 10 when looking at whether posting a hyperlink could lead to liability and said that an individual assessment was necessary in each case. In the present case, the Court found that the Hungarian domestic law on objective liability for disseminating defamatory material had excluded the possibility of any meaningful assessment of the applicant company's right to freedom of expression in a situation where the courts should have scrutinised the issue carefully. Such objective liability for using a hyperlink could undermine the flow of information

[8] Kalda v. Estonia, application no. 17429/10, Judgement 19 January 2016.

[9] Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v. Hungary, application no. 22947/13, Judgement 2 February 2016.

[10] Savva Terentyev v. Russia, Application no. 10692/09, Judgement 28 August 2018.

on the Internet, dissuading article authors and publishers from using such links if they could not control the information they led to. That could have a chilling effect on freedom of expression on the Internet. The Court therefore found that, overall, the applicant company had suffered an undue restriction of its rights[11].

IV. Freedom of expression and smartphone applications

With regard to freedom of expression and the use of smart applications, a special issue concerns the limits of this right of individuals in the face of election events. In other words, the question is in which cases and for what purposes political parties can use smartphone applications. The following case can provide response to this question.

Magyar Kétfarkú Kutya Párt v. Hungary case concerned a political party's mobile application which allowed voters to photograph, anonymously upload and comment on invalid votes cast during a referendum on immigration in 2016. The applicant party complained about a violation of its rights under Article 10 of the Convention. The Grand Chamber found in particular that the provision of domestic election law relied on by the authorities, a breach of the principle of the exercise of rights in accordance with their purpose, had not allowed the applicant party to foresee that it could be penalized for providing such an app, which had been an exercise of its freedom of expression. It concluded that the considerable uncertainty about the potential effects of the provision had exceeded what was acceptable under the Convention and that the lack of sufficient precision in the law to rule out arbitrariness and allow the applicant party to regulate its conduct had led to a violation of Article 10 of the Convention[12].

V. Freedom of expression and secret tapping

When it comes to freedom of expression and secret tapping and monitoring, it should be pointed out that the basic issue is to establish a balance between the public interest which requires restriction of this right and freedom to express thoughts and ideas without interference by public authorities. The following two cases stressed out that problem.

Haldimann and Others v. Switzerland case concerned the conviction of four journalists for having recorded and broadcast an interview of a private insurance broker using a hidden camera, as part of a television documentary intended to denounce the misleading advice provided by insurance brokers. The applicants complained that their sentence to payment of fines had amounted to a disproportionate interference in their right to freedom of expression. In this case, the Court was for the first time called on to examine an application concerning the use of hidden cameras by journalists to provide public information on a subject of general interest, whereby the person filmed was targeted not in any personal capacity but as a representative of a particular professional category. The Court held that, in the applicants' case, there had been a violation of Article 10 (freedom of expression) of the Convention, considering in particular that the interference in the private life of the broker, who had turned down

[11] Magyar Jeti Zrt v. Hungary, application no. 11257/16, Judgement 4 December 2018.

[12] Magyar Kétfarkú Kutya Párt v. Hungary, application no. 201/17, Judgement 20 January 2020.

an opportunity to express his views on the interview in question, had not been serious enough to override the public interest in information on malpractice in the field of insurance brokerage. The Court further also asserted that the applicants deserved the benefit of the doubt in relation to their desire to observe the ethics of journalism as defined by Swiss law, citing the example of their limited use of the hidden camera[13].

Brambilla and Others v. Italy case concerned the conviction of three journalists who intercepted radio communications between carabinieri in order to arrive quickly at crime scenes and report on them for their local newspaper. The Court held that there had been no violation of Article 10 of the Convention. Stressing the notion of responsible journalism and noting that the decisions of the domestic courts had been duly reasoned and had focused primarily on the need to protect national security and prevent crime and disorder, the Court found in particular that the Italian courts had made an appropriate distinction between on the one hand the duty of the three journalists to comply with domestic law, which prohibited in general terms the interception by any persons of communications not addressed to them, including those of the law-enforcement agencies, and on the other hand the pursuit of their journalistic activities, which had not been restricted per se. The Court also noted that the penalties ordered by the domestic courts, consisting in the seizure of the radio equipment and the imposition of custodial sentences, had not been disproportionate, as the sentences of the three journalists had been suspended and the authorities had not prohibited them from bringing news items to the public's attention[14].

VI. Conclusion

The right to freedom of expression is guaranteed by Article 10 of the Convention as a basic human right related to the personal sphere of individuals. However, when it comes to the stated right, it should be borne in mind that it is not of an absolute nature, which is why its application does not apply in all cases. In that sense, regarding this freedom the Convention provides several restrictions that disable the absolute enjoyment of this right, as well as the conditions under which they are allowed. Precisely, restrictions of the right to freedom of expression are allowed under the following conditions. Firstly, the interference with the right to freedom of expression should be provided by law. Secondly, such restrictions should respect the fundamental substance of the rights of expression. Finally, the restrictions should represent a necessary and proportionate measure in a democratic society with the aim to prevent, investigate, detect or prosecute criminal offenses or execute criminal sanctions.

According to the case-law of the Court when restricting the right to freedom of expression, it should be taken into account the substance of given right, purpose of the restrictions, the nature and scope of the restriction and the relationship between the restriction and the purpose of the restriction as well. In other words, in cases concerning the application of Article 10 of the Convention, the right to freedom of expression may be limited under restrictive conditions, taking into account the principle of necessity in terms of the necessity of conducting criminal proceedings or protecting of national security, proportionality in terms of the goal to be achieved in a democratic society as well as restrictiveness in the sense that in this particular case

[13] Haldimann and Others v. Switzerland, application no. 21830/09, Judgement 24 February 2015.
[14] Brambilla and Others v. Italy, application no. 22567/09, Judgement 23 June 2016.

there is no other way to limit the rights of citizens. In this regard, it should be concluded that the restriction of the right to freedom of expression is possible under three conditions: a) for the purposes permitted by the Convention; b) to the extent necessary to satisfy these purposes in a democratic society and c) without interfering with the substance of the guaranteed right.

References

1. Brambilla and Others v. Italy, application no. 22567/09, Judgement 23 June 2016.
2. Cengiz and Others v. Turkey, application nos. 48226/10 and 14027/11, Judgement 1 December 2015.
3. Delfi AS v. Estonia, application no. 64569/09 Judgement 16 June 2015
4. Editorial Board of Pravoye Delo and Shtekel v. Ukraine, application no.3 3014/05, Judgement 5 May 2011.
5. European Convention on Human Rights, Council of Europe, 1950.
6. European Court of Human Rights, Factsheet – New technologies, European Court of Human Rights, Strasbourg, 2020.
7. Haldimann and Others v. Switzerland, application no. 21830/09, Judgement 24 February 2015.
8. Kalda v. Estonia, application no. 17429/10, Judgement 19 January 2016.
9. Magyar Jeti Zrt v. Hungary, application no. 11257/16, Judgement 4 December 2018.
10. Magyar Kétfarkú Kutya Párt v. Hungary, application no. 201/17, Judgement 20 January 2020.
11. Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v. Hungary, application no. 22947/13, Judgement 2 February 2016.
12. Nagla v. Latvia, application no. 73469/10, Judgement 16 July 2013.
13. Savva Terentyev v. Russia, application no. 10692/09, Judgement 28 August 2018.
14. Times Newspapers Ltd v. the United Kingdom (nos. 1 & 2), application nos 3002/03 and 23676/03, Judgement 10 March 2009.

Future Developments and Challenges in Criminalistics as Part of Criminal Justice

Fenyvesi Csaba*

Abstract

Cryptocurrencies are designed as a secure form of financial transaction via the Internet. However, the development of information and communication technology has created new space for their misuse in criminal purposes, especially in the area of money laundering and terrorist financing. Bearing in mind the complexity in conducting financial transactions via the Internet, the paper in the first part deals with most important legal challenges regarding the misuse of cryptocurrencies through money laundering and terrorist financing. Furthermore, in the second part of the paper, the most relevant crime detection methods are considered. Finally, the practical challenges at the level of the protection of financial This study analysis the futuring theoretical and practical development possibilities of criminalistics – as universal factscience. It tries to sign the further tendencies of forensic sciences in the XXI. century as well. The author composes scientific fields where can be and need to real, intentional strengthening of recent criminalistical methods and writes about his future guessing, suggestions and challanges of criminalistics.

Keywords: *criminalistics, developmental suggestions, scentmap, brainreader, identification, FISH, mobile lab, digital data, technical improvements.*

I. Introduction about the concept of criminalistics

First of all it is useful to give a meaning to the subject of our thesis, criminalistics. In this field the literature appears unified, as can be read below in our explanation; criminalistics is the mostly practical (and in some cases) theoretical doctrine of criminal and general investigation, the part of criminal sciences, which opens up to creates the detection (and prevention) of crimes, and the means and modes of proof adopting in certain legislation across the world. Besides effective crime prevention as a by-product, the basic function of criminalistics is the detection and collection of the most and authentic evidence in order to get the final aim; a legal (criminal) impeachment – avoiding any miscarriages of justice.

In short, criminalistics is the science of the effective, professional, law enforcement, which serves to combat against crime and purposes to bring the delinquents to trial.

Our study attempts to label the stages of development corresponding with the tendencies of XXI century. We have drafted from the scientific fields, within which progress in forensic methods is expectable and necessary, and we resume our surmise, developmental suggestions or future challenges of criminalistics.

* Professor, University of Pécs Faculty of Law Criminal and Civil Procedure Law Department. Contact: fenyvesi.csaba@ajk.pte.hu.

II. The discovery of human scent

A) People believe as fact, due to the reality regarding actual experiments of natural science, that after a few years or decades, we can receive the answer to the main forensic question – "Who committed the crime?" – through the scent left behind by the perpetrator.

The detection of the perpetrator who fled the crime scene based on following their scent may be valuable – largely because it rarely succeeds – even more valuable is the scent connected to the crime, or the perpetrator that is attached by posterior identification.

Currently this special forensic field; the odorology knows only one "instrument" for the identification and detection of scents. It is known as a "biodetective", and is none other than the dog.

The source of many problems is the animal itself, because it has no moral or legal responsibility.

It cannot report about its methodology of identification, therefore the control of the signs cannot be positive and could cause false consequences. The "biodetective" can be wrong when you regard the technical practice of the applying countries (e.g. Belgium, South-Africa, Netherlands, Poland, Germany, Romania, Slovakia and France since 2003), just as was shown in Hungary as well[1].

The researches into miscarriages of justice and past cases show, as well, the danger of possibly incorrect consequences and failure.

We have to highlight – when examining our best research – that nowadays there are no responsible control-tests, so without these examinations you can only note the correspondence and the failure of the dog. We recommend, the possibility of a validity test, because we ourselves can create the test scent and complete the controlling scent-identification. Until a better method is created, whether it is an independent method of science or criminalistics, one stronger than the dog, then experts should control and improve this available method, discover its credibility value, and undertake widespread testing on individuals.

B) As a fact for a progress in the methodology of scent identification we need transparent, clear, verifiable examining methods and individuals who could be responsible for their results. It bases on a research result that we don't know yet and also could be honored by a prestigious international award (as the Nobel-prize for instance): and this result could be the description of the structure of the human scent. In other words the modelling of the molecular structure of human scent. Just as researchers are willing to make the human genome map complete, it could be also desired to create the „scentmap" about the internal components of the human scent.

What kind of advantages could we earn from inventing a „scentmap" about the internal components of the human scent?

We surely admit that in the criminalistics it could gain an important identification, which is typify only one individual („scentfingerprint");

We could describe the clear, plain ingredients of an individual's scentmap and could be understood by anyone;

By years becomes obvious that we can talk about permanance or variability (based on ages) in the case of human scent;

---

[1] See more about it: Horváth, O. (2018), Kereső és azonosító kutyák kriminalisztikai alkalmazása. (Searching and identificating dogs in the criminalistcs.) Ph.D,-theses, Pécs, PTE ÁJK.

The experts of scent identification could perform his researches based on global standards (supervised, submitted by the Daubert-test as well);

The tests and results could be checked by controltests/controlresearchs;

The person expertised in scent identification also has responsibility (just like in case of the identification of fingerprints or DNA) and could be controlled in cross examination in the context of jurisdiction/administration of justice;

There will be a good chance, that the result will show or at least will be close to reality;

Could creat a result with strong validity, which could be used as evidence in the procedure and could reach its main aim, to avoid miscarriages of justice and to identify the actual perpetrators.

C) There are experiments to invent „fake noses" to apply in the health system, but these cannot solve the real problem, they just use them instead of the animals (dogs). A huge step could be the discovery of the scent's internal structure just as a material remain in the terms of criminalistics because it refers to the internal – unique structure. We know what is it made of, it's sources (continuously peeling epithelials from the surface of the skin, sweat, phlegm of sebaceous glad with various components of fat acid, but we don't know the components of it's mixture. Does it exist or not or is it possible to examine or describe it at all? The experts who do the main researches have to give us the answers to the previous questions. If the answer is no, then unfortunately we have to count on the irreplacable animals (as dogs, pigs, wasps, rats, mice) or the „fake noses" which replace the below mentioned animals for a long term.

III. Monoscanner („brainreader") instead of polygraph

A) The polygraph in the investigation (as an orienting part) and in the control of the detecting versions is similar to the dogs' scent identification, which is usually called as „lie examiner" or „truth examiner" by others. The way it works is when an individual says a not true statement there will be physiological mutations, so the potential perpetrators could be spotted and mapped. Also in some cases with the right tactical questioning we could get to answer one of the seven main questions of criminalistics. (Questions as where could we find the stolen object, the instrument of the perpetration for instance.)

Essentially and in general we have the knowledge that the examined individual did not tell the truth to one of the questions. However the method does not give any explanations about the reasons. Thus the result could and will be deformed, because there are a ton of irrespective (or coherent) reasons from the felony, why the questioned person did not tell the truth. (Previous personal positive or negative experiences, other individuals or in order to cover another feasance for instance.)

B) With this end in view our theoretical model has two main aims:

B/1. Spot and cut out the unknown deformations.

B/2. Collect appraisable data and information for criminalistics.

It will serve both, if we will not test the physiological phenomena by the individual who's under prosecution, then the memories and real thoughts that appears in the brain. So a body polygraph is less useful, than a „monoreader", a scanner totally focused on the brain. Only with the permission of the person who's under procedure and in an no-secret procedure –just like in the case of the polygraph – the authorities would have the chance to resort experts to read the signs and images of the brain meanwhile the

authorities question the person about general and concrete aspects of the felony. To succeed this result, the „only" need is to identify and explore the technique of reading and picturing the thoughts of our mind. No exaggeration, it could defenitely win a Nobel prize, like Paul C. Lauterbur did in 2003 for the invention of the installations of the magnetic resonance tomograph – fMRI – which could separate a piece from the brain in the resolution of 1,5 mm x 1,5 mm x 4 mm (similar to the size of a piece of rice) from a volume of 150 thousand size of these one single rice.

The fMRI by realizing the brain's use of oxygen, the amount of streaming blood could track the human decision-making process, reasoning, emotions, thus the truth-telling as well. First of all it's extremely expensive, but the main problem is the functioning of the brain cannot be seen or sensible neither the mental pictures appearing inside the brain, which would have a useful knowledge about the offender for the law enforcement and which could not be hidden or limited by the examined individual. It claims the invention of another high-impact, scientific instrument.

C) The advantages of the „monoscanner" – as we named it, or also called monoreader, brainreader[2];

a) The examined individual's brain (thoughts) – compared to the low source of material remains – are available in every single case.

b) The images appearing in the examined individual's brain – regarding to the nature of cerebration – could be less or not manipulated, which means there will be real pictures appearing in the brain, related to the felony by the questions at the actual perpetrator.

c) No guilty people would be scanned easier, because there will not appear pictures in their brain related to the felony (absent information). Even by any application for retrial would be possibly used posteriorly, if the instrumental resource and the scientific method reaches reliability in general. (Just like nowadays at the post-DNA identification.)

d) In context of the real images, there are chances of other efficient, proper, investigative acts. For example authorities could have house search at the place that appears on the brain-image, other individuals (other perpetrators, plaintiffs etc), objects related to the felony could be traced as well.

e) The real (criminal) brain-images (information present) – according to our point of view – are displayed, so by chance it could be printed as well (by „monoprinter" or „monophoto"), which could be a part of the evidence or criminal investigation/procedure.

IV. Other "honesty controlling" methods

A) Not only the mono-scanner or fMRI are the possible sources of detecting dishonesty and false statements in the future. The researches about this topic opened up that there is a possibility in the examination of eye-temperature to detect false statements by using/adopting a special eye-thermometer. This method brings a relation between the increase of metabolism of the eye and false statement, assuming that more blood flows into the iris and due to this effect the temperature of the eye increases, when the person lies.

[2] See more details: Fenyvesi, Cs. (2017) A kriminalisztikai tendenciái. (Tendencies of Criminalistics) Budapest, Dialóg Campus Kiadó.

The other method/instrument was invented in the United States as well, named as Psychological Stress Evaluator (PSE), which measures and graphs the components of human voice related to stress. The procedure based on two tones of the human voice – one is audible, the other is not. At the existence of human stress (which could be based on a lie) the PSE shows the non-sensible tones for the human ear. The scientific evaluation and control of the efficiency of the instrument is yet not extensive enough, but it's supporters think, the use is way easier than the polygraph's, even though it could be used indirectly through telephone conversation or record.

As a second option we need to mention the "thermal-cam" method throughout you can conclude the existence of honesty or dishonesty by the changes of body temperature. Based on a Hungarian experimentation 1/3 Celsius (0,3 – 0,4) grades are the differences in general between the temperatures measured on the reference points – as the middle of the forehead, under the left eye, under the right eye in the middle, middle of the lips, middle of the neck – between these points the most irrelevant difference was the temperature on the middle of the forehead (0,37 Celsius) and the most relevant was at the lips (0,47 Celsius). At the evaluation of this experiment experts draw the inference, that at some of the reference points, the general maximum temperatures are higher when the person is dishonest than the average temperatures at honest responses and the same difference was shown by the minimum temperatures.

On third place we mention the Layered Voice Analysis (LVA), which gives results about the honesty of the said statement or denial. The LVA was invented in 1977 and can sense the person's mental state, level of stress and its changes by the human speech and shows the cognitive processes going through the speaker, so the mental process of – observation, – remembrance, – information conversion could be detected.

Among the possible methods of the searching for the truth or the exploration of lies you can find processes related to graphology. Tamás AGÁRDI reports one of these methods[3]. The main point is that the expert does various statements just like in the polygraph tests and the person has to reply with –yes or – no answers. But this time the person has to draw a circle by "yes" and a square by "no". Through these experiments the tests show what the kind of suspicious signs appeared as the result of psychic lie, how is the unfeatured presentation of reality – just as elongated reaction time, vague marks, fractions or hesitancy. By the expression of the dishonest contents seems;

a) Ordinary writing changes, automatism is taken over by a complex process controlled on purpose,

b) Reaction time elongates,

The spontaneous, harmonic writing skills come apart, the dynamic stereotypes are loosing their priority; intense control is noticeable.

E)In searching for the truth, as it is mentioned in the D) point, there are further refinements needed in the field of grapho-researches. In this context we have to highlight the future possibilities in grapho-comparison, grapho-analysis and grapho-linguistics. All three handwriting researches based on the same source, which is the fact that handwriting is a personal-specified, learnt for a long term, stereotype activity, practiced permanently, which is a projection of someone's personality and inner side. Especially because as it is known since a long time, that the brain writes and not the hand. Comparison means the identification of handwriting and it's future possibilities will be detailed in the next point.

---

[3] Agárdi, T.-Kármán, G. (1999), A hazugságvizsgálatról más szemmel. (Lying examination – from other aspect.) *Belügyi Szemle,* vol. 10. 99-105.

In the aspect of the exploration of reality-untruth, we have to highlight that with the combination of these techniques could come into existence the so-called "three-probe procedure". It bases on once experts map out the handwriting criterias and system of specialities connected to the untruth, then they confer the questioned handwriting from the exact same person to a surely false and to a surely true handwriting sample and then they value by quantity and quality the matching/corresponding or distinct writing specialities. Through this procedure another type of polygraph (the known one based on speech and hearing) and this one would be based on handwriting, as the grapho-polygraph.

Besides the polygraph nature, the profiler nature could be discovered and used, because the grapho-linguistics and grapho-analysis could draw a conclusion about the writer's/author's sex, age, education (profession), illnesses (mental state) or deviance, but only as a possibility, not as a fact.

In a wide/broad meaning you will receive a profile, so it could be a so-called profiling, so grapho-profiling is basically a profile made out of handwriting. Its importance is mainly in the detection; in the identification of the possible suspects and in this context in the fomentation of setting up various possible versions, efficient investigation and in planning of secret service operations. Based on researches, the grapho-linguistics and grapho-analysis also aspire to hedge in with the most efficiency and possibility. In this endeavor in gracious cases they can count on special handwriting characteristics.

Besides the mentioned methods, a "double grapho-profiling" could be useful, when the results of grapho-linguistics and grapho-analysis show a coincidence. This type of "double-profiling" could be lead to a personal identification supplemented by any other technical featured handwriting research, not only by grapho-comparison. This is the reason why you can reckon on the development and refinement of this type of modus. In this pursuit the science of psychology has a major role by giving potent help to improve this field of criminalistics.

V. Techniques and possibilities in writing-identification

A) The grapho-cpmparison is more valuable than the grapho-analysis or grapho-linguistics because it gives specific/personal identification. This is the reason why these type of experiments and investigations need to receive more attention in the forensic detection. These are mostly techniques finished by criminalistics itself, therefore we can likely trust in them in the future as well. We find the most enticing the ones build on computers, special softwares and digital data. From these we see future opportunities and chances for development in the German FISH (Forensische Information-System Handschriften), which was started in 1988 and it works as a sorter and library system. There is a strong chance that having various on-going and intensive achievements in computer techniques and with its graduation the program will put on more minim information on the map and compare them in the writing identification, therefore the validity, possibility and credibility of modus will approach an even more closer level to reality.

B) Another similar computer based method is called graphometry. The computer based graphometry procedure starts with the digitalizing of the writing. It happens with the use of a scanner, camera or digitalizing tablet and continues with the screening of the "noises". The program registers static features (as figure, shape, extensity, position) and dynamic parameters (as pressure, speed, the position of the pen etc.) and measures through previously defined settings and resolution. After follows the processing by statistic methods, evaluation and decision-making. Its

greatest advantage is that the "text probability scales" can be changed by the level of significance and the certitude showed in numbers. The personal identification characteristics are definable and the possibility of matching with the incriminated writing is numerically expressive. Other progress could be the measurement and analysis of the frequency of some writing-characteristics/features in the population. With this method the strength of the value of each writing parameter could be definable. Regarding to this subject the authors, AGÁRDI – KÁRMÁN highlight the future chance to establish databases by the help of computerized graphometrial procedures, which opens up an automatic way by generating huge amount of data. By this method the establishment of computerized database based on handwriting will be in reachable proximity, which – with adequate searching and identifying functions – could be a new addition to the automatized personal identification systems[4].

C) From literature we know other promising experiments about the fields of writing-identification, so we have to point out the American CEDAR for first, which deals with the exploration and comparison and mostly diversion and not identification of handwritings objective, reproducible characteristics. Between the characteristics tested by forensic experts 21 was processed as algorithm and thru tests based on 1.500 people's handwriting sample, identified the source of the handwriting with a 98% efficiency and security, even though the program was invented to distinct handwritings and not for identification.

The Dutch development, the TRIGRAPH is the next one which based on pattern recognition and image processing. The modus tests some characteristics of the handwritten documents as the automatics, the writing hand-measured geometric characteristics and in the end the variants of letters.

VI. The future of mobile labs and DNA tests

A) Inspections are so called inevitable investigation actions in general, which expression refers to the "periculum in mora" situation; to the requirement of essential velocity. How could it be even more increased, how could make faster the quest, fixing and researches of traces and material remains? The answer is, you have to make shorter the way of "scene-lab-court" triangle in the future. The way how it is reachable, is we have to locate the lab into the scene. Bringing there the most important, mostly basic trace and material remain "searcher" tools. What are we thinking of: what options are close to reality in the near and further future?

In these days there are only a few crime-investigations that need no special expertise. In this way we can freely think and organize equipment (experts and special techniques) at the well-modeled crime scenes, just as homicides. The logistics of criminalistics could help to direct the powers, objects, tools and vehicles (vans and trucks e.g.) to the scene of special "mini-labs". In these mini-labs you could already find digital scanners, which could make the digital image of the trace, fixed at the scene and a high-efficiency computer could execute the database-comparison right there as well. The exact same procedure would happen to the DNA content of the material-remains (mostly blood, spit, sweat, sperm) – collected from the crime scene –

[4] Agárdi, T. (2003), Grafológia a nyomozásban, grafológiai hazugságvizsgálat. (Graphology in the investigation.) *Grafológia,* vol. 4. pp. 7-11.; Agárdi, T.-Kovács, Zs.-Hamperger A.-Holéczy, Zs.-Nemes, A. (2009), Alternatív hazugságvizsgálati módszer kifejlesztése. (Development of alternative polygraph.) Budapest, Közép-magyarországi Regionális Innovációs Ügynökség Innovációs Nagydíj pályázata

and after its examination the record-comparison could be accomplished. The inspection is not even done yet – all these examinations run during the procedure – and the perpetrator could be identified right at the crime scene. The identification of inner identity at the scene could be also useful, for example if different material remains belong to one person, or the distinction of the blood (material remain) of the victim and perpetrator. It could give a clear sight, helps to build up the right versions and to choose the adequate investigation action. Especially efficient in the detection of "white-powder" bio-weapons, when a possible virus could jeopardize not only the forensic investigator but the wider environment as well. In case of these types of public danger, the immediate bio-exam and the actuation of these mentioned "mini-labs" at the scene is almost inevitable[5].

B) Obviously there is a continuous development in the 1985 elaboration of DNA identification. This process will not stop and it is not hard to predict that other refinements are expected in the subsidiary utilization of genetic systems and technologies. The next generation technologies will fundamentally change the nature of DNA tests and not only with the localization to the scene – as mentioned in A).

We will discuss only a few from these.

B.a) The actual DNA "interrogating" materials apply automated gel tests (e.g. Hitachi FMBio, Molecular Dynamic Fluor-Imager, BioRad Multi-Imager) including tabular gel electrophoresis and the capillary electrophoresis systems as well. The further, new instruments would be expended to offer a way wider capacity than the actual ones.

B.b) The matrix-helped laser-absorbing mass spectrometria (MALDI-TOF MS) is an existing technology, which can finish genetic analysis in seconds. Thousands of analyses are done in one single day with the robotic sample-product and sample-loading. It could examine extremely small samples as well, with low expenses under its highly qualified leading.

The development of this technology leads to a possible chance of assaying bigger and bigger samples.

B.c) The nowadays used drained-capillary electrophoresis instruments (PE Biosystems 3700, Molecular Dynamics Mega BASE 1000) in the expensive cases with a wide database are based on the successive sample dosage, in which's number of channels an improvement is definitely expected.

B.d) The DNA identification and its significance/importance will be even more improved, because it will be possible to search for material remains – and its structure – inside traces. E.g. a blurred fingerprint could be perfectly able to fix material remains in it and to detect/determine the DNA content in the end.

To achieve this level we have to improve the making samples, pay special attention to the elaboration of cleaning techniques and the optimization of some type of material remains (male-female, animal-vegetal).

VII. The future of digital exploration/discovery

A) We can surely say, this field has a dynamic, bright future. Basically, there are no technical tools/materials in our environment, which have not been touched by any digital technology in some point, and this fact will not change. Contrarily, law enforcement have to permanently count on the fact that criminals will also use up the

[5] Belgrader, P.-Bennett, W.-Hadley, SD.-Richards, J.-Stratton, P.-Mariella, R.-Milanovichh, CH F (1999), PCR detection of bacteria in seven minutes. *Science,* volume, 284. 449-450.

advantages of digital technology, this involves to be aware of a "cyber war", so you have to unremittingly work on preceding, preventive, exploratory and evidentiary materials and credit the advantages of digital data (as second generation evidence).

For this general purpose, there is a need for unremitting digital data collection and updated/timely, wide registration where the data collection, ("Rasterfahndung" – in Germain), induction takes place with maximum output computers and programs by trained "digit-commando" and special subunits.

These systems have to be connected to other law enforcement officers' notebook stores as well. As an example, the British Police (PITO – Police Information Technology Organization) together with the NPIA developmental agency (National Policing Improvement Agency) works on the development of a monitoring system for the entire subway system in London, which could identify wanted persons by their faces. The base of this idea is establishing a huge multifunctional database. The cameras would have a direct contact with the police registration, so an immediate identification would be possible in this way.

The photos and it's criminal database/information for the identification would be available in mobile formats, so the police and detectives in service/on duty in the streets could reach the entire information, furthermore they would be provided by portable fingerprint-recognizers.

B) To reflect the past, digital-visual recording of accidents could be a perfect material in the exploration of the circumstances of traffic accidents, through a miniature video-camera, fixed in the margin of the upper windshield for example, in vehicles (automobiles, trucks or in any other hydraulic, aeronautic or vehicular vehicle), which after the electronic ignition records continuously – just like nowadays' lane-follower distronic system. The situation could be even luckier and more accurate/exact, if every single vehicle which were involved in the accident had this automatically or post-built in "eye-witness" systems and also "ear-witness" system as well, because voice/noise recording is possible too with these digital cameras, so the reconstruction of scenes would be more accurate and evident.

C) The never-ending international fight against 3D printers started in 2013 and it probably will not stop at its beginning. Law enforcement have to be aware of and be prepared against this way of weapon or explosive transportation. They have to work out the preventive, exploratory opportunities and special know-hows.

In this context we have to highlight the future requirement and challenge that the criminalists need to participate in effective, fast and on-going education (with priority) and in training, because there is no chance for a relief in cyber-crimes in the near future; they have to compete in knowledge against the other side; against the well-prepared criminals, who feel themselves home in the cyber-field. Only special rained expert groups will not be enough (certified forensic computer examiner) in the digital internet-war (network forensics), each "fighter" have to learn with accelerated "knowledge-transportation" the basic and most important cognitions about hardware – software – internet – media/data carries – PC properties and the preventive, – monitoring, – seizure, – investigational, – security materials and modus (computer aided investigative environment). In our point of view, these will be the main challenges in the next years and decades for the World's criminalist.

D) Beyond that criminalistics needs those highly certified computer hacking forensic investigators, who could do digital entering/invasion; who could help to map, detect the "digit" criminals, organizations, systems and at the same time are able to paralyse and stop their field.

We can prognosticate breach or at least further development and excursion in the way of personal categorized identification in the method of digital voice/sound identification. Nowadays, in spite of the unbelievably developed acoustic materials and technologies – will not be able to ensure number – "1"-value personal sound-identification. Following our presumption, the forensic acoustic "sound works" – using sound engineers scientific results – will configure a comforting, reassuring technique related to some records (just as phone messages, tape-dictaphone records and other digital messages).

E) A growth in the data of digital networks, which was not seen before is probable in the future, on one part because of the junction of international network and on the other part because of the flare of the applying of informatics – analytics systems and its international dissipation.

In the framework of cross-border police and forensic collaboration in favor of fighting against crimes, the junction of national data networks already exist in many fields. The junction is under a continuous and intensive expansion in some continents; let us just think about Interpol, Europol, Eurojust, OLAF, Eurodac and Schengen – System. This process will continue in the future – even if homogenization is not probable – by trying to build up standards on criteria in data-comparison.

We assume, that in the application of Geographical Information and Analysis System (GIS) the future center of the so called "crime – mapping" digital mapping will move to the side of totally computerized, almost automatically run, prognostic "hot spots" data analysis.

F) The use of higher level of digital technique is a requirement not only with the scenes related to computers, but also with traditional (classic) crimes (attack upon life and physical integrity of a person, robbery, sexual assaults) as well. It is necessary to have a strong quality camera – and tape records, which are able to reconstruct the scene by any competent criminalist or any other law enforcement personnel in the future and any other viewer could digitally imagine him or herself at the scene and observe. They can monitor/control sizes, distances, colors, the spatial position of traces and material remains and the finished exploration actions.

The innovation will not stop in the process of super-projection with having more precise digital scanners, cameras; the Forensic Face Reconstruction (FFR) will develop as well. The anatomy knowledge and data from autopsies and successful identifications gives a chance to make the FFR become a scientifically acceptable technique. For this aim, an objective method need to be processed, which always bring adequate, same results tested by other experts. Therefore materials as the computerized tomography, the magnetic resonance image, photogrammetry and leaser exams – which lead face-forming to another meticulous level – for example at the definition, modelling of eye-hair colors or chin-ear-lip shape will help a lot. Also, the computerized animation procedures will be extended to the face-reconstruction, therefore the model will be able to smile, laugh or talk on the screen in the future by changing the face's features. We believe also, that the brave idea of recognizing a face only by DNA in the future will be possible thanks to the fast-changing/developing science of DNA mapping.

VIII. Development of secret techniques

In our point of view, nowadays sensible valorization tendency in between secret powers-materials-methods will moreover continue, you can expect the broadening of applications and entering of methods. This forecast based on the development of

digital data – mentioned in point 6 – because the technical knowledge and material /base/ system behind it is in continuous progress; there are more sophisticated, more sensitive and even smaller micro-nano materials/tools available for secret monitoring and for making sound-and-photo records in stable-fixed places (as public – or private properties) or even in moving vehicles (just as in cars, trucks, airplanes, helicopters, ships etc.), and articles.

It is also true about materials of secret operations, which are under a continuous pressure of digital and online improvement in the virtual field of operative crime – interventional, crime –response and exploration activities. For example, new version of "spy-programs" with a positive aim need to be invented, produced to get with the powers against it[6].

IX. Further future developmental possibilities and suggestions

The most important parts were point 1-7, but now we sum up some fields where less change is expected, but improvements would be needed.

A) The institutional introduction of a forensic nursing – forensic nurse system (which works well in the English-speaking/anglo/common law countries) could be one of the changes, in the continent, especially in the Hungarian practice. It would be needed on one side for the interest of the plaintiffs, for the prevention and avoidance of secondary victimization, and on the other side because of criminal-tactical interests of fast and silent acquisition of testimonies.

The Bayes-analysis (which is also based on English speaking/anglo/common law countries' theoretical and practical results) supposes to have more attention, that gives an objective solution-model for handling insecurity in the valoration of mathematical feasibility in the continental – especially in the Hungarian law enforcement and jurisdiction – evidence, mainly the expert's opinions (and the guiltiness of the accused). It is time, that after Biology (in prediction of virus-spread, DNA-profile analysis, reconstructional eye-color modelling); Physics (in gravitational waves); Economics (in game-theory, in marketing as in the separation of products); Computer Science (as Google uses Bayes-filters for the unwanted letters); to appear in this field as well and be used/applied efficiently[7].

B) Profiling – also with English (American) origins, theory and praxis is used in a smaller circle, but with success – which is a person-identifying (better explained as a person-constrictor method) has to be developed as well. Profiling system needs to be deepen by giving more help and feedback to the criminalists to identify/constrict the circle of possible perpetrators. Knowing more data, details about the perpetrator/s, criminalists could set up a smaller group of possible perpetrators – and finally in the end – the one person, who actually committed the crime.

Forensic advices are also the technical improvement, the deeper, wider application of cognitive interviews. Especially for the clarification of testimonies. We cannot give up on the improvement, discovery and testing of further, new interrogation methods (just as PEACE, SUE, SAI).

---

[6] Mészáros, B. (2019) Fedett nyomozó alkalmazása a bűnüldözésben. (The covered agent during investigation.) Dialóg Campus Kiadó, Budapest.

[7] Orbán, J. (2018) Bayes-hálók a bűnügyekben. (Bayes-nets in criminal cases.) Ph.D-theses. Pécs, PTE ÁJK.

X. Conclusion

As being at the end of our study, we cannot finish without mentioning a noteworthy thought, that even if all of our prognosis become facts and if technique, digitalization, computer,-natural,-and social sciences get together, not even then could be exchangeable or replaceable the real key of the future's successful criminalistics; the criminalist him/herself.

He/she is the other focus besides identification. The expert, the explorer, the data collector, the effective detective, who takes risk and danger, who stands against continuous challenges, the crime-fighter in the never-ending real and virtual battlefield, where he/she only has one weapon in their hands: the criminalistics, as an "international treasure"[8].

References

1. Agárdi, T.-Kármán, G. (1999), A hazugságvizsgálatról más szemmel. *Belügyi Szemle,* vol. 10. pp. 99-105.

2. Agárdi, T. (2003), Grafológia a nyomozásban, grafológiai hazugságvizsgálat. *Grafológia,* vol. 4. pp. 7-11.

3. Agárdi, T.-Kovács, Zs.-Hamperger, A.-Holéczy, Zs.-Nemes, A. (2009), Alternatív hazugságvizsgálati módszer kifejlesztése. Budapest, Közép-magyarországi Regionális Innovációs Ügynökség Innovációs Nagydíj pályázata

4. Angyal, M. (2014), Ismeretlen személyazonosságú holttestek azonosítása. Ph.D-theses, Pécs, PTE ÁJK

5. Belgrader, P.-Bennett, W.-Hadley, SD.-Richards, J.-Stratton, P.-Mariella, R.-Milanovich F (1999), PCR detection of bacteria in seven minutes. *Science, volume,* 284. pp. 449-450.

6. Beveridge, W.I.B (1957), The Art of Scientific Investigation. New York, Random House.

7. Budaházi, Á. (2014), Poligráf. Műszeres vallomásellenőrzés bűnügyekben. Budapest, NKE Szolgáltató Kft.

8. Chauveau, L. (1993), Les traces du crime. Enquete sur la police scientifique. Calmann-Lévy.

9. Csernyikné Póth, Á. (2011), Svéd szakmai útibeszámoló. (kézirat-manuscript) Budapest, RTF, V. 30.

10. Elek, B. (2008), A vallomás befolyásolása a büntetőeljárásban. Debrecen, Tóth Kft. Debrecen.

11. Fejes, I. (2009),: Tendencies of Criminalistics Development in the 21th Century. In: *NBP Journal of Criminalistics and Law,* Beograd, Kriminalisticko-Policijska Akademia.

12. Fenyvesi, Cs. (2014, 2017), A kriminalisztika tendenciái. Budapest, Pécs, Dialóg Campus Kiadó.

13. Fenyvesi, Cs.-Herke, Cs.-Tremmel, F. (2004), Új magyar büntetőeljárás. Budapest-Pécs, Dialóg-Campus Kiadó, pp 210-230. and pp. 253-287.

[8] „The Forensic Sciences – An International Treasure." (President of American Academy of Forensic Sciences 2011): UBELAKER, D.H.: *The Forensic Sciences: International Perspectives, Global Vision.* Journal of Forensic Sciences. 2011/5. Volume 56. 1091.

14. Fischer, J. (1963), The Art of Detection. New York, Carlton Press.

15. Guyomare,'H, P.-Stephan, C.N (2012), The Validity of Ear Prediction Guidelines Used in Facial Appromixation. *Journal of Forensic Science,* Vol. 6. 57. pp. 1427-1441.

16. Hack, P. (2011): *Az igazságszolgáltatás kudarcai.* In: Fenyvesi, Cs. (ed.): A Magyar Büntetőjogi Társaság Jubileumi Tanulmánykötete. Budapest-Debrecen.-Pécs, MBT, pp. 35-45.

17. Handrik, A. (2011) A justizmordok okai – tévedési források a büntetőeljárásban. *Belügyi Szemle,* vol. 9. pp. 41-63

18. Hautzinger, Z. (2003), *Az emberi szagok kriminalisztikai azonosítása.* In: Fenyvesi, Cs.-Herke, Cs. (eds.): Emlékkönyv Vargha László egyetemi tanár születésének 90. évfordulójára. Pécs, PTE ÁJK, pp. 79-89.

19. Hautzinger, Z. (2005): The Present and the Future of Forensic Identification. Jurisprudencija, Volume 7, 99-105.

20. Hautzinger, Z. (2004), Az igazságügyi őszinteségvizsgálat. In: Korinek, L.-Kőhalmi, L.-Herke, Cs. (eds.): Emlékkönyv Irk Albert egyetemi tanár születésének 120. évfordulójára. Pécs, PTE-ÁJK

21. Hautzinger, Z.: Gondolatok a kriminalisztika elméleti rendszeréről. In Jura, 2019/1. 84-93.

22. Horváth, O. (2018), Kereső és azonosító kutyák kriminalisztikai alkalmazása. Ph.D-theses, Pécs, PTE ÁJK.

23. Ishii, M.-Yayama, K.-Motani, H.-Sakuma, A.-Yasjima, D.-Hayakawa, M.-Yamamoto, S.-Iwase, H. (2011), Application of Superimposition-Based Personal Identification Using Skull Computed Tomography Images. *Journal of Forensic Sciences,* vol.4. 56. pp. 960-966.

24. Katona, G. (2001), A kriminalisztika aktuális kérdései. Budapest, BM Kiadó,

25. Kármán, G.: Az objektivizálás korlátairól. *Grafológia*, 2001/11. pp. 5-15.

26. Kukuck, W.-Philipp, M. (1989), FISH – Das Forensische Information-System Handschriften. In: Stier, C.B. (ed.): Grundlagen, Methoden und Ergebnisse der forensischen Schriftuntersuchung. Lübeck, Festschrift für Lothal Michel. pp. 159-187.

27. Künzel, H. (1989), Die Erkennung von Personen anhand ihrer Stimme. *Neue Zeitschrift für Stafrecht.* vol. 9. pp. 400-405.

28. Lee, H.Y.-Park, M.J.-Kim, N.Y.-Yang, W.I-Shin, K.J. (2011), Rapid Direct PCR for ABO Blood Typing. *Journal of Forensic Sciences,* Volume 1. pp. 179-182.

29. Metenko, J.: Kriminalisticka taktika. Akadémia Policajného Zboru v Bratislave, Bratislava, 2012

30. Mészáros, B. (2019) Fedett nyomozó alkalmazása a bűnüldözésben. Dialóg Campus Kiadó, Budapest, 2019.

31. Nagy, F. (1980), A kriminalisztikai szövegnyelvészet. Budapest, Akadémiai Kiadó.

32. Orbán, J. (2018) Bayes-hálók a bűnügyekben. Ph.D-theses. Pécs, PTE ÁJK.

33. Póczos, E. (2006), A hazugságvizsgálat jövőképe. *Belügyi Szemle*, vol. 5.

34. Pophal, R (1949), Die Handschripft als Gehirnschrift. Greifen.

35. Rogers, M.-Seigfried, K (2003), The future of computer forensics: A needs analysis survey. *Computers and Security,* vol. 23. pp. 12-16.

36. Sheets, H.D.-Bush, P.J.-Bush, M.A. (2013), Patterns of Variation and Match Rates of the Anterior Biting Dentition: Characteristics of a Database of 3D Detentions. *Journal of Forensic Sciences, volume* 1. and 58. pp. 60-68.

37. Tancredi, L.R.– Brodie, J. D (2007), The Brain and Behavior: Limitations in the Legal Use of Functional Magnetic Resonance Imaging. *American Journal of Law Medicine.* vol. 2-3. szám.

38. Tremmel, F.-Fenyvesi, Cs.-Herke, Cs. (2005), Kriminalisztika. Tankönyv és Atlasz. Budapest-Pécs, Dialóg-Campus Kiadó.

39. Weedn:, V.W. (2000), Future Analitical Technique. In.: Siegel, J.A.-Saukko, P.J.-Knupfer, G.C.: Encyclopedia of Forensic Sciences 1-2-3, San Diego – San Francisco – New York – Boston – London – Sydney – Tokyo, Academic Press, II. volume, pp. 496-497.

40. Ubelaker, D.H. (2011), The Forensic Sciences: International Perspectives, Global Vision. *Journal of Forensic Sciences.* volume, 5., 56. p. 1091.

41. Vígh, A. (2007), A kriminalisztikai írásvizsgálatok alapjai. Budapest, Kriminalisztikai Jegyzetek és Tanulmányok, RTF, pp. 55-58.

42. Yasinac, A.-Erbacher, R.-Marks, D-Pollitt, M-Sommer, P. (2003), Computer forensics education. *IEEE Security and Privacy*. July-August, pp. 15-23.

43. Zlinszky, J. (1990), Római büntetőjog. Budapest, Tankönyvkiadó.

Online Hate Speech in the Time of the Covid-19 Crisis and Challenges for Serbian Criminal Justice System

Aleksandar R. Ivanović [*]

Abstract

The author presents the results of research on how young people from three multicultural regions of Serbia perceive hate speech on the Internet, as well as their experiences when it comes to hate speech on the Internet during the crisis with the COVID-19 virus. After that, analyzing the conclusions of the research conducted within the project " Combating discrimination, online hate speech and toxic narratives in multicultural regions of Serbia ", the author gives an overview of criminal law provisions that sanction hate speech in the Republic of Serbia, and then gives certain recommendations for amendments of criminal law with the aim to adequately respond to the current state of hate speech, with a special focus on online hate speech, and to provide adequate and equal protection for all groups that most often occur as victims of hate speech in Republic of Serbia.

Keywords: *online hate speech, criminal law, research, victims, protection.*

I. Introduction

This paper will first present the results of a project called "Combating discrimination, online hate speech and toxic narratives in multicultural regions of Serbia" which was implemented in Serbia from June until September 2020, and then, based on the analysis of these results, the challenges facing the criminal justice system of the Republic of Serbia when it comes to online hate speech will be pointed out with special focus on time of crisis with virus COVID-19.

The project "Combating discrimination, online hate speech and toxic narratives in multicultural regions of Serbia" was implemented by CSO MONITOR[1] from Novi Pazar

---

[*] Associate professor of Criminal law, Department for law sciences, International University of Novi Pazar, Republic of Serbia. Contact: a.ivanovic@uninp.edu.rs.

[1] Association of citizens MONITOR has been founded in March 2011, as a non-governmental non-profit association of citizens, which mission include the indication of current social problems and raising awareness of citizens about the same, as well as proposing concrete recommendations and directing social actions towards their resolution. Through its work, MONITOR strives to point out the current problems of the society from the field of human rights, security, culture, information and ecology by conducting research, monitoring and transparent presentation of the state of socio-economic and socio-political circumstances, relationships and processes, as well as by education of citizens raise awareness of the same, all in order to build the capacity of society to solve them. In previous three years MONITOR realize several projects which dealing with issues of hate speech, hate crimes, discrimination, extremism, nationalism, radicalism and human security. Association of citizens MONITOR operates in different parts of Serbia, through projects and activities. Most activities of Monitor for now are located in South-west part of Serbia. The focus of MONITOR is promoting

(Republic of Serbia), with the financial support of the European Union and the Council of Europe through their joint program "Horizontal Facility for the Western Balkans and Turkey 2019-2022". and a project within it entitled "Promotion of Diversity and Equality in Serbia". This project was created with the aim of combating the consequences that the COVID-19 virus pandemic had on already vulnerable groups in society. Within the project conducted research through anonymous questionnaires in which the project team sought to determine the existence of certain forms of hate speech and discrimination, patterns that appeared during the state of emergency and after the state of emergency, as well as young people's perception of these phenomena in which over 300 young people participated. Before we present results of conducted research we will first briefly explain background of this intervention.

Many of research before crisis with virus COVID-19 shows that there are presence of serious amount of online hate speech and toxic narratives based on of national, religious or racial belonging, and sexual orientation in the territory of Republic of Serbia. Considering the pronounced overlap of religious and national identities among the most represented social groups living in the territory of Serbia (Serbs-Orthodox, Hungarians-Catholics, Bosniaks-Muslims, Croats-Catholics, Albanians-Muslims…)[2], project team start from the assumption that the areas in who has the greatest concentration of these social groups (both majority and minority) will be most sensitive to the spread of hate speech and toxic narratives based on ethnical and religious belonging. The World Health Organization (WHO) declared a pandemic on March 11, 2020, and the state of emergency in Serbia was declared on March 15, 2020, and lasted until May 6, 2020. During the state of emergency, a number of human rights and freedoms were abolished or restricted (eg freedom of movement). This has had consequences for the enjoyment of numerous rights, and has particularly affected minority groups and encouraged the now desirable "distance" between people, which particularly affects members of minority groups. Even after the lifting of the state of emergency, numerous measures remain that restrict human rights and freedoms. The WHO has not declared an end to the COVID-19 virus pandemic, and it can be expected that, given the unforeseen circumstances, the reintroduction of restrictive measures, and one educational and research project could be very important to prevent future negative consequences for members of minority groups such as intolerance, discrimination and hate speech. The Internet is a suitable ground for such activities, as social distance is recommended and freedom of movement is restricted. Within educational part of the project team plan was to organize trainings for trainers who will in the future train other trainers. On this way a base is created for future work related to the prevention of hate speech on the Internet, which is a modern and "desirable" form of communication among young people. The state of emergency and restriction of freedom of movement have shown this in practice. Through the survey, project team tended to determine the consequences and patterns that occurred during

---

social, environmentally sustainable, multicultural, multinational and multiconfessional interaction in society. Its main office is located in Novi Pazar (www.monitor.org.rs).

[2] According to the 2011 census, Serbia has 7,186,862 inhabitants. By ethnicity, 5.988.093 (83.3%) of persons declared themselves Serbs, and another 20 ethnic communities has more than 2,000 members each (Hungarians 253,889 (3.52%), Roma 147,604 (2.05), Bosniaks 145,278 (2.02%), Croats 57,900 (0.81%), Slovaks 52,750 (0.73%), Montenegrins 38,527 (0.54%), Vlachs 35.330 (0.49%), Romanians 29.332 (0.41%), Yugoslavs 23.303 (0.32%), Macedonians 22.755 (0.32%), Muslims 22.301 (0.31%), Bulgarians 18.543 (0.26%), Bunjevci 16,706 (0.23%), Rusyns 12,246 (0.20%), Gorani 7,767 (0.11%) Albanians 5,809 (0.08%), Ukrainians 4,903 (0.07%), Germans 4,064 (0.06%), Slovenians 4.033 (0.06%), Others 17.558 (0.24%)).

the state of emergency and measures after the state of emergency regarding online hate speech and discrimination. Regarding to that, project team identified three areas (regions) in Serbia which are most diverse in national, ethnic and religious composition and where the concentration of inhabitants from biggest minority groups is highest. That are: Southwestern Serbia, South Serbia and North Serbia. When it comes to racially based hate speech, among almost all ethnic groups there is intolerance toward Roma population. According to the latest 2011 census, the Roma population in Serbia is mostly represented in the southern part of Serbia, where about 38.7% live, then in the northern part of Serbia (Vojvodina), where 28.7% live, Belgrade region (18.6%) and the region of central and southwestern Serbia where there are about 14%.

According to the aforementioned, the areas most suitable for appearance of hate speech and toxic narratives on Internet in Serbia are those areas where we have the largest concentration of different national and religious groups that have a long history of conflicts and numerous unresolved issues from the past with each other or with the majority (Serbian) ethnic group, as well as those areas where their motherland states is in the neighborhood. These are the territories of Southwestern Serbia, South Serbia and North Serbia. At the same time, these three regions of Serbia are the area's most populated by members of the Roma population. Also, these areas represent migrant routes and these areas have the highest number of migrant reception centers, which, after Roma population are most vulnerable to hate speech based on racial belonging (Ivanović & Soltvedt, 2020:73).

The problem addressed by this project is hate speech and toxic narratives on the Internet in certain local communities and regions of Serbia, with a particular focus on ethnic, religious and racial hatred. Namely, due to various unresolved problems from the past, although there are no open conflicts, there is a high level of hate speech in local electronic media and social networks in this region on ethnic, religious and political basis. Namely, hate speech and toxic narratives in local media and on social networks in this regions of Serbia (South Western, South Serbia and North Serbia) is very pronounced, perhaps more than in relation to the rest of Serbia. In this areas, there are numerous of local electronic media for which publicly does not know who stand behind, but on the basis of the reporting method, it can be concluded that they are close to some ethnic, religious or political options and are at the same time hostile to members of other ethnic, religious and shallow ones. Almost every local political option (mostly from minority groups) operating at the local level uses one or more electronic media to promote their ideas, and to make insults, and even direct discredit and threat to members of other political options. In these media, professional journalists are mostly not employed, which results in the fact that the news or texts that are published are not written in accordance with the ethical codex and standards of the journalistic profession (Ivanović, 2018:413). All of this has for result that often news at local electronic media as well as journal texts on these portals has been written in a way to contain hate speech or to encourage hate speech among its readers, according to members of a particular ethnic, religious, political group, or members of certain sexual orientation or fan groups. What makes the problem of hate speech and toxic narratives on local electronic media and on social networks makes it even more dangerous in this regions is the fact that there is lack of reaction of local officials, competent institutions, representatives of political parties, religious institutions, educational institutions, representatives of civil society etc. the appearance of this form of speech from hatred. This is a problem because the hate speech and toxic narratives at local electronic media and on social networks can represent a generator

of some future conflicts and discriminatory behaviors on a national, religious, political or any other basis, that is, the emergence and adoption of radical and extreme ideologies that promote the application of faith. This state of affairs is the result of above all the lack of will to discuss this problem, as well as to take action in terms of reducing of hate speech in local electronic media and on social networks, as well as the lack of knowledge among citizens, and above all young people, about causes of manifest forms, and the consequence of hate speech on these media, as well as the issues of legal regulation of these issues, referral mechanisms in charge of preventing and suppressing such phenomena.

II. Analysis of research results

The conducted survey within the project "Combating discrimination, online hate speech and toxic narratives in multicultural regions of Serbia" included 303 respondents, of which 110 (36.30%) were male and 193 (63.70%) were female. Participants were of the following age structure: one person (0.33%) was aged 10 to 15 years, 155 (51.16%) persons aged 15-25 years, 147 (48.51) aged 25 to 30 years. Regarding the geographical structure of the research participants, 126 respondents (29.04%) are from South and South-eastern Serbia, followed by 88 respondents (29.04%) from South-Western Serbia, while 89 participants (29.37%) from North Serbia participated.

When asked if they know what is meant by hate speech, 263 respondents (86.80%) answered in the affirmative, while 40 respondents (13.20%) answered in the negative. When asked to answer what is meant by hate speech, the respondents gave a wide range of different answers. For these answers, as well as for the answers about what discrimination is, the largest number of respondents gave incorrect or incomplete definitions of hate speech, and the conclusion is that it is necessary to organize additional trainings in order to introduce the younger population to the concept of hate speech and its manifestations, all with the aim of detecting and effectively suppressing hate speech.

By analyzing the given answers to question regarding source of their knowledge about hate speech, respondents stated that mostly of them have got their knowledge of hate speech over the Internet, more precisely, this option is marked by 101 (33,33%) of respondents, while 74 (24,42%) of respondents have chosen option that their knowledge about hate speech is mainly based on what they learned at school or university, or through their formal education, 61 (20,13%) of them marked option from newspapers or from television as the basis of their knowledge regarding this term. Personal experience as the basis for knowing about notion of hate speech is marked by 37 (12,21%), while only 30 (9,90%) of respondents tagged option that this knowledge have been acquired in some other way.

Also, on the base of given answers, we can see that half of the respondents know that the hate speech is sanctioned by national legislation, namely, 178 (58,75%) chose this option, while 125 (41,25%) of respondents declared themselves that hate speech is not sanctioned by national legislation. So, we can conclude that opinions on this issue are divided among respondents. Namely, around 58% stated that national legislation provides sanctions for hate speech, while 41% think that national legislation do not prescribes sanctions for this kind of behavior. When asked what are the key causes of

hate speech, two thirds of respondents (201 – 66.34%) answered in the affirmative, while one third of respondents (102 – 33.66%) answered in the negative. Respondents who stated that they know the key causes of hate speech, stated a large number of alleged causes (media, social networks, politicians, intolerance, (in) openness of society, insufficient education, but also religion, upbringing, jealousy and the environment). The most present answers were: media, social networks, politicians, intolerance and insufficient education (Stojanović, 2020:6). When asked whether they are familiar with the ways in which hate speech manifests itself on the Internet, 223 respondents (73.60%), therefore, almost three quarters of respondents answered in the affirmative, and 80 respondents (26.40%) answered in the negative. When asked whether it is justified to respond to hate speech with the same measure, 259 respondents (85.48%) answered in the negative, while 44 respondents (14.52%) answered in the affirmative. Looking at the regions, the answers of the respondents are almost identical – a significantly larger number of respondents are of the opinion that hate speech should not be answered with the same measure (Stojanović, 2020:8).

When asked whether since the beginning of the crisis caused by the COVID-19 virus pandemic, they felt insulted, injured, discriminated against with content on the Internet, 212 respondents (69.97%) answered that they did not, 38 respondents (12.54%) did, once, and 53 respondents (17.49%) answered yes several times. Regarding the answers on this question according regions, and focus groups situation is as follows:

Responses from participants from South and South Eastern Serbia

Offered answers	**Yes, once**	**Yes, several times**	**No**	**Sum**
Number of participants	17	19	90	126
Percentage	13,49	15,08	71,43	100

Responses from participants from South Western Serbia

Offered answers	**Yes, once**	**Yes, several times**	**No**	**Sum**
Number of participants	15	18	56	89
Percentage	16,85	20,22	62,92	100

Responses from participants from North Serbia

Offered answers	**Yes, once**	**Yes, several times**	**No**	**Sum**
Number of participants	6	16	66	88
Percentage	6,82	18,18	75	100

Responses from participants who belongs to Serbian nation

Offered answers	**Yes, once**	**Yes, several times**	**No**	**Sum**
Number of participants	24	35	154	303
Percentage	11,27	16,43	72,30	100

Responses from participants who belongs to national minorities

Offered answers	**Yes, once**	**Yes, several times**	**No**	**Sum**
Number of participants	32	32	129	193
Percentage	16,58	16,58	66,84	100

The results obtained in the survey, which refer to the fact that during the interaction on the Internet, 173 respondents (57.10%) out of 303 respondents witnessed a situation in which someone was attacked or harassed over the Internet, are worrying. Regarding the answers on this question according regions, and focus groups situation is as follows:

Responses from participants belonging to South and South Eastern Serbia

Offered answers	Yes	No	No answer	Sum
Number of participants	55	71	0	126
Percentage	43,65	56,35	0,00	100

Responses from participants belonging to South Western Serbia

Offered answers	Yes	No	No answer	Sum
Number of participants	56	33	0	89
Percentage	62,92	37,08	0,00	100

Responses from participants belonging to North Serbia

Offered answers	Yes	No	No answer	Sum
Number of participants	62	26	0	88
Percentage	70,45	29,55	0,00	100

Responses from participants belonging to Serbian nation

Offered answers	Yes	No	No answer	Sum
Number of participants	116	97	0	213
Percentage	54,46	29,55	0,00	100

Responses from participants belonging to national minorities

Offered answers	Yes	No	No answer	Sum
Number of participants	52	33	0	85
Percentage	61,18	38,82	0,00	100

A particularly high percentage was recorded in the south-west regions (62.92%), namely 56 out of 89 respondents and north 62 (70.45%) out of 88 respondents. Also, more than half of the affirmative answers regarding the fact that they witnessed a situation of attack or harassment over the Internet were recorded among the majority Serb population, as well as among members of national minorities, but also among members of both sexes.

Regarding the manner in which the abuse was committed, the largest number of respondents, as many as 192 (63.37%), responded to the abuse committed by pronouncing and naming a person with derogatory names due to some specific trait or affiliation. Respondents in all these regions listed this form of abuse as the most common, with 64 (73.73%) out of 88 respondents in the North region listing this form of abuse as the most common, as well as 61 (68.54%) out of 89 respondents from the South-West region.

By analyzing the affiliation of the group on which these harassments were based, the largest number of respondents stated national or ethnic affiliation – 42.90% of respondents, followed by political affiliation 38.61%, religion 37.95%, sexual orientation 29,70%, and sex 19,47%.

When asked whether they were victims of hate speech on the Internet or a social network, 35 respondents (11.74%) gave an affirmative answer, while 236 (88.26%) respondents gave a negative answer. Based on the answers related to group affiliation on which online hate speech addressed them was based on we can see that 39 (12,87%) cases they were victims of the hate speech on the religious basis, then 32 (10,56%) cases were marked hatred on political affiliation, 12 (8,25%) cases were marked hatred for ethnic or national grounds and 10 (3,30%) cases hatred for sex and 8 (2,64%) cases were marked hatred for age range, 6 (1,98%) cases hatred because sexual orientation, and 5 (1,65%) cases because gender identity. Here, looking at regions, ethnicity and gender, there were no discrepancies in the answers given.

When asked whether, in the opinion of the respondents, the reaction of society and responsible state bodies to hate speech on the electronic media and on social networks in the local community in which they live is adequate, the statistical data are also worrying. Thus, according to only 11 respondents – 11 (3.69%), the reaction is adequate, while according to as many as 164 respondents (54.36%) it is not. As a partially adequate reaction of the society, 94 respondents (31.54%) recognized it, and 31 respondents (10.40%) believe that it is mostly adequate. Also, no major discrepancies in the answers of the respondents were recorded either by regions, or by the national and gender structure of the respondents.

When asked whether the method of reporting online hate speech, only one third of the respondents answered in the affirmative – 100 (33.56%), while two thirds of the respondents stated that they did not know – 198 (66.44%). Here, too, looking at regions, ethnicity and gender, there were no discrepancies in the answers given.

When asked immediately after the question whether they know how to report hate speech online, and referred to whom they would report a case of hate speech on social networks, the results nominally showed that respondents do not know how to report hate speech. Thus, almost three quarters of the respondents answered that they did not know – 217 (72.82%), while only 81 respondents (27.18%) answered that they knew. Those who responded to know who to report to also cited a wide range of entities – portals and social network administrators, the Equality Commissioner, the Press Council, SOS state and non-state telephones (without specifying which telephones are and who provides such assistance), civil society organizations, and to a lesser extent the police and the judiciary. The school psychologist was mentioned among the answers. Based on the analysis of the given answers, it is clear that young people are generally aware, at least in small numbers, that there are types of reporting hate speech, but without a clearly defined way of reporting and sanctioning, as well as not knowing the competencies of the authorities (Stojanović, 2020:12).

Based on the data processed, in accordance with the assumptions set by the project team, as well as the goals defined by the project, we make the following conclusions regarding the processed data:

1) More than 10% of respondents do not know meaning of notion hate speech. Also, respondents are not fully aware of the meaning of hate speech. Namely, although 86,80% of respondents answered to this question positively, when it comes to defining hate speech, the processed data show that its meaning is not clearly familiar to the respondents. Namely, to question number where from participants were asked to describe by their own words meaning of hate speech, we can see that most of them (approximately 60% of them) hate speech define through notions such as nationalism, racism, discrimination, threats, insults, mostly identifying hate speech with the meaning of these terms. And that most of them do not identifying in its definition of

hate speech hatred motive because of some personal character or affiliation of person. Also, very small numbers of them mention in his description that hate speech encourages, promotes, or justifies intolerance, discrimination and hostility towards a member of another race, gender, sexual orientation, origin and other personal belonging of an individual or group. Also there is no offered definition by respondents according to which hate speech include communications that foster climate of prejudice and intolerance which may fuel discrimination, hostility and violent attacks later on. Because of everything foregoing mentioned we can conclude that the majority of the respondents are not familiar clearly with truly meaning of the term hate speech.

Also, we can conclude that among the half of respondents knowledge regarding hate speech is mainly based on information from the Internet, that is, information from the media, because about 50% of the respondents stated Internet, newspapers or televisions as a source of their knowledge of hate speech. In addition to that, 41% of respondents think that hate speech is not sanctioned by national legislation.

From results of survey we can conclude that 85,48% do not justifying responding on hate speech with the same measure. However, 14,52% of the respondents think that such response is justified.

2) Also, we can conclude that around 30% of respondents felt offended, insulted or discriminated due to some Internet content once or several time during crisis caused by the COVID-19. Besides that, 57% of the participants were witnesses of a situation in which someone else was assaulted or harassed over the Internet on some basis. From this number of respondents 63,37% participants stated that they were mostly witnesses of online insults, which were manifested in the calling and naming of a person with offensive names because of some personal property or some affiliation, while 21,12% of them answered that they were witnesses of online threatening by a physical attack on life and body to some other person, and 15,51% sexual harassment.

3) On the basis of the results of survey we can see that 42,90% of participants were the witnesses of cases where someone was victim of hate speech based on national or ethnic affiliation, and 38,61% hatred because political belonging and 37,95% religious belonging, 29,70% sexual orientation, and 19,47% sex.

4) Based on the results of survey we can see that 88,26% of the participants were not victims of hate speech on the Internet or social networks. Those who were victims of hate speech on the Internet stated that those speeches were based on hatred towards religious (12,87%), political belonging (10,56%), national affiliation (8,25%), sex (2,64%), sexual orientation (1,98%), and gender identity (1,65%).

5) Around half of respondents think that reaction of state authorities on the presence of hate speech on electronic media and on social networks in their local communities is inadequate. Also, more than a half or precisely 72,81% of respondents do not know to whom can be reported hate speech.

6) The processed data tells us even though they were not directly victims of hate speech, almost half of respondents met with hate speech on the Internet, i.e. with the situation that they were witnesses of such situation, or situation in which someone was offended, insulted, discriminated mainly based on religious affiliation, sexual orientation, national or ethnic and political affiliation. At the end, we can say that respondents are only in general aware of the meaning of the notion of hate speech, that they do not have a clear idea of the detailed meaning of this term, as well as the elements of hate speech and concrete forms of the expression of the hate speech on the Internet.

III. Criminal law sanctioning of hate speech on the Internet in the Republic of Serbia

Criminal Code of the Republic of Serbia[3] Article 317 prescribes the criminal offense of Instigating National, Racial and Religious Hatred and Intolerance. The protective object of this crime is the national, religious and racial equality of the citizens of the Republic of Serbia. Equality and unity of citizens in the Republic of Serbia is built on mutual respect and trust of all who live in it. This unity is preserved by constant nurturing, respect for all the characteristics of national, religious, racial, cultural and other values that characterize certain peoples and ethnic communities in the Republic of Serbia (Jović, 2011:240). The Code prescribes the basic, qualified and special form of this criminal offense. Intent is the only form of guilt for this criminal offence.

The act of committing the basic form of this crime is set alternatively as instigating or exacerbating national, racial or religious hatred, or intolerance (paragraph 1). This further means that the act will exist both in a situation when there is no national, racial, religious hatred or intolerance between peoples or ethnic communities, so it is provoked in different ways (i.e. it creates, causes), and when it exists as latent, a state or as a state of lesser intensity, and then further inflamed (Stojanović, 217:936). Instigating implies the creation of hatred or intolerance on the mentioned grounds, in a situation where such phenomena did not exist, while exacerbating is an increase (deepening, i.e. expansion) of already existing hatred, intolerance and bigotry. Thus, Instigating or exacerbating national, racial or religious hatred or intolerance can be done in different ways and by different means: speech, inscription and other actions, which influences the creation or strengthening of certain feelings or attitudes towards a nation or ethnic community. In terms of the nature of this crime, hatred is understood as a negative feeling of high intensity which represents a very fertile ground for undertaking various excessive behaviors towards members of a certain people or ethnic community. When it comes to intolerance, it is understood in relation to hatred as a negative feeling of "milder" intensity (the so-called vestibule of feelings of hatred), which can also cause certain negative behaviors that may ultimately contribute to the commission of this crime. It should be noted here that in criminal law theory, the question arises, and there are conflicting opinions, as to whether contempt for a nation or ethnic community can be included in the notion of intolerance. Namely, unlike hatred and intolerance, contempt for a nation or ethnic community, is a negative attitude that is most often expressed in the form of ignoring and as such does not contain the potential to perform certain activities and actions against a nation or ethnic community, so that provoking and inciting contempt would still not be sufficient for the existence of this crime (Stojanović, 2017:936). The passive subject in this criminal offense is represented by peoples, national minorities and ethnic communities living in the Republic of Serbia, and in connection with this, committing actions under this criminal offense against national or ethnic groups not living in the Republic of Serbia cannot constitute this criminal offense.

The criminal offence has been done by undertaking an activity with the aim of instigating or exacerbating hatred or intolerance, i.e. it is not necessary that these activities have led to the provocation or incitement of hatred or intolerance, or that a

[3] Criminal Code of Republic of Serbia *("OG", no. 85/2005, 88/2005, 107/2005,72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 and 35/2019).*

consequence has occurred. Therefore, the very consequence of this act is endangering the equality of citizens regardless of national, racial or religious affiliation. This form of criminal offence is punishable by imprisonment from six months to five years.

The qualified form of this criminal offense exists when some of the legally established qualifying circumstances (paragraph 2) have been met, which indicate the commission of the basic form of the criminal offense: a) coercion, b) abuse, c) endangering security, d) exposing national, ethnic or religious symbols, e) damage to other people's property, f) desecration of monuments, memorials or graves (Simonović, 2010:624). For this form of criminal offence is punishable by one to eight years in prison.

The second qualified form will exist when the basic form or the first serious form of this criminal offense is committed by abuse of position or authority or if as a result of these acts there were riots, violence or other serious consequences for the common life of peoples, national minorities or ethnic groups living in Serbia (paragraph 3). For this form of offense, in the event that under the qualifying circumstances the offense referred to in paragraph 1 was committed, a sentence of imprisonment of one to eight years is prescribed, and if the offense referred to in paragraph 2 is committed, imprisonment of two to ten years.

In addition to the aforementioned criminal offense, Article 387 prescribes the criminal offense of Racial and Other Discrimination, paragraph 3 of which prescribes the conduct of this criminal offense, which is reflected in: a) spreading the idea of superiority of one race over another, b) propagating racial hatred or inciting racial discrimination. These are actually three forms of racist propaganda (Ivanović & Ranđelović, 2019:55). For this form of crime, a prison sentence of three months to three years was listed. Also, paragraph 4 of this criminal offense prescribes the act of committing this offense, the form of which is reflected in the dissemination or otherwise making publicly available texts, images or any other presentation of ideas or theories that advocate or incite hatred, discrimination or violence against any persons or groups of persons based on race, color, religion, nationality, ethnic origin or any other personal characteristic. This form of crime is punishable by imprisonment from three months to three years.

Article 174 prescribes the criminal offense of Infringement of Reputation Due to Racial, Religious, National or Other Affiliation, which stipulates that whoever publicly exposes a person or group for belonging to a certain race, skin color, religion, nationality, ethnic origin or any other personal characteristic shall be punished with a fine or imprisonment for up to one year.

Article 138 prescribes the criminal offense of Endangering Security, Article 1 of which stipulates that whoever endangers the security of a person by threatening to attack the life or body of that person or a person close to him, shall be punished by a fine or imprisonment for a term not exceeding one year. The act of committing the basic form of a criminal offense (paragraph 1) is the use of the threat to attack the life or body of a person or a person close to him. So, it is not ordinary, but the so-called a qualified threat, given that it is necessary to threaten a specific evil – an attack on the life or body of a passive subject or a person close to him. It can be threatened either only by an attack on life, or only by an attack on bodily integrity (therefore, the threat of inflicting light bodily injuries is sufficient), or cumulatively by an attack on life and an attack on the body. Under the notion of a close person in the sense of this incrimination should be considered blood relatives in the direct line, brother and sister, spouse and a person living in a permanent extramarital union, adoptive parent

and adoptee, custodier and custodian. As the criminal offense of endangering security in Serbian criminal law is set as a consequential criminal offense, it is understood that the passive subject knows about the threat. Also, for the existence of the criminal offense is not affected by whether passive subject find out for threat directly from the perpetrator or from another person (so-called "indirect threat"). Paragraph 2 stipulates that whoever commits the act referred to in paragraph 1 of this Article against several persons, or if the act caused disturbance of citizens or other severe consequences, shall be punished by imprisonment for a term between three months and three years (Ivanović, 2020).

IV. Instead of conclusion

Considering that, when it comes to online hate speech, there is certainly a pronounced dark figure of this type of criminal manifestation, and that official police, prosecutorial and court records do not give a true picture of the state of this type of criminal manifestation, we took the results of research of perception and experience regarding online hate speech. Also, we deliberately took into account the attitudes of young people on this issue during the crisis with the COVID-19 virus because they moved to the online world to a large extent due to measures of social distancing and isolation of mutual interaction of young people from the real world. Based on the results of the research presented in this paper, we can conclude that about 30% of young people felt offended by some Internet content during the crisis with the COVID-19 virus, that about 42% witnessed a situation in which someone was insulted or belittled on the Internet. the basis of some group affiliation, while about 12% of young people pointed out that they were direct victims of hate speech on the Internet in this period. Also, we can see that in most cases it was about calling people a derogatory name and threatening to attack, and when it comes to group affiliations on which hate speech was based, we can conclude that it was based on national affiliation, religious affiliation, political affiliation, gender, sexual orientation and gender identity. The question we want to address in this paper is whether the current criminal legal protection against online hate speech in the Republic of Serbia is adequate, and in which direction it can be improved.

The first thing we can notice is that the criminal justice system of the Republic of Serbia explicitly recognizes only national, racial and religious hatred, stating the wording "and other personal characteristics". The question is what about political belief, sexual orientation, gender or gender identity as the basis of hatred? Does this mean that public incitement to hatred towards these groups is not covered by the being of incriminated behavior? Namely, the legislator did not limit the groups, ie personal characteristics that are protected by the aforementioned incriminations, but listed the most typical ones and then, through the formulations of "another personal characteristic", enabled those that are not explicitly listed to be included (Ćorović, et. al. 2020:90). Taking into account that the law does not contain certain what is considered personal characteristics, such a formulation can create a problem when applied in practice when other personal characteristics are in question, such as sexual orientation, gender, gender identity etc. The problem of political affiliation may arise in particular, because there are conflicting opinions in the literature as to whether it can be considered a personal property or not. Can we, therefore, state that the existing criminal law provisions do not represent a satisfactory and comprehensive solution in

terms of achieving an adequate fight against hate speech and that, probably, the legal incrimination of the aforementioned crimes should be formulated in such a way as to explicitly recognize personal characteristics such as sexual orientation, gender, gender identity, disability, age, property status, political affiliation etc. In addition, we can state that there is no explicit criminal offence of hate speech, but hate speech can occur as a way of committing several crimes. In this regard, the provisions of the criminal legislation of the Republic of Serbia should be amended in the manner in which it is done in Croatia or the Republika Srpska. Namely, the criminal laws of Croatia[4], as well as the Republika Srpska[5], recognize a criminal act called "Public incitement to violence and hatred".

The act of this criminal offence is committed by a person who through the press, radio, television, computer system or network, at a public gathering or otherwise publicly encourages or makes available to the public leaflets, pictures or other materials calling for violence or hatred directed at a group of people or a member groups of people because of their racial, religious, national or ethnic affiliation, language, origin, skin color, gender, sexual orientation, gender identity, disability, or any other characteristics. We believe that the introduction of such incrimination in the criminal legislation of the Republic of Serbia would greatly contribute to better criminal legal protection than online hate speech. First of all, because the current provisions do not contain a definition of the meaning of the element "public", since we believe that this is an essential feature of the commission of criminal acts related to hate speech. What, then, is meant or is meant by public incitement to hatred, discord, or intolerance? Will this element be satisfied for the purposes of prosecuting perpetrators if hatred is spread or transmitted to a narrow circle of people, at protests or demonstrations in public, if it spreads on the Internet, either through portals or social networks? Will the action of the act be done if it is provoked or transmitted on an online closed forum, which you can enter only if you have registered and thus gained access? Therefore, in terms of the area or space in which acts related to hate speech can be committed, the current provisions do not provide a clue. By prescribing a general criminal offense of hate speech, such a shortcoming would be compensated, and doubts would be resolved. Also, prescribing such a crime would have an encouraging effect on the victims themselves to report the crime, because due to ignorance and current legal wording, many victims are not sure whether they enjoy protection in terms of the aforementioned crimes, so they decide not to report. Finally, this formulation, in addition to explicitly listing other characteristics, also provides equality in terms of recognizing personal characteristics as a motive for insulting and inciting attacks on a certain group or individual.

References

1. Ćorović, E., Ivanović, R. A., Ivanović, B. A., Ranđelović, D., Šemović, A., Novaković, M., Dečković, S., Baćićanin, A., Fetahović, A., (ed. Aleksandar R. Ivanovic) (2020) *Manual for hate crime moot court* [*Priručnik za simulaciju suđenja iz oblasti zločina iz Mržnje*], Novi Pazar: MONITOR.

[4] Criminal law of Republic of Croatioa [Kazneni zakon Republike Hrvatske*]* (OG 125/11, 144/12, 56/15, 61/15, 101/17, 118/18, 126/19).

[5] Criminal code of Republica Srpska [Krivični zakonik Republike Srpske*]* ("OG", no. 64/2017 i 104/2018 – decision CC).

2. Criminal Code of Republic of Serbia *("OG", no. 85/2005, 88/2005, 107/2005,72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 and 35/2019);*

3. Criminal code of Republica Srpska [Krivični zakonik Republike Srpske] ("OG", no. 64/2017 i 104/2018 – decision CC)

4. Criminal law of Republic of Croatioa [Kazneni zakon Republike Hrvatske] (OG 125/11, 144/12, 56/15, 61/15, 101/17, 118/18, 126/19).

5. Ivanović, R. A., (2018) *Hate speech on Internet through illegality to punishment*, Yearbook Human rights protection: From unlawfulness to legality, Provincial Protector of Citizens – Ombudsman and Institute of Criminological and Sociological Research, Novi Sad, pp. 405-418. (SRB).

6. Ivanović, R. A., (2020) *Hate speech in electronic media and challenges for the criminal justice system of the Republic of Serbia*, Journal for Eastern-European Criminal Law, vol. 7, no. 1, Faculty of law of University of Temisoara and Faculty of law of University of Pėcs, Editura Universul Juridic.

7. Ivanović, R. A., Slotvedt, L. P. (2020) Conflict management & trust building in multicultural communities with the aim of combating radicalism and extremism [Mirno rešavanje konflikata i izgradnja poverenja u multikulturalnim sredinama u svrhu borbe protiv radikalizma i nasilnog ekstremizma], Novi Pazar: MONITOR.

8. Ivanović. R. A., Ranđelović, D., (2019) *Sanctioning hate speech on the internet, according to the national regulations of the Republic of Serbia* [*Sankcionisanje govora mržnje nainternetu prema nacionalnoj regulative Republike Srbije*], Arhiv za pravne i društvene nauke vol. 1, no. 1, Law faculty Lukavica.

9. Jović, M. (2011). *Criminal law – special part – script I* [*Krivično pravo – posebni deo – skripta I*], Novi Pazar: International university of Novi Pazar.

10. Simonović, D. (2010) *Criminal offenses in Serbian legislation* [*Krivična dela u srpskoj legislativi*], Belgrade: Službeni glasnik;

11. Stojanović, B. (2020) *Qualitative and comparative report on the survey regarding discrimination and hate speech conducted in three multicultural regions of Serbia*, Novi Pazar, MONITOR.

12. Stojanović, Z. (2017) *Commentary on the Criminal Code: Sixth Amended Edition* [*Komentar Krivičnog zakonika: šesto izmenjeno i dopunjeno izdanje*], Belgrade: Službeni glasnik.

Jurisdictional Challenges of Cybercrime

Dávid Tóth [*] ***– Zsolt Gáspár*** [**]

Abstract

As a result of the development of technology, the appearance of cybercrime set up new challenges for almost all fields of criminal law. New crimes appear in the criminal substantive law, like information system fraud, or criminal offenses related to non-cash payment instruments. The detection or seizure of electronic evidence can cause difficulties for the criminal procedure law, too (see the appearance of virtual currencies, e.g. bitcoin). According to the starting hypothesis of the study, the traditional principles used in international criminal law are not, or not sufficiently able to give adequate answers to the difficulties created by cybercrime.

The research aims to demonstrate and examine the practical and theoretical challenges revealed by cybercrimes. The first part of our research deals with the traditional principles of jurisdiction, and the theoretical and practical problems that can come up in the field of cybercrime. Relating to international cybercrime, positive jurisdictional collisions can be observed frequently, for which we devise suggestions. In the second part of our study, we investigate the difficulties and the institutional regards of the criminal cooperation connected to cybercrime. In the third part, we analyze The Convention on Cybercrime of the Council of Europe, whether if it provides suitable answers for jurisdictional challenges. In the closing part of our study, we summarize the conclusions and devise suggestions.

Keywords*: cybercrime, jurisdiction, EU law, international law, Cooperation in criminal matters*

I. Introduction

In history, there have been several difficulties for the states in the cooperation in criminal matters. A traditional problem was, for example, the harm of sovereignty, the slow processes of extradition, the conflicts between the states. Despite these difficulties, some principles have been evolved, which can solve many questions (e.g. jurisdiction, extradition, legal aid).

With the development of society, the legal regulations became more and more complex in international criminal law[1]. Until the 20-21. century criminality was a local

[*] PhD, adjunct, Univesity of Pécs, Faculty of Law, Criminology and Penal Executional Law Chair

[**] PhD student, Univesity of Pécs, Faculty of Law, Criminology and Penal Executional Law Chair

[1] „The international criminal law is a segment of the international law and the national criminal law, which involves the institutions of the cooperation in criminal matters and the regulations of international crimes." Citing: László, Kőhalmi, 'A nemzetközi bűnügyi együttműködés [The international cooperation in criminal matters] ' in Ágnes, Balogh – Mihály, Tóth (eds), *Magyar büntetőjog Általános rész [Hungarian criminal law General part]* (Osiris 2010) 375.

phenomenon. The principles regulating the criminal jurisdiction were built to the basic axioms, that the dictum is a phenomenon bound to a determined geographical area. As a result of technological development, the appearance of cybercrime set up new challenges for almost every field of criminal law. New crimes appear in the criminal substantive criminal law, like the crimes conducted with information systems or the crimes related to the non-cash payment instruments. The investigation or seizure of electronic evidence can cause difficulties for the criminal procedure law also (see the virtual currencies, like the appearance of Bitcoin). Even before the appearance of cybercrimes, there were a rising number of delicts, which were able to harm or endanger two or more states' legal system due to the citizenship of the perpetrator, or the circumstances of the crime[2].

Cybercrime multiplies this phenomenon and changes the image of criminality in its basis, making it an international phenomenon that knows no borders. In the virtual space, for example, the crime of money laundering[3] has become more widespread. Cybercrime also provides a new financing area for the terrorists[4].

According to the initial hypothesis of the study, the traditional principles used in international criminal law cannot give adequate answers to the difficulties set up by cybercrime. In the first part of our study, we are dealing with the international sources of law and the jurisdictional principles in general. After that, in correspondence with the aim of the research, we are presenting and observing the practical and theoretical challenges connected to cybercrimes. In the third part of the study, we are presenting the regional efforts of the European Union against cybercrime.

II. Jurisdictional principles

The jurisdiction is a legal term used in international law. Under this institution a state has the right to legislate, apply and enforce the law. The jurisdiction creates the possibility of the application of the law and it is also it's requisite. We can talk about the criminal jurisdiction in a wider and a narrower sense. Criminal jurisdiction in a wider sense means that the state has the right to create a criminal law regulation. The narrower sense of criminal jurisdiction consists of the applicability of the national criminal regulation and the range of the competence of the authorities proceeding in criminal cases[5]. The Permanent Court of International Justice stated in the Lotus-case in 1927, that international law does not limit the criminal jurisdiction of the state, it

---

[2] Péter, M. Nyitrai, *Nemzetközi és Európai Büntetőjog [International and European Criminal Law]* (Osiris 2006) 208.

[3] István László, Gál, 'The Techniques of Money Laundering.' in István László, Gál – László, Kőhalmi (eds.), *Emlékkönyv Losonczy István professzor halálának 25. évfordulójára*. (Pécsi Tudományegyetem, Állam- és Jogtudományi Kar 2005) 129-138.

István László, Gál, 'A pénzmosás szabályozásának régi és új irányai a nemzetközi jogban és az EU-jogban [The old and new tendencies in the regulation of money laundering in the international and EU Law]' Európai Jog. [2007] 12-23.

[4] See further about the financing of terrorism: István László, GÁL, 'Új biztonságpolitikai kihívás a XXI. században: a terrorizmus finanszírozása. [New challenges of security policy in the 21st century: the financing of terrorism] ' Szakmai Szemle [2012] 5-15.

GÁL István László, *A terrorizmus finanszírozása: Die Terrorismusfinanzierung, [The financing of terrorism]* (PTE Állam- és Jogtudományi Kar Gazdasági Büntetőjogi Kutatóintézet 2010)

[5] cf Nyitrai (n 2) 209.

can enforce it if it has an effective possibility to do so[6]. An exception of the main rule is that during the practice of its penitentiary power, a state cannot intervene in another state's internal affairs, because that is its exclusive right. Under the decision of the Lotus-case, the territorial principle is not sole, therefore the jurisdiction of the states can be extended to the crimes committed by foreign citizens abroad[7]. If a state decides to extend its jurisdiction to the territory over its borders, then international only requires that's some kind of connection exists between the punishable conduct and the sovereignty of the country.

Several principles deal with this connection and are generally accepted in international law like the territorial, the personal, the protective and the universality principle. In these cases the state exercises its original sovereignty and are called original jurisdictional cases. Occasionally derivative jurisdiction can also occur in a few cases, where the state with the primary jurisdiction hands over its jurisdiction to another state while using the so-called aut dedere aut judicare or in other words representation principle[8]. The latter one serves to fill a regulatory gap. This supplements the criminal jurisdiction of other countries.

In legal cases containing international elements, conflicts can appear on deciding which country has jurisdiction. The Anglo-Saxon literature lists the following jurisdictional principles:

- *jurisdiction to prescribe*: the establishment of the future assertion of the state's punitive power. This answers the question, if there is any jurisdictional principle (e.g.: the territorial principle), according to which, an act can be subsumed under the inner criminal law. The actual practice of punitive power can emerge after this. In the continental legal systems, as well as in the Hungarian, we can find the jurisdictional regulations in the territorial and personal scope of the law. Another legal source of this area are the conventions on international legal aids in criminal matters[9].
- *jurisdiction to adjudicate*: the second term means the jurisdiction of the sentencing, based on which the sovereign power can subsume people or organizations under the procedure of the state court to decide whether an infringement has happened or not.
- *jurisdiction to enforce*: the third term means the possibility and limits of the actual practice of jurisdiction. The executive jurisdiction also involves the extradition after the decision[10].

---

[6] The essence the case is the following: the French ship, named Lotus crashed with a Turkish ship on the Sea of Marmora. After the accident the ships came to anchor in Istanbul. The two states got into a debate in front of the International Court of Justice due to the case. The question was if Turkey had jurisdiction over the French citizens who were involved in the case. According to the decision of the International Court of Justice, there is no regulation in the international law, which states that only the country has jurisdiction whose flag the ship wears. That means Turkey can assert its jurisdiction based on the presumption of sovereignty. See further: János, Bruhács, *Nemzetközi Jog I. Általános rész. [International Law I. General part.]* (Dialóg Campus Kiadó 2009) 21.

[7] Péter, Polt, 'A magyar büntető joghatóság. [The Hungarian criminal jurisdiction.]' in Polt et. al. (eds.) A Büntető Törvénykönyvről szóló 2012. évi C. törvény nagykommentárja. (Opten 2016) 26.

[8] Katalin, Ligeti, *Büntetőjog és bűnügyi együttműködés az Európai Unióban [Criminal law and Cooperation in criminal matters in the European Union]* (Közgazdasági és Jogi Könyvkiadó 2004) 43.

[9] ibid 43-44

[10] Henry Jr. H. Perritt, 'Jurisdiction in Cyberspace' Villanova Law Review [1996] 3.

The jurisdiction to prescribe can be decided based on various principles. Based on the territorial principle, the criminal law of the sovereign state has to be applied to every crime committed within the territory of the country, irrespectively to every other circumstance (e.g. the citizenship of the perpetrator or the victim)[11].

The quasi territorial principle extends this jurisdiction to ships and aircraft that sail or fly under the flag of the state[12]. This principle is often called the flag principle as well[13].

Under the nationality principle, the state can impeach its citizens, no matter whether they committed the crime in the country or abroad. This principle is called the active nationality (personality) principle. The other form of the principle is the passive nationality principle (which is also contained in the Hungarian Criminal Code). Based on this principle, the state can expand its jurisdiction for the crimes committed against its citizens abroad[14].

According to the self-defense of the state principle *(principium reale),* the state can sanction the people whose act harms the values or subjects protected by the criminal law system of the country, irrespectively to the citizenship of the perpetrator or the location of the act[15].

Based on the universality principle, the crimes harming the recognized subjects of law can be penalized and subsumed under the jurisdiction of the state, irrespectively to the location of the act or the citizenship of the victim or the perpetrator. It is also called the absolute punitive power, which usually appears in international conventions and expresses the sovereignty of the states. It is disputed though, which crimes can be subsumed under the principle of universality principle[16]. According to the fifth article of the International Criminal Court Statute approved on 17th July 1998 in Rome, the crimes that are under the Court's jurisdiction are the followings:

- the crime of genocide;
- crimes against humanity;
- war crimes;
- and the crime of aggression[17].

During the development of international law, the nationality jurisdiction has appeared earlier than the territorial but nowadays the territorial jurisdiction is applied more preferably by the states. The nationality principle did not disappear from the practice, it only has been reversed compared to by the application of the territorial principle, as a principle of jurisdiction[18].

---

[11] István László, Gál, 'Jogszabálytan. [Legal dogmatics]' in Balogh Ágnes – Tóth Mihály, *Magyar Büntetőjog Általános Rész.* (Osiris 2015) 75-76.

[12] cf Ligeti (n 8) 44.

[13] Helmut Satzger, *International and European Criminal law* (C.H. Beck, 2012) 17.

[14] Krisztina, Karsai, 'A magyar büntető joghatóság [The Hungarian criminal law jurisdiction]' in Krisztina, Karsai (eds.) *Nagykommentár a Büntető Törvénykönyvhöz: Nagykommentár a Büntető Törvénykönyvről szóló 2012. évi C. törvényhez,* (Wolters Kluwer 2019) 39-40.

[15] cf Gál (n 11) 75-76.

[16] cf Ligeti (n 8) 47.

[17] See further: Ferenc, Sántha, 'A Nemzetközi Büntetőbíróság joghatóságába tartozó nemzetközi bűncselekmények vázlata [Outline of international crimes within the jurisdiction of the International Criminal CourtOutline of international crimes within the jurisdiction of the International Criminal Court]' In Bragyova, András (eds.) *Tanulmányok a bűnügyi tudományok köréből.* (Gazdász Elasztik 2013) 170-197.

[18] A. Imre Wiener, 'A Nemzetközi Büntetőbíróság joghatóságáról' [About the jurisdiction of the International Criminal Court] Magyar Jog [2001] 457.

III. The regulation of the jurisdiction in the field of international cybercrime

Several international sources of law deal with the question of jurisdiction in connection with cybercrime. We would highlight the followings without the intention of being exhaustive:

- The Convention on Cybercrime accepted on 23rd November 2001 in Budapest by the Council of Europe deals with the question of jurisdiction;
- Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems, Strasbourg, 28.1.2003, ETS No. 189, Article 4. (1);
- Arab Convention on Combating Information Technology Offences, Cairo, 21.12.2001, Article 30. (1)(a).

What is common in the above-listed conventions, that they all consider the territorial principle as a primary jurisdictional rule. In our study, we are focusing on the Budapest Convention on Cybercrime, due to its Hungarian relations.

Until September 2020, the international convention was ratified by 65 countries, inter alia, by Hungary, too.

Our country promulgated the convention with the Act LXXIX of 2004.

The jurisdictional regulations of the convention can be found in Article 22 of Section 3. Based on this regulation, states can establish jurisdiction over any offense committed in its territory; or onboard a ship flying the flag of that state; or onboard an aircraft registered under the laws of the state; or committed by one of its nationals. The signing parties can present their reservations or conditions against the regulations of the convention.

The convention also gives solutions to jurisdictional conflicts. When more than one Party claims jurisdiction over an alleged offense established following this Convention, the Parties involved shall, where appropriate, consult to determine the most appropriate jurisdiction for prosecution[19].

The question of extradition is tightly connected to the jurisdiction, which is also regulated by the cybercrime convention. According to Article 24: *"This article applies to extradition between Parties for the criminal offenses established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty."*

Where different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply[20].

The criminal offenses described in paragraph 1 of this article shall be deemed to be included as extraditable offenses in any extradition treaty existing between or among the Parties. The Parties undertake to include such offenses as extraditable offenses in any extradition treaty to be concluded between or among them[21]. It is an important rule, that the extradition should meet the requirements set up in the

[19] Budapest Cybercrime Convention, Article 22. 5.
[20] Budapest Cybercrime Convention, Article 24. 1.
[21] Budapest Cybercrime Convention, Article 24. 2.

requested country's national law or the extradition treaties in force, without that, the extradition request can be denied.

If extradition for a criminal offense referred to in the Budapest Cybercrime Convention is refused solely on the basis of the nationality of the person sought, or because the requested state deems that it has jurisdiction over the offense, the requested state shall submit the case at the request of the requesting state to its competent authorities for prosecution and shall report the outcome to the requesting state in due course[22].

Similarily to the convention, the fifth point of Article 15 of the United Nations Convention against Transnational Organized Crime[23] also declares that if a State Party *"has been notified, or has otherwise learned, that one or more other States Parties are conducting an investigation, prosecution or judicial proceeding in respect of the same conduct, the competent authorities of those States Parties shall, as appropriate, consult one another to coordinate their actions."*[24]

In a summary, the presence of the Budapest Cybercrime Convention is positive, because it laid down the basis of cooperation for the states involved. From the other side – according to our point of view – the regulations of the convention should be renewed because it still does not solve several questions and problems, that cannot be dealt with under the territorial principle. The consultation is a necessary precondition, but it does not give a concrete answer or at least a guideline to the problems. Until today, international law did not set up a priority order between the jurisdictional principles[25]. As these types of crimes are getting more frequent, the slow and difficult consultation procedures will not be sufficient in the fight against cybercrimes. It might enlarge the problem, that a lot of times these negotiations does not lead to successful result between the states.

IV. Theoretical problems in cybercrime cases

4.1. Which cybercrimes can set up jurisdictional problems?

In this chapter, we would like to present through hypothetic examples, which jurisdictional problems can appear in the cases of crimes realized in cyberspace. Various types of cybercrimes can be differentiated. According to a theoretical division, we can make a difference between cybercrimes crossing local and international barriers. In the former case, there is usually no territorial jurisdictional problem. At most, the nationality of the perpetrator, or the victim, can bring an international element to the case, which is relatively easier to resolve through the traditional principles of international criminal jurisdiction (territorial principle, nationality principle etc.). However, inner jurisdictional disputes can be caused by local cybercrime where in some cases it is difficult to decide which court has competence of the case[26].

---

[22] Budapest Cybercrime Convention, Article 24. 6.

[23] About organized crime see further: Mihály, Tóth – László, Kőhalmi, 'A szervezett bűnözés [The organized crime]' in Borbíró et. al. (eds.) *Kriminológia.* (Wolters Kluwer 2016) 603-625.

[24] <https://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-e.pdf> accessed 19 September 2020.

[25] Susan W. Brenner, 'Cybercrime jurisdiction.' Crime, law and social change. [2006] 189-206.

[26] See further: Tibor, Ibolya, *A számítástechnikai jellegű bűncselekmények nyomozása [The investigation of IT crimes]* (Patrocinium Kiadó 2012)

The other case is the so-called international or transnational cybercrime, where the perpetrator and the victim are located in different states.

Working in cross-border cyberspace grants even more benefits for the perpetrators, they can stay hidden and they can hide their identity, they can focus on more victims, causing even bigger damages in a short time. The perpetrator can aim at hundreds or even thousands of victims, for example with a so-called distributed denial-of-service (abbreviated DDoS) attack.

Jurisdictional conflicts can appear when more states have the right and the intention to proceed in a criminal case containing international elements (positive jurisdictional collision). The negative jurisdictional conflict is when no state has the right or the intention to proceed in a criminal case. This case is also called *vacuum iuris* in latin[27].

4.2. Hypothetical example for jurisdictional conflict

The following hypothetic case can be an example of a positive jurisdictional collision. A perpetrator from Congo commits a so-called "419 fraud" (which stands for the 419th paragraph of the Nigerian Criminal Code) to deceive English, Brazilian and Chilean victims. If all three countries start a criminal procedure at the same time against the perpetrator, it will lead to a positive jurisdictional conflict. All the countries valuate the case differently in consonance with their criminal codes (e.g. fraud, computer fraud, online abuse). Also, there are differences between the countries in the number of victims and on the scale of the caused damages. The question is given, that in the case of positive jurisdictional collision, which state has the priority against the other states, to proceed in the case.

Pursuant to Susan Brenner, the following factors should be taken into consideration while solving a positive jurisdictional conflict:

- procedural and practical processes, which were used to solve similar conflicts,
- standards, which were used to solve other kinds of jurisdictional conflicts,
- the special characteristics of cybercrimes[28].

However, Brenner highlights that alongside the mentioned ones, other aspects can also be taken into consideration with different emphasis. In the next subsection, we are examining how efficiently can the different jurisdictional principles solve the hypothetical case.

According to Zoltán Nagy, in addition to the above, the following aspects should be taken into account in jurisdictional issues:

- the interests of the defendant,
- the interests of victims and witnesses,
- the admissibility of the evidence, or
- delays in the case[29].

4.3. Which jurisdictional claim has priority?

4.3.1. The place of commission

Current international law most generally accepts the principle of territoriality as a principle of jurisdiction. Based on our hypothetical case, pursuant to the territorial

---

[27] cf Ligeti (n 8) 50.

[28] cf Brenner (n 25) 198.

[29] Zoltán András, Nagy, 'A joghatóság problémája a kiberbűncselekmények nyomozásában [The problems in the investigation of cybercrimes]' in Homoki-Nagy et. al. (eds.): *Ünnepi kötet dr. Nagy Ferenc egyetemi tanár 70. születésnapjára.* (Szegedi Tudományegyetem Állam- és Jogtudományi Kar 2018) 761

principle, the Congolese perpetrator should be held liable in Congo, because he continued his activity there. On the other hand, there was no victim of the crime in Congo, so there was no question of instituting criminal proceedings in that country. The victims report the crime in their own country and criminal proceedings are initiated there. All three countries represented by the victims (England, Brazil and Chile) cannot invoke the territorial principle because the perpetrator did not commit a criminal offense in their country. Another problem can be if the place of the offense and the IP address (see chapter 5.1 for more details) point to an unknown location. With the use of the so-called VPN services, the authorities would discover a location where the perpetrator has never been (points to a false place of commission).

Based on these facts, the territorial principle is not a solution for the hypothetical example.

4.3.2. The location of the arrest of the perpetrator

It could be a logical solution if the arresting state had the priority to proceed against the presumed offender. In traditional crimes this is a frequently used solution, but international cybercrime makes this field more complicated.

It is possible, that the perpetrator in the arresting state has caused damages only to a few victims, but to hundreds in another state, so this solution of the jurisdictional conflicts may seem unfair.

Let us assume that the Congolese perpetrator committed a terrorist act in England, instead of cyber-frauds. The perpetrator exploded a bus, in which citizens of Brazil and Chile died. England is detaining the perpetrator for committing a terrorist act. All states want to prosecute him. The relevant factor in the case is that the offense was committed in England, which gave the English authorities priority to institute criminal proceedings. If England successfully prosecutes, the other countries may decide not to continue the proceedings and are content with the English sentence.

In the case of cyber-fraud, the location where he committed the crime is completely irrelevant, just like the place of the victims. The legitimacy of the proceedings requires some other decisive argument or reason for the English State to prosecute the Congolese perpetrator. Such an expediency argument may be that the evidence is found in the country where the perpetrator committed the crime.

The place of detention may, in our view, provide a more effective solution in such cases than the application of the territoriality principle.

4.3.3. The location of the occurrence of the harm

In jurisdictional disputes, guiding factors can be the damage caused by the perpetrator and the number of victims. However, these should not be decisive either, because it can be problematic if the same amount of damage has occurred or the number of victims is the same in each country. It is also possible that the offender has caused millions in damage to a victim in England and, also caused small amounts of damage to hundreds of Brazilian citizens. Quantifying industrial espionage or identity theft can cause even greater difficulties in establishing a jurisdictional sequence[30].

Notwithstanding the above, it is important to take the magnitude of the damage into account in such matters, but it cannot in itself be a decisive argument for deciding jurisdiction.

[30] cf Brenner (n 25). 200-201.

4.3.4. The citizenship of the victim (passive personality)

The nationality of the victims has traditionally been of great importance in jurisdictional matters. Of course, this may be an important consideration in deciding the case, but it is still not certain to be decisive. All three states have victims, so the jurisdictional dispute can't resolved by this factor alone[31].

The principle of passive personality may be a more appropriate solution than the territorial principle, as in a significant number of cases victims report the crime and the criminal proceedings will presumably be initiated in these countries. On the other hand, this can also cause logistical difficulties, if the perpetrator is in a very distant country.

4.3.5. The citizenship of the perpetrator

Based on the nationality of the perpetrator, Congo would have the right and duty to proceed in the case. The application of the principle of nationality implies that a State is responsible for the actions of its own nationals, so that it will be responsible for prosecuting and bearing the costs of crime.

As Geoffrey R. Watson wrote, "*If disturbance of the legal order within a State's territory is considered the most persuasive reason for penal jurisdiction, such disturbance may be found in the presence unpunished of an offender who has committed crime elsewhere*"[32].

The application of the principle of nationality can be strengthened by the application of the principle of "*aut dedere, aut judicare*" ((Latin for "either extradite or prosecute"). This principle refers to the legal obligation of states under public international law to prosecute persons who commit serious crimes with international element where no other state has requested extradition. This presupposes that the "A" citizen offender flees to country "B" from the investigating authorities, and in this case, they are obliged to extradite the perpetrator or at least initiate criminal proceedings[33].

V. Practical difficulties

5.1. Technical background

The Internet Protocol (or shortly IP) is a unique set of identification numbers assigned to computer devices to be able to recognize each other and send data to each other through the Internet[34]. IP addresses are maintained by an international non-profit company called Internet Corporation for Assigned Names and Numbers (ICANN for short), which was founded in 1988, and which also performs coordination tasks[35]. IP addresses can also be linked to geographical locations, which as a result could determine the origin of a particular cybercrime based on the attacker's IP address. However, the problem is rooted in the fact that no competent perpetrator

[31] Ibid 202-204.

[32] Geoffrey R. Watson, 'The Passive Personality Principle.' in Texas International Law journal [1993] 17.

[33] BRENNER, Op.Cit. p. 198.

[34] Da-Yu Kao – Shiuh-Jeng Wang, 'The IP Address and Time in Cyber-Crime Investigation.' Policing: An International Journal of Police Strategies & Management 32, [2009] 195.

[35] <www.icann.org/history> accessed 19 September 2020

uses their IP address for an attack, also, there is a huge variety of techniques available to them to maintain their anonymity[36]. On one hand, the IP address of the device used by the attacker can be easily exchanged for the IP address of another device, making the attack appear to come from a different location than where it originates[37].

Besides, changing the IP address is a very easy-to-learn technique, so it is used by many users, and there are also several guides on online interfaces that describe in detail how to use this method[38]. Another preferred solution is the use of private or public proxy servers, which act as a kind of intermediary tool between the attacker's computer system and the victim's system so that the attacker can remain anonymous[39]. Public servers are more accessible. On the other hand, because they are used by many, they are slower, less reliable than private servers. Nowadays, such services can be accessed relatively cheaply and easily, as countless companies lease them[40]. In addition to the formerly mentioned ones, the most commonly used and most effective technique is when they remotely take control over a device in a foreign country, and using that device they launch an attack on a third party. This so-called "victim-computer" is usually the last piece in a long chain that is composed of several devices and states[41].

5.2. The Ivanov and Gorshkov-case

The US government claims that Aleksey Vladimirovich Ivanov in 2000 hacked into the computer system of the Online Information Bureau, Inc. (OIB) and took the key passwords, with which he could take over control of the entire system of the OIB. According to the indictment, Ivanov then began to threaten to destroy the company's entire computer system and demanded roughly $ 10,000 in exchange for not doing so. When he was rejected, he sent another threatening e-mail to an OIB-employee working in Vernon, Connecticut, using the system of Lightrealm (an internet provider from Kirkland, Washington) remotely from Russia[42].

The FBI agents caught the perpetrators in a very unusual way, as part of which, disguised as a businessman, they lured the two Russian hackers to Seattle for a job interview. During the interview, they had to show their IT skills on a computer on which the FBI had previously installed spyware programs. With the help of these programs, the FBI agents obtained those passwords from the hackers, which gave them access to their computers, from which federal agents later backed up the data and then used it as evidence in the criminal proceedings[43].

Aleksey Vladimirovich Ivanov and Vasiliy Gorshkov have been indicted in the United States for conspiracy, computer fraud, and related activity, extortion, and

---

[36] Jean-Baptiste Maillart, 'The limits of subjective territorial jurisdiction in the context of cybercrime' ERA Forum [2019] 378-379

[37] ibid 379.

[38] See e.g.: <https://www.safervpn.com/blog/how-to-change-ip-address> accessed 19 September 2020

[39] cf Maillart (n 36) 379.

[40] <https://medium.com/@ProxiesAPI.com/public-proxy-servers-vs-private-proxy-servers-for-web-scraping 1c5b27549cca> accessed 19 September 2020

[41] cf Maillart (n 36) 379.

[42] <https://law.justia.com/cases/federal/district-courts/FSupp2/175/367/2419190/> accessed 19 September 2020

[43] Önder Kutay Seker, *International Regulation of National Cybercrime Jurisdiction.* (Tilburg University 2012) 10.

unauthorized access to assets. Ivanov argued, that because he was in Russia at the time when the crimes were committed, he could not be charged with the violation of the law of United States[44]. However, the court found that it has jurisdiction over the case, on one hand, because the intentional and actual harmful effects of Ivanov's acts (committed in Russia) developed in the United States, on the other hand. After all, all the substantive legal facts realized by Ivanov are applicable regardless of the territory, according to Congress[45].

The Russian authorities, on the other hand, had a different view about the case, arguing that the decision violated the traditional principles of jurisdiction, besides, they were criticizing the events of the investigation and the obtainment of the evidence, giving voice to their disagreement with the accusation of the FBI agents in Russia of hacking, which in itself raises another issue of jurisdiction[46].

5.3. The Gary McKinnon-case

Gary McKinnon was an unemployed computer administrator from the UK who gained unauthorized access to 97 U.S. government computers from his home in London. Among other things, he has been proven to erase data from their operating systems, and as a result, the U.S. Army had to shut down more than 2,000 from its computers in Washington for 24 hours. In November 2002, the states of New Jersey and Virginia also raised charges against McKinnon. The U.S. government wanted to make a bargain with McKinnon's lawyers, as part of which McKinnon would plead guilty and give consent to his extradition, in exchange for spending 37-46 months in prison, of which he could return home after serving 6-12 months in the US. to serve his remaining sentence in the United Kingdom. Then, he could have been released under English law, as a result of which he would only have to spend between 18 and 24 months in prison, but if he did not cooperate, he would have had to face 8-10 years (of which max. 15% could have been waived) in a high-security prison without the possibility of returning home[47]. In August and September 2004, after McKinnon refused the deal, the states of Virginia and New Jersey also sought an arrest warrant against McKinnon, and they also requested his extradition from the Secretary of State. After accepting the applications, McKinnon was arrested on June 7, 2005, and after hearings in 2006, the Secretary of State informed him that he had issued an order for his extradition. In 2008, the House of Lords dismissed his appeal against his extradition[48]. However, in 2012, Home Secretary Theresa May revoked the extradition warrant against McKinnon because he had been diagnosed with Asperger's Syndrome and, according to experts, he would be at risk of suicide if he was extradited[49].

---

[44] Ibid 10.

45 <https://law.justia.com/cases/federal/district-courts/FSupp2/175/367/2419190/> accessed 19 September 2020

[46] cf Seker (n 43) 10.

[47] Nicola Padfield, 'Shining the Torch on Plea-Bargaining.' The Cambridge Law Journal [2009] 11-14.

[48] <https://publications.parliament.uk/pa/ld200708/ldjudgmt/jd080730/mckinn-1.htm> accessed 19 September 2020

[49] <https://www.gov.uk/government/news/theresa-may-statement-on-gary-mckinnon-extradition> accessed 19 September 2020

VI. The European Union's institutional and regulatory solutions

6.1. Regulations connected to cybercrime

The first EU regulation dealing with cybercrime jurisdiction was the Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, in the Article 17. According to this article, the State has jurisdiction and shall take the necessary measures, if the offense was entirely or in part committed within its territory or the offender is one of their nationals. If a State establishes its jurisdiction over an offense regardless of the above-mentioned cases, the State shall inform the Commission. This can happen in the following cases:

- if the offense is committed against a national of that Member State or a person who has his or her habitual residence in the territory of that Member State; or
- the offense is committed for the benefit of a legal person established in the territory of that Member State; or
- the offender is habitually resident in the territory of that Member State[50].

The second significant source, the 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 brought only minor charges in connection with jurisdiction. According to Article 12 of the Directive, a State can establish jurisdiction if the crime was committed in whole or in part within their territory, or by one of their nationals, at least in cases where the act is an offense where it was committed.

Regarding the territoriality principle, the directive also stipulates that if the offender is physically present in the territory of a State at the time when the offense is committed, it shall have jurisdiction, regardless of whether the offense was against an information system within its territory, and also if the offender is not in the territory of that State but the offense is against an information system located within its territory. Similarly to the Directive 2011/92/EU, the State shall inform the Commission in the following cases:

- the offender has his or her habitual residence in its territory, or
- the offense is committed for the benefit of a legal person established in its territory[51].

The Directive (EU) 2019/713 of the European Parliament and of the Council of 17 April 2019 on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA applies the same logic as the before-mentioned directives. The jurisdictional regulations can be found in Article 12, according to which a State can establish jurisdiction if the offense was entirely or in part committed within its territory or the offender is one of their nationals. The

[50] Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, Article 17.

[51] 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, Article 12.

Commission should be informed if a Member State establishes its jurisdiction over an offense that was committed outside of its territory and:

- the offender has his or her habitual residence in its territory,
- the offense is committed for the benefit of a legal person established in its territory,
- the offense is committed against one of its nationals or a person who is a habitual resident in its territory[52].

6.2. The institutional side of the fight against cybercrime: the Europol

The judicial and police cooperation has developed in parallel with the strengthening of economic ties between the Member States of the European Union. The abolition of controls has led to an increase in cross-border crime, so there has been an urgent need to institutionalize the cooperation between the Member States in these areas[53].

Criminal judicial cooperation between the Member States and the establishment of the European Police Office (Europol for short) was already an objective set out in the 1992 Maastricht Treaty, with the idea of establishing police cooperation between the Member States to strengthen the fight against terrorism, drug trafficking and other forms of international crime, based on Europol by ensuring the flow of information. In 1995, the Europol Drugs Unit (EDU) was set up temporarily with the main task of curbing drug trafficking and money laundering[54].

However, in the following year, the Council of Ministers extended its powers and Europol became generally accepted among the Member States[55].

The main objective of Europol is to facilitate the work of Member States' investigative authorities and increase their effectiveness in the fight against terrorism and international crime.

Its main tasks include (among others):

- the facilitation of the flow of information among the Member States,
- the provision of assistance to the operations of the investigative authorities of the Member States,
- collecting, organizing, and investigating information on crime,
- the development and maintenance of the computerized IT systems for data analysis,
- providing practical and technical assistance to the investigations processed by the Member States' investigative authorities[56].

---

[52] Directive (EU) 2019/713 of the European Parliament and of the Council of 17 April 2019 on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA, Article 12.

[53] Željko Nikač, The European Arrest Warrant-Europol.International Journal of Economics and Law [2014] 91-92.

[54] Eszter, Karoliny, 'Igazságügyi együttműködés büntetőügyekben; a kölcsönös elismerés elve. A ne bis in idem elve az Európai Unió Bíróságának ítélkezési gyakorlatában. [Cooperation in criminal matters, the mutual recognition and the principle of ne bis in idem in The practice of the European Court of Justice]' in Mohay Ágoston – Szalayné Sándor Erzsébet (eds.*): Az Európai Unió Joga.* (Dialóg Campus Kiadó 2015) 206-217.

[55] <https://www.policija.si/eng/areas-of-work/other-areas/international-cooperation/europol> accessed 19 September 2020

[56] cf Nikač (n 53) 92.

The organization's competencies have been expanded during the years, which now deals with the prevention and the combat of the following crimes: trafficking in human beings, illicit car trafficking, human smuggling, child pornography, trafficking in nuclear and radioactive materials, money laundering[57]. In 2013, Europol set up the European Cybercrime Center to support strengthened EU legislation on cybercrime and to protect EU citizens, governments, and businesses. The ECC publishes an annual report on the Internet Organized Crime Threat Assessment (IOCTA for short), which also gives proposals for strengthening the legislation in this area and provides key information for Member State governments and EU citizens and businesses. Since 2014, the ECC has a cybercrime task force (the so-called Joint Cybercrime Action Taskforce or shortly J-CAT), which, as an action group, inter alia, coordinates the cross-border cybercrime investigations and operations. The establishment of the mentioned institutions has led to several successes, including:

- the coordination of a joint operation, including private-sector partners to target a botnet called Ramnit, that had infected millions of computers around the world,
- coordination with Eurojust in an operation targeting large-scale malware attacks that originated in Ukraine and that were being investigated by several agencies – an operation that led to tens of arrests and continues to supply evidence that supports other cybercrime investigations,
- an operation targeting a major cybercriminal forum engaged in trading hacking expertise, malware and botnets, Zero Day Exploits, access to compromised servers, and matching partners for spam campaigns and malware attacks[58].

6.3. The European Arrest Warrant

The European arrest warrant is a decision issued by a judicial authority issued in a Member State of the European Union to have the person apprehended by another Member State and hand it over to the issuing judicial authority[59]. The primary purpose of the EAW is the conduction of the criminal proceedings and, also, the arrest and handover of the requested person to enforce a custodial measure and/or a custodial sentence[60]. In Hungary, the regulation was implemented with the Act CLXXX. of 2012 on the Cooperation in Criminal matters with Member States of the European Union.

It applies to offenses punishable by at least 12 months' imprisonment and penalties involving deprivation of liberty of at least four months. The arrest warrant only sets aside from double criminalization only in the case of cataloged offenses, but in those cases only, if the maximum sentence under the law of the issuing State reaches a term of imprisonment of at least three years[61]. Groups of cataloged crimes without the need for completeness: participation in a criminal organization, terrorism, trafficking in human beings, sexual exploitation of children and child pornography, illicit trafficking in arms,

---

[57] Péter, Fejes, 'Az Európai Unió, mint büntető joghatóság? [The European Union as a criminal jurisdiction?]' in Európai Jog [2005] 5.

[58] <https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime> accessed 19 September 2020

[59] László, Kőhalmi, 'Az európai bűnügyi együttműködés. [The European cooperation in criminal matters]' In: Ágnes Balogh – Mihály Tóth (eds.)*Magyar büntetőjog Általános rész.* (Osiris 2010) 390.

[60] Petra Bárd, '*Az európai elfogatóparancs Magyarországon. [The European arrest warrant in Hungary]*' (Országos Kriminológiai Intézet 2015) 26.

[61] Act CLXXX. of 2012, 3.§ (3)

munitions, and explosives, illicit trafficking in narcotic drugs and psychotropic substances, corruption, money laundering, intentional homicide, and cybercrime, but also the Council of European Union can extend the scope of cataloged criminal offenses[62]. Regarding the extradition, there are certain types of exceptions to the rules of the European Arrest Warrant, based on which the Metropolitan Court refuses (for mandatory reasons) or may refuse extradition (for optional reasons).

The mandatory grounds for refusal are set out in the 3rd subchapter of the Act CLXXX. of 2012, for example, if the requested person is not punishable due to childhood, or according to Hungarian law the punishability is expired, if the offense on which the European arrest warrant is based falls within Hungarian jurisdiction etc.[63]. Extradition shall also be refused if it was issued to enforce a decision rendered in the absence of the requested person, unless:

- the requested person has been duly notified,
- an authorized or seconded lawyer acted at the hearing on behalf of the requested person,
- the decision has been served, the person concerned has been duly informed about the remedies but has not exercised it or the decision has not been served to the requested person, but after the handover, it shall be served and the requested person shall be informed about the ordinary and extraordinary remedies and the deadline[64].

Besides, extradition should also be refused if the European arrest warrant has been issued to serve a custodial sentence or measure involving deprivation of liberty and the requested person is a Hungarian citizen who resides in the territory of Hungary. In this case, the Minister of Justice shall initiate (at the Member State) the taking over of the execution of the sentence or custodial measure of the sentenced person[65]. The act also summarizes in the same subchapter the optional grounds for refusal, in which cases the Metropolitan Court may decide on the execution or refusal of the European Arrest Warrant:

- if the arrest warrant relates to a criminal offense committed in whole or in part in the territory of Hungary[66], or
- if two or more Member States have issued a European arrest warrant against the same person, the Metropolitan Court shall decide, considering all the circumstances, which European arrest warrant should enjoy priority[67].
- If there are no grounds for refusal, a European Arrest Warrant can be requested. The application must include:
- the personal data and nationality of the requested person,
- name, address, telephone number, the e-mail address of the requesting authority,
- the arrest warrant, the evidence of the proceedings to be enforced, or any other judicial decision which they intend to enforce,
- the nature and legal assessment of the act committed,
- a description of the circumstances of the offense, including the time, place, and degree of guilt, and

[62] cf Bárd. (n 60) 25-27.
[63] Act CLXXX. of 2012, 5.§
[64] Act CLXXX. of 2012, 6.§
[65] Act CLXXX. of 2012, 8.§ (1)
[66] Act CLXXX. of 2012, 7.§
[67] Act CLXXX. of 2012, 9.§ (1)

- the penalty imposed, if there is already a final decision in the case, or, if not, the penalty which may be imposed in the Member State[68].

An application for a European Arrest Warrant may arise for several reasons, in particular for the investigation of a criminal offense, to enforce a final judgment or for pre-trial detention, providing an opportunity to fight transnational crime and other forms of crime more effectively.

VII. Conclusion

International cybercrime poses new challenges for states. In many cases, it can lead to the positive and negative collision of jurisdiction. While some jurisdictions have adopted cybercrime-specific jurisdiction rules, the principles underlying fair enforcement of criminal jurisdiction may also justify the enforcement of jurisdiction against internal and external criminals.

A clear set of rules at the EU level could serve as a compass for the Member States in matters of jurisdiction, but directives in this area do not make it entirely clear which state is entitled to act in a particular case. From an institutional point of view, however, Europol's coordinating work across national jurisdictions and its growing role in the European area can be seen as a positive outcome. In addition to Europol, the role of the European Arrest Warrant should also be emphasized in the fight against cybercrime, which is the basis for international criminal cooperation and the recognition of other Member States' jurisdictions.

The principles of jurisdiction are difficult to rank. In many cases, it may be case-specific to decide which principle of jurisdiction may be the best solution. It would be necessary to renew existing international legislation or to adopt the new convention that emphasizes the principle of citizenship or passive personality. Also, it is appropriate for the states to lay down specific rules. Adopting special laws for cybercrime, (as in the United States,) can also be a solution to jurisdictional issues[69].

References

1. Bárd P, *Az európai elfogatóparancs Magyarországon. [The European arrest warrant in Hungary]* (Országos Kriminológiai Intézet 2015)

2. Brenner S.W, 'Cybercrime jurisdiction.' Crime, law and social change. [2006]

3. Bruhács J, *Nemzetközi Jog I. Általános rész. [International Law I. General part.]* (Dialóg Campus Kiadó 2009)

4. Da-Yu K – Shiuh-Jeng W, 'The IP Address and Time in Cyber-Crime Investigation.' iPolicing: An International Journal of Police Strategies & Management 32, [2009]

5. Fejes P, 'Az Európai Unió, mint büntető joghatóság? [The European Union as a criminal jurisdiction?]' Európai Jog [2005]

6. Gál I. L, 'A pénzmosás szabályozásának régi és új irányai a nemzetközi jogban és az EU-jogban [The old and new tendencies in the regulation of money laundering in the international and EU Law]' Európai Jog. [2007]

[68] cf Nikač (n 53). 96.

[69] Réka Eszter, Gyaraki, *'A számítógépes bűnözés nyomozásának problémái. [The problems around the IT crimes investigation]'* (PTE-ÁJK 2019) 80.

7. Gál I. L, 'Jogszabálytan. [Legal dogmatics]' in Balogh Ágnes – Tóth Mihály, *Magyar Büntetőjog Általános Rész*. (Osiris 2015) 75-76.

8. Gál I. L, 'The Techniques of Money Laundering.' in István László, Gál – László, Kőhalmi (eds.), *Emlékkönyv Losonczy István professzor halálának 25. évfordulójára*. (Pécsi Tudományegyetem, Állam- és Jogtudományi Kar 2005) 129-138.

9. Gál I. L, 'Új biztonságpolitikai kihívás a XXI. században: a terrorizmus finanszírozása. [New challenges of security policy in the 21st century: the financing of terrorism]' Szakmai Szemle [2012] 5-15.

10. Gál István László, *A terrorizmus finanszírozása: Die Terrorismusfinanzierung, [The financing of terrorism]* (PTE Állam- és Jogtudományi Kar Gazdasági Büntetőjogi Kutatóintézet 2010)

11. Gyaraki R.E, *A számítógépes bűnözés nyomozásának problémái. [The problems around the IT crimes investigation]* (PTE-ÁJK 2019) 80.

12. Ibolya T, *A számítástechnikai jellegű bűncselekmények nyomozása [The investigation of IT crimes]* (Patrocinium Kiadó 2012)

13. Karoliny E, 'Igazságügyi együttműködés büntetőügyekben; a kölcsönös elismerés elve. A ne bis in idem elve az Európai Unió Bíróságának ítélkezési gyakorlatában. [Cooperation in criminal matters, the mutual recognition and the principle of ne bis in idem in The practice of the European Court of Justice]' in Mohay Ágoston – Szalayné Sándor Erzsébet (eds.): *Az Európai Unió Joga*. (Dialóg Campus Kiadó 2015)

14. Karsai K, 'A magyar büntető joghatóság [The Hungarian criminal law jurisdiction]' in Krisztina, Karsai (eds.) *Nagykommentár a Büntető Törvénykönyvhöz: Nagykommentár a Büntető Törvénykönyvről szóló 2012. évi C. törvényhez*, (Wolters Kluwer 2019)

15. Kőhalmi L, 'A nemzetközi bűnügyi együttműködés [The international cooperation in criminal matters]' in Ágnes, Balogh – Mihály, Tóth (eds), *Magyar büntetőjog Általános rész* (Osiris 2010)

16. Kőhalmi, L 'Az európai bűnügyi együttműködés. [The European cooperation in criminal matters]' In: Ágnes Balogh – Mihály Tóth (eds.) *Magyar büntetőjog Általános rész.* (Osiris 2010)

17. Ligeti K, *Büntetőjog és bűnügyi együttműködés az Európai Unióban [Criminal law and Cooperation in criminal matters in the European Union]* (Közgazdasági és Jogi Könyvkiadó 2004) 43.

18. M. Nyitrai P, *Nemzetközi és Európai Büntetőjog [International and European Criminal Law]* (Osiris 2006)

19. Maillart J, 'The limits of subjective territorial jurisdiction in the context of cybercrime' ERA Forum [2019]

20. Padfield N, 'Shining the Torch on Plea-Bargaining.' The Cambridge Law Journal [2009]

21. Perritt H, 'Jurisdiction in Cyberspace' Villanova Law Review [1996]

22. Polt P, 'A magyar büntető joghatóság. [The Hungarian criminal jurisdiction.]' in Polt et. al. (eds.) *A Büntető Törvénykönyvről szóló 2012. évi C. törvény nagykommentárja.* (Opten 2016)

23. Sántha F, 'A Nemzetközi Büntetőbíróság joghatóságába tartozó nemzetközi bűncselekmények vázlata [Outline of international crimes within the jurisdiction of the International Criminal Court Outline of international crimes within the jurisdiction of the International Criminal Court]' In Bragyova, András (eds.) *Tanulmányok a bűnügyi tudományok köréből.* (Gazdász Elasztik 2013)

24. Satzger H, *International and European Criminal law* (C.H. Beck, 2012)

25. Seker Ö. K, *International Regulation of National Cybercrime Jurisdiction*. (Tilburg University 2012)

26. Tóth M – Kőhalmi L, 'A szervezett bűnözés [The organized crime]' in Borbíró et. al. (eds.) *Kriminológia*. (Wolters Kluwer 2016)

27. Watson G.R, 'The Passive Personality Principle.' in Texas International Law journal [1993]

28. Wiener A. I,, 'A Nemzetközi Büntetőbíróság joghatóságáról' [About the jurisdiction of the International Criminal Court] Magyar Jog [2001]

The Refusal to Carry Out Unpaid Work for the Benefit of the Community by the Defendant – From Right to ”Procedural Trap”

Matei-Ciprian Graur*

Abstract

This approach starts from the regulation contained in Article 4 of the European Convention on Human Rights, which regulates as a fundamental right the prohibition of slavery and forced labour. The purpose of this right – the right not to work forcibly – is obvious, but the way in which Member States protect this right through domestic regulations can be different and can create controversy.

In our analysis we want to stop in criminal and criminal proceedings, being certain that other matters of law may face regulatory problems, but also considering that the scope of criminal law in general presents a series of hypotheses with special consequences, including, as we shall see, in the freedom of the individual. Far from wanting to find a clear solution to the problems that we will expose, we want to ask some questions regarding the internal protection offered in criminal law and criminal proceedings in relation to Article 4 of the Convention.

Does the legislator manage to be predictable? Is the right to refuse unpaid community service a "trial trap"? These are just two of a few natural questions raised as a result of the careful passage of the texts of law, but also from the analysis of case law in the matter.

Keywords: *Art. 4 ECHR, prohibition of forced labor, accused, right not to work, conditional freedom, suspension under supervision, postponement of penalty enforcement*

I. ECHR Standard Art. 4 – forced or compulsory labour

According to Articles 4 par. 2 and 3 of the European Convention on Human Rights, ”2. No one can be compelled to perform forced or compulsory labour. 3. 'forced or compulsory work' within the meaning of this Article shall not be considered as: any work normally imposed on a person subject to detention under the conditions laid down in Article 5 of this Convention or during his or her probation”.

For the purposes of this Convention, the term "forced or compulsory labour" means "any work or service claimed by an individual under the threat of any punishment and for which the name individual has not willingly offered himself". The Court adopted this definition as a starting point for the interpretation of Article 4 § 2 of the Convention (Graziani-Weiss against Austria; Stummer vs Austria (MC) and Adigüzel vs Turkey)[1].

Article 4 § 2 of the Convention prohibits forced or compulsory labour [Stummer vs Austria (MC)]. However, Article 4 does not define what is meant by 'forced or compulsory work', and the various Council of Europe documents relating to the

* Judge, Center for Research in Criminal Sciences, faculty of Law, West University Timisoara. Contact: matei.graur88@e-uvt.ro.

[1] Art. 4 ECHR guide, p. 8, www.ier.gov.ro, 13.12.2020.

preparatory work of the European Convention (Van der Mussele against Belgium, point 32) do not contain any guidance on this matter. In Van der Mussele v Belgium, the Court invoked ILO Convention No 29 on forced or compulsory labour. For the purposes of this Convention, the expression "forced or compulsory labour" means "any work or service claimed by an individual under the threat of any punishment and for which the name individual has not willingly offered himself". The Court adopted this definition as a starting point for the interpretation of Article 4 § 2 of the Convention (Graziani-Weiss against Austria; Stummer vs Austria (MC), and Adigüzel vs Turkey (paragraphs 26 to 27, and the caselaw cited there)[2].

Article 4 § 3(a) of the Convention states that the expression 'forced or compulsory work' does not include 'any work normally imposed on a person subject to detention' (Stummer vs. Austria (MC), point 119) or while he is on parole.

In determining what type of activity must be considered as 'work normally imposed on a person subject to detention', the Court shall take into account the standards prevailing in the Member States (point 128). For example, when the Court had to consider the work imposed on a repeat offender, whose release was conditional upon the accumulation of a certain amount of savings, although he admitted that the work in question was compulsory, found no infringement of Article 4 of the Convention on the grounds that the requirements laid down in Article 4 § 3(a) (Van Droogenbroeck against Belgium, point 59) were met. In the Court's view, the work imposed on him did not go beyond what was 'normal' in this context, since it was established to help him reintegrate into society and was legally based on provisions which have an equivalent in certain Member States of the Council of Europe (Stummer vs Austria (MC), point 121; De Wilde, Ooms and Versyp against Belgium, point 90][3].

As regards the remuneration of detainees, the Commission stated that Article 4 does not contain any provision concerning the remuneration of prisoners for the work carried out (Twenty-One persons held against Germany, the Commission's decision; Stummer vs. Austria (MC), point 122). The Court noted that there have been further developments in attitudes to this issue, reflected in particular in the European Prison Rules of 1987 and 2006, which require fair remuneration of the work of prisoners (Zhelyazkov against Bulgaria, point 36); Floroiu vs. Romania (point 34).

However, it considered that the mere fact that a prisoner was not paid for the work carried out does not, in itself, preclude the finding that such work constitutes 'work normally imposed on a person subject to detention' (paragraph 33). For example, in Floroiu against Romania, the Court noted that inmates could perform in prison either paid work or, as regards the day-to-day administration of the prison, unpaid work, but which granted the right to a reduction of the sentence. Under national law, detainees could choose between the two types of work after being informed of the conditions for each type of work. Given that the applicant has been granted a significant reduction in the remaining sentence to be served, the Court found that the work performed by the applicant was not deprived of any form of remuneration and that the work carried out by him can therefore be regarded as 'work normally imposed on a person subject to detention' within the meaning of Article 4 § 3(a) of the Convention (paragraphs 35-37)[4].

---

[2] *Ibidem.*

[3] Art. 4 ECHR guide, p. 11, www.ier.gov.ro, 13.12.2020.

[4] *Ibidem.*

In a case in which the complainant complained about the obligation of detainees to work in prison after they had reached retirement age, the Court, having regard to the purpose of the required activity, its nature and extent, as well as the manner in which it was to be carried out, and noting that there was no consensus among the Member States of the Council of Europe on this matter, decided that there could be no absolute ban on the existence of an absolute prohibition under Article 4 of the Convention, and that the work of the applicant could be considered in the meaning of the compulsory person concerned[5].

The imposition of unpaid work shall not constitute forced labour under Article 4(3) of the final sentence of the Convention.

Must a state of parole be given a *lato sensu* interpretation? Does it refer only to the situation following the conditional release and the completion of the term of punishment, or should it cover all situations where an obligation to work against a person is ordered as a result of the determination of his or her guilt as a result of an offense (e.g. in the case of ordering a solution to postpone the application of the penalty or suspended under supervision of the execution of the sentence)?

It is important to specify the position of the Constitutional Court which, by Decision no. 666/2018[6], established that the concept of "conditional freedom" used in Article 42 paragraph (2) letter b) of the Romanian Constitution is synonymous with that of "conditional freedom" contained in Art. 99-106 of the Criminal Code.

Therefore, the unpaid work of a convicted person cannot be regarded as being forced within the surveillance period set as a result of the order of conditional release.

The premised situation regulated by Art. 91 par. (1) lett. c) of the Criminal Code does not concern the conditional release, but the order of suspension of the service of the sentence under supervision, so that the exceptional situation related to the work performed during the period of conditional liberty is not incidental in question. Therefore, the Court finds that, in the event of ordering the suspension of the service of the sentence under supervision, any unpaid work for community service must be qualified as forced, in the absence of consent of the offender[7].

Thus, at least internally, we cannot establish as a similar situation unpaid community service during the term of conditional release and unpaid community service as a result of the suspended sentence under supervision of the sentence. As regards the second situation, the consent of the convicted person shall be required, contrary to being in the event of forced labour, thereby infringing, including Article 4 of the Convention.

II. Refusal to provide unpaid community work – a right or a procedural trap?

Under Art. 83 par. 1 lett. c Criminal Code, the court may order the postponement of penalty enforcement, establishing a period of supervision, if the following conditions are met: The offender has consented to perform unpaid community service, and according to Art. 91 par. 1 lett. c) Criminal Code, the court may order the suspension under supervision of execution of the penalty if the following conditions

[5] Art. 4 ECHR guide, p. 12, www.ier.gov.ro, 13.12.2020.
[6] Online at www.ccr.ro, 13.12.2020.
[7] Parag. 22 of Decision No. 666/2018 of the Constitutional Court.

are met: The offender has expressed his consent to perform unpaid community service.

Also, other European legislations have similar provisions. Thus, carrying out a comparative law study, the Constitutional Court[8] observes that in many European countries performing an unpaid work for community service, namely performing a "work of general interest" – in case of suspension of the service of the sentence under supervision, the conditional suspension of the execution of the sentence, the suspension of the trial with probation, substitution/replacement of penalty of fine or imprisonment, or as a primary or complementary punishment – is ordered by the court only with the consent of the convict.

Thus, in Albania, Article 63 of the Criminal Code stipulates that, in case of conditional suspension of penalty enforcement, the court may order, with the consent of the convict, the performance of unpaid work for community service. In Andora, according to Art. 49 par. 1 of the Criminal Code, community service consists of an unpaid provision of public utility services in favour of the state, other public institutions, associations or foundations, which always require the prior consent of the convict. In Armenia, Article 54 of the Criminal Code defines community service as the performance of authorised, unpaid and useful activity to society by a person convicted in his spare time, in accordance with the provisions of the local authorities. Community service is decided as an alternative to the prison sentence, with the written consent of the person to be convicted, given prior to the sentence. In Belgium, according to Article 375 of the Criminal Code, for less serious offences, the judge may issue a penalty for employment in the case of community service, stating in the sentence the amount of the fine or the length of the prison to be served in the event of non-compliance. This punishment may be applied at the initiative of the judge, prosecutor or defendant. Community service may be imposed only with the informed consent of the defendant, expressed directly or through intermediary. In Bosnia and Herzegovina, Art. 44 par. 1 of the Criminal Code stipulates that the court may order, with the consent of the convict, that the sentence of imprisonment under one year shall be replaced by community service. In Croatia, Art. 43 par. 2 of the Criminal Code stipulates that, in cases where the criminal fine cannot be paid, the court shall decide, with the consent of the convict, to replace this penalty with community service. In Estonia, Article 69 of the Criminal Code provides for the possibility of the court to substitute the penalty of imprisonment up to 2 years with unpaid work for community service, with the consent of the convict. In Finland, Section 11 of Chapter 6 of the Criminal Code provides for the possibility for the court to substitute the penalty of imprisonment for up to 8 months with community service, with the consent of the convict. In Luxembourg, Art. 22 of the Criminal Code stipulates that the court may order, in the case of offenses punishable by imprisonment under 6 months, that the convict performs unpaid work for community service, as a primary punishment. This measure cannot be taken with regard to a defendant who is not present at the hearing. Before the sentence is given, the president of the court must inform the defendant of his right to refuse the execution of community service[9].

Coming back internally, from our point of view, domestic legislation presents a vicious circle. In order to be able to order a solution to postpone the application of the

[8] Parag. 28 and following from Decision No. 666/2018 of the Constitutional Court.

[9] *Ibidem.*

penalty or to suspend under the supervision of the execution of the sentence, the defendant must agree to preset unpaid work for community service.

If the defendant refuses to agree to work, the court, if they find him guilty, will order a detention sentence, failing to meet the positive condition.

Subsequently, the defendant, permanently sentenced to a custodial sentence, is incarcerated and forced to perform certain household activities (which can often be the equivalent of unpaid community service).

Regarding the obligation of detainees to perform certain unpaid activities the European Court of Human Rights has consistently established that they do not violate the protection afforded by Article 4 of the Convention.

In fact, even Art. 4 of the Convention excludes from protection the case of activities performed by inmates, specific to the place of detention.

Where the Court had to examine the work imposed on a repeat offender, whose release was conditional upon the accumulation of a certain amount of savings, although it admitted that the work in question was compulsory, it found no infringement of Article 4 of the Convention on the grounds that the requirements laid down in Article 4 § 3(a) were met (Van Droogenbroeck, point 59). In the Court's view, the work imposed on him did not go beyond what was 'normal' in this context, since it was established to help him reintegrate into society and was legally based on provisions which have an equivalent in certain Member States of the Council of Europe (Stummer vs Austria (MC), point 121; De Wilde, Ooms and Versyp against Belgium, point 90].

Therefore, we can appreciate the fact that the condemned person, even if he refuses to work, will still work in the end. In these circumstances, we consider that we are in the situation of a procedural trap that can derive from both the manner of regulation and the way in which the possibility of refusal to work is presented to the defendant by the judicial bodies.

Is this refusal presented as a genuine right or is it presented as a condition without which the defendant will not be able to enjoy the gentler individualisation of the penalty, according to Art. 83 and 91 Criminal Code?

III. Internal jurisprudential controversies

By criminal decision no. 680/A/14.07.2020 Timisoara Court of Appeals accepted the appeal declared by the defendant C.C. against criminal judgment no. 970/27.03.2020 rendered by the Timisoara Court[10].

The defendant was sentenced by the first court to a sentence of execution under detention because the condition of the agreement to perform unpaid community service was not fulfilled, and he did not appear before the judicial bodies in order to express his consent to this effect.

However, the defendant was present before the appellate court, where he made a statement acknowledging the facts, filed an employment contract and requested a postponement of penalty enforcement.

Thus, the appellate court found that, given that more than 3 years have passed since the defendant committed the offense, who at that time was 30 years old, that he is a socially integrated person with a job, and the act for which he was convicted by the first instance represents an event isolated in relation to his conduct, that he is at

[10] Unpublished.

the first contact with the criminal law, it is necessary to change the solution of the first court and to punish the defendant by delaying the application of the penalty for a period of time.

In this respect, we note that the appellate court only changed the individualisation of the penalty given that during the appeal phase the defendant fulfilled the positive condition of giving his consent to perform unpaid work for community service, without which the court cannot order a solution to postpone the application of the penalty or to suspend under supervision of the execution of the sentence.

By criminal decision no. 791/A/05.09.2019 Timisoara Court of Appeals accepted the appeal declared by the defendant C.S.D. against criminal sentence no. 2502 of 19.07.2019 delivered by the Timisoara Court in case no. 3816/325/2018[11].

The defendant's chosen lawyer has requested the admission of the declared appeal and ordering the suspension of the execution of the sentence under supervision, taking into account the reduced gravity of the offense, the fact that the defendant has given her consent to perform unpaid work for community service and the mitigating circumstances provided for by Art. 75 par. 2 let. b Criminal Code, respectively the circumstances related to the committed act that diminish the seriousness of the offense or the danger of the offender.

It is also stated by the defendant's chosen lawyer that the damage was recovered in full and also that the conditions for ordering the suspension of the execution of the sentence under supervision and in first instance, with the exception of the defendant's agreement to perform unpaid community service, were met, which could not appear in order to give herself this agreement.

Also, the chosen lawyer shows that the defendant has admitted her crime since the criminal investigation and her mistake may also be blamed on her youth.

The prosecutor also placed conclusions to admit the appeal declared by the defendant, and the conditions for ordering a suspended sentence under supervision of the execution of the sentence were met.

The defendant said she was asking for a change in how to individualise the execution of the sentence.

We note that in both cases the appellate court abolished the judgment of the first court without finding an error of judgment, but, on the contrary, considering that, indeed, the substantive court had not fulfilled the positive condition that there was an agreement to perform unpaid work for community service, a condition subsequently fulfilled by presenting the defendants before the appellate court and expressing consent to work.

IV. Procedural problems

Therefore, the question of practitioners after the entry into force of the Criminal Code and the Code of Criminal Procedure was whether this agreement is necessary even if the court does not move towards a solution to postpone the application of the penalty in which to oblige the defendant to work unpaid for community service.

This litigation dilemma arose as a result of the non-binding disposition of unpaid work in the event of a postponement of penalty enforcement, as opposed to the suspension under supervision of the execution of the sentence.

[11] Unpublished.

We mention that it was attempted to validate or invalidate the imperative character of the agreement to work by the High Court of Cassation and Justice itself, but the complaint was rejected as inadmissible by decision no. 27 of 12.12.2017[12].

Before the Supreme Court, a preliminary ruling was sought to resolve the following issues of law in principle:

"- if the manifestation of the agreement to perform unremunerated community service by the defendant, provided by Art. 83 par. (1) lett. c) of the Criminal Code, is an imperative condition in order to be able to retain as being satisfied the conditions provided by Art. 83 of the Criminal Code for the postponement of the penalty application in the situation where the defendant does not present himself for trial in order to express his consent to perform unpaid work for the benefit of the community, and the court considers that no penalty is imposed on the provision of the obligation provided by the Community.

— if the manifestation of the agreement to perform unpaid work for community service by the defendant, provided by Art. 83 par. (1) lett. c) of the Criminal Code is an imperative condition in order to be able to retain as being fulfilled the conditions provided by Art. 83 of the Criminal Code for the postponement of penalty enforcement in the situation in which the defendant at the hearing shows that he does not give his consent to perform unpaid work for the benefit of the community, and the court considers that no penalty is required to establish the obligation stipulated by the letter provided by the law".

In relation to the method of formulation of the two questions by the referring court, which combines elements of fact and law or which concerns the specificities of the case concerning the presence/absence of the defendant from the appeal trial or the procedural position of the defendant in the sense of expressing the refusal to perform community service, the High Court of Cassation and Justice found that, in reality, it is not required to interpret legal provisions *in abstracto*, but a resolution of the substance of the case within the limits of the appeal procedure, which refers to the fact that the law of the court is not required to interpret legal provisions *in abstracto*, but a resolution of the substance of the case within the limits of the appellation, which refers to the condition of the court of appeal.

With regard to this solution, we consider that some ideas should be remembered from the prosecutor's conclusions at the time of the settlement of the referral of the High Court of Cassation and Justice[13].

Thus, it was stated by the prosecutor before the Supreme Court that "the postponement of the penalty enforcement has a double nature, by substantial law (a means of legal individualization of the sanction) and of procedural law (procedural solution of the criminal action under Art. 396 par. 4 of the Criminal Procedure Code).

As a means of individualization, the legislator imposed a number of conditions for the incidence of this institution. The inclusion of the consent of the offender to perform unpaid community service, as a subjective condition, among the conditions of incidence of the institution leads to a single conclusion, that it has the same legal value as the other conditions, that is, it is an imperative condition which must be fulfilled cumulatively, along with the others. Just as the absence of any of the conditions stipulated by Art. 83 par. 1 letters a, b, d of the Criminal Code prevents the incidence

[12] www.scj.ro, 20.12.2020.

[13] www.mpublic.ro, 02.01.2021.

of the postponement of penalty enforcement and the absence of the conditions stipulated by Art. 83 par. 1(c) of the same code has the same effect, regardless of the concrete form in which the absence of this condition may be materialized (the defendant, present at the resolution of the case, refuses to express any position on this issue or, expressly, shows that he does not express his consent, according to Article 378(3)).

Therefore, the conclusion of the imperative nature of the condition stipulated by Art. 83 par. 1 letter c of the Criminal Code results from the systematization of the regulation of the postponement of penalty enforcement.

In the context of characterizing the postponement of penalty enforcement as a means of individualization, based on whether or not the condition stipulated by Art. 83 of the Criminal Code is fulfilled, the judge has the possibility of valuing the conduct of the perpetrator also during the criminal trial, respectively his attitude towards the realisation of justice[14]. In the same sense, it was pointed out[15] that, even if the imposition of an unpaid work for the benefit of the community is optional, it is important the consent given by the defendant, an agreement meant to emphasize his desire to act for the benefit of the social order which he disturbed or[16] the conduct of the defendant is assessed in the light of some objectified elements, such as the agreement to perform work for the community, being obvious that the assessment of the postponement of penalty enforcement can be more easily used in the form of the disobedience of the criminal order.

Moreover, the doctrine expressly stated that, in the absence of such an agreement, it cannot be ordered to postpone the application of the penalty, even if the imposition of unpaid work for the benefit of the community is optional in nature[17].

Therefore, the condition stipulated by Art. 83 par. 1 letter c of the Criminal Code is not in an exclusive relationship, unequivocal with the obligation stipulated by Art. 85 par. 2 letter b of the same code, but is, first of all, in relation to the necessary conditionality with the very existence of the institution to postpone the application of the penalty. In other words, Art. 83 par. 1 letter c of the Criminal Code has, in relation to the institution of postponement of the penalty enforcement role as an imperative condition of its incidence/existence, and in relation to Art. 85 par. 2 letter b of the same code has the nature of a guarantee of compliance with Art. 4 paragraphs 2 and 3 ECHR.

A similar argument is represented by the provisions of Art. 378 par. 3 of the Code of Criminal Procedure, which provide that, in situations where the law provides for the possibility that the defendant may be obliged to perform an unpaid work for community service, he shall be asked whether he or she expresses his consent in this respect.

Therefore, the manifestation of the defendant in the specified sense must exist when there is a legal possibility, and not a judicial possibility (by the specific assessment of the court) to have applied the obligation to perform unpaid work for the benefit of the community.

---

[14] D. Nițu, *Cancellation of waiver and postponement of penalty enforcement. Incongruities in practical application,* Judicial Coordinator no. 3/2014, p. 162.

[15] A. Rasnita, *Delaying the penalty enforcement in the new Criminal Code*, Criminal Law No. 2/2013, p. 95.

[16] F. Ciopec, *Judicial Individualisation of Penalties*, CH Beck Publishing House, Bucharest, 2011, p. 410, 411.

[17] M. Udroiu, *Criminal Law, General Part*, Edition 3, CH Beck, Bucharest, 2016, p. 347; L.V. Lefterache in M. Udroiu (coordinator), *Criminal Code. Comments on articles*, Edition 2, CH Beck, Bucharest, 2016, p. 299.

Consequently, regardless of whether or not the court will establish the obligation stipulated by Art. 85 par. 2 letter b of the Criminal Code under the defendant, in order to order the postponement of the penalty, there must be the consent of the defendant to perform an unpaid work for community service.

Even the mere fact that the defendant is willing to perform unremunerated community service may be a catalyst in the process of establishing the opportunity to order a solution to postpone the application of the penalty, and it is not necessary to effectively perform work[18].

Therefore, it can be concluded that in the absence of this agreement, the defendant does not have the vocation to benefit from the postponement of the penalty, regardless of whether or not the court seeks to oblige him to perform unpaid work for the benefit of the community, the failure to fulfil this condition leading to the inapplicability of the institution".

V. Conclusions

Regardless of the position we mean to embrace – as a procedural trap or as a right, the way in which the defendant will relate to express the agreement to perform unpaid community service is based on the very way in which the judicial body presents the legal issue, before or during the hearing.

The good faith of the judicial bodies must prevail in this case, as agreement on unpaid work may raise issues of loyalty of the administration of proof to criminal procedural requirements in relation to the right to a fair trial.

That is why a mistake by the judicial bodies at this stage of the hearing can lead to a double violation of the standards imposed by the European Convention on Human Rights. On the one hand, the obligation to work unpaid for community service, without a valid agreement, leads to violation of Art. 4 of the Convention, and on the other hand, the honest failure to present the consequences of the absence of this agreement may outline a violation of Art. 6 of the Convention, given the loyalty of the administration of proof in the component of the defendant's declaration regarding the giving of consent to work.

In our conclusions we cannot fail to consider some of the arguments presented by the conclusion of 22 June 2017, delivered in Case no.2.048/197/2016, by which the Court of Appeal Brasov – Criminal Section notified the Constitutional Court with the exception of unconstitutionality of the provisions of Art. 91 par.(1) letter c) of the Criminal Code.

In order to justify the exception of unconstitutionality, the author states that, by obliging the defendant to obtain the consent of the defendant to perform community service, prior to the ruling on the defendant's guilt or innocence, the judge of the case is placed in the situation of pronouncing the defendant's guilt. The criticized provisions oblige the judge to seek the consent of the defendant to perform community service before remaining in judgment on the merits of the case, which is likely to affect the judge's impartiality, especially in cases where the defendant has not recognized the commission of the offence of which he is accused. If the defendant does not recognize the commission of the offence, his question by the judge about his consent to perform unpaid community

[18] Alexandru Rîşniţă, Ioana Curt, *Resignment of Punishment. Postponement of penalty enforcement*, Legal Universe, Bucharest, 2014, p. 160.

service may lead to the idea that the judge will order a solution to the conviction in question.

We appreciate the need for the legislator to consider whether or not order should be reversed. Thus, by law *ferenda*, we consider that it would be more appropriate for the agreement to work to be taken in the execution phase by the Probation Counsel and not by the court.

In support of this position, we can argue that the court should individualize the execution of the sentence according to the specific circumstances of the case, without negotiating with the defendant what way of individualization fits in the file (negotiation being specific to the criminal investigation phase, for example in the case of concluding a guilty plea).

Regardless of the solution adopted, what must be the first step in a possible change in the logic of agreeing to work is predictability. Therefore, the way in which the agreement to work will be taken must ensure that the defendant has a real representation of the consequences of a possible refusal. At the same time, we cannot fail to conclude our brief approach with a question: Is it fair that refusal to work should lead to punishment?

References

1. Ciopec, F., *Judicial Individualisation of Penalties*, CH Beck Publishing House, Bucharest, 2011.
2. Decision No. 666/2018 of the Romanian Constitutional Court, www.scj.ro.
3. ECHR guide, www.ier.gov.ro, 13.12.2020.
4. Nițu, D., *Cancellation of waiver and postponement of penalty enforcement. Incongruities in practical application,* Judicial Coordinator no. 3/2014.
5. Rîşniţă, A; Curt, I., *Resignment of Punishment. Postponement of penalty enforcement*, Legal Universe, Bucharest, 2014.
6. Rîsnita, A. *Delaying the penalty enforcement in the new Criminal Code*, Criminal Law No. 2/2013.
7. Udroiu, M. (coord.), *Criminal Code. Comments on articles*, Edition 2, CH Beck, Bucharest, 2016.
8. Udroiu, M., *Criminal Law, General Part*, 3rd edition, CH Beck, Bucharest, 2016.
9. www.ccr.ro, 13.12.2020.
10. www.mpublic.ro, 02.01.2021.

Necessity of the Regulation of Virtual Currency in Bosnia and Herzegovina in the EU Harmonisation Process

Goran Maričić*
Gojko Pavlović**

Abstract

Given the fact that most virtual currencies are not regulated by national governments, they are considered alternative currencies that exist outside the borders of national monetary policy. Therefore, the main goal of this study is to point out the basic specifics of virtual currencies and their legal status in the legislation of individual European countries through an analysis of available academic literature and positive legal regulations, with special reference to regulation at different authority levels in Bosnia and Herzegovina. Moreover, the purpose of this study is to point out the achieved European standards in this area, which should be followed by the legislation at different authority levels within BiH in the process of European integration.

Keywords: *virtual currencies, EU accession, lack of legal regulation.*

I. Initial considerations

Virtual currencies are alternative means of payment and a type of digital, predominantly unregulated money used to conduct transactions within a specific virtual community, which are not controlled by a country's central bank. The fast-growing market for these currencies has also brought to the fore the various terms used to describe the various products that all fall under the broader term cryptocurrency[1]. That is, this modern form of private money may have different names such as virtual, digital, alternative or cryptocurrencies, money or coins. The main conceptual difference between different types of virtual currencies lies in the possibility of their use in international business[2]. Behind the virtual currency stands a team of developers, and its value is determined in the market in a pure supply-demand relationship[3].

This raises the question of the legal status of virtual currencies in national legislations[4]. The problem is that in most countries there are no specific regulations related to virtual currencies. Also, the legal status of virtual currencies differ from

---

[1] Ehrenfeld, J., Gallagher, R., Lyon, M., Potter, T., Rosenblatt, J., 2019, „Panel: Legal issues surrounding blockchain, cryptocurrency, & bitcoin“, *Transactions: The Tennessee Journal of Business law*, Vol. 20, pp. 1135-1168.

[2] „*In the digital world, a distinction is made between virtual currency and cryptocurrency, coins, stablecoin, utility tokens and security-like tokens.*“Turudić, D.A, Milić, J., Štulina, K., 2017, „Korištenje kriptovaluta u medjunarodnom poslovanju“, *Zbornik sveučilišta Libertas*, Br.1-2, str 191-210.

[3] Radivojević, A., 2018, *Virtual Currency Development and Regulation, Foundation for the Development of Economic Science*, No. 29, pp. 61.

[4] See: The Law Library of Congress, *Regulation of Cryptocurrency Around the World*, June 2018, p.1. https://www.loc.gov/law/help/cryptocurrency/cryptocurrency-world-survey.pdf.

country to country and some countries therefore consider this currency a product, while others consider it an asset or financial instrument[5]. In this regard, states approach this issue in two ways: whether by defining the legal nature and regulatory status of virtual currency through existing financial regulations or by adopting new legal solutions on virtual currencies.

II. Regulation at the level of the european union and specific EU countries

At the European Union level, there have been attempts to regulate cryptocurrencies through the *Electronic Money Directive and the Payment Services Directive*, but it is argued that virtual currencies differ from electronic money in a way that, unlike electronic money, funds within virtual currencies are not denominated in a traditional unit of account rather but in a virtual unit of account. Therefore, cryptocurrencies should nevertheless remain outside these directives.

The first official definition of virtual currencies is set out in Directive (EU) 2018/843, better known as the Fifth Anti-Money Laundering Directive[6]. According to the definition in Directive (EU) 2018/843, "Virtual currencies represent a digital display of value that is not issued by the Central Bank". The Central Bank or public body does not guarantee transactions and payments in virtual currency. Also, virtual currencies do not have the legal status of currency or money, but natural or legal persons accept it as a means of exchange and it can be transferred, stored and traded electronically[7].

However, this definition of virtual currency is function-based and no distinction is made as to whether virtual currencies are generated by a crypto mining process or by exchanging goods or services using blockchain technology[8].

Thus, for example, amendments to the Austrian Law on the Prevention of Money Laundering and Terrorist Financing in Financial Markets (Finanzmarkt-Geldwäschegesetz – *FM-GwG*) implemented Directive (EU) 2018/843 into Austrian legislation and adopted a definition of virtual currency in accordance with Article 1. Paragraph 2 (d) of the Directive. However, there are no specific regulations regarding investments in virtual currencies in Austria. Virtual currencies are not formally money, nor are they a means of payment in Austria The transactions involving virtual currencies are subject to existing legal provisions[9].

---

[5] Tomć, K., 2020, „Pravno reguliranje virtualnih valuta u Austriji i ostalim zemljama članicama Uuropske unije“, *Zbornik radova Usaglašavanje pravne regulative sa pravnim tekovinama Evropske unije*, godina 4, broj 4, str. 370-384.

[6] Directive (EU) 2018/843 of the European Parliament and of the Council from May 30, 2018 amending Directive (EU) 2015/849 on the Prevention of the Use of the Financial System for the Ppurpose of Money Laundering or Terrorist Financing and amending Directives 2009/138 / EC and 2013/36 / EU, Official Journal of the European Union L 156/43.

[7] Article 1, paragraph 2, point (d) of Directive (EU) 2018/843.

[8] Tomić, K., 2018, „Blockchain tehnologija, pametni ugovori i njihova implementacija u industriji osiguranja“, *Zbornik radova Pravo i praksa osiguranja –izazovi, nove tehnologije i korporativno upravljanje*, str.133-144.

[9] In relation to Bitcoin business, the Austrian Financial Market Authority (FMA) explicitly states in its report that “Bitcoin is not unregulated.” A similar rationale should apply to other virtual currencies. https://www.fma.gv.at/en/cross-sectoral-topics/fintech-navigator/bitcoin-co/ (the last visit to website on February 23, 2020).

In this regard, the existing taxation system in Austria applies to the taxation of transactions in virtual currencies. For example, in the case of the sale of Bitcoin within one year from the date of purchase, there is an obligation to pay personal income tax (*Einkommensteuer*) because this type of purchase is considered speculative. On the other hand, virtual currency mining falls under the commercial activity (*gewerblicheTätigkeit*) in which new value is created. This activity falls under taxation like any other creation of new values. Trade in virtual currencies can be viewed as trade in any other goods, and to perform the activity of trade it is necessary that a legal entity or a natural person – an entrepreneur meets the general conditions for performing the activity. Cryptocurrency mining imposes obligations to obtain a license to conduct trading activities. This is related to the much more complex question of whether cryptocurrencies should be viewed as commodities or currencies. If we look at cryptocurrencies as currencies, mining with cryptocurrencies would be an illegal banknote production activity over which the state has a monopoly. It would be more correct to view cryptocurrencies, as commodities and mining cryptocurrencies, as a trading activity because there is no source that claims that cryptocurrencies are completely illegal and that it is a violation of monopoly[10].

On the other hand, in FR Germany there is still no specific regulatory framework for virtual currencies and virtual assets, and instead the laws are used that regulate the financial sector. Different types of virtual currencies, virtual financial assets, innovative technologies and services fall under the law regulating the capital market, banking, financial services, anti-money laundering and other laws[11]. The classification of virtual currencies by a certain type of money in FR Germany has the consequence that virtual currencies are considered like foreign currencies. Therefore, income or profit from the sale of virtual currencies within one year from the acquisition of the currency is considered taxable income. Income or profit from the sale or purchase of virtual currency after one year from the purchase of currency[12].

German law does not provide for a general ban on the issuance, crypto mining, delivery and trading of virtual currencies. However, in cases of investments and transactions in virtual currencies, the provisions related to licensing are applicable. From a technical legal perspective, in 2013 the German financial supervisory authority *BaFin* (*BundesanstaltfürFinanzdienstleistungsaufsicht*) classified virtual currencies as financial instruments in Article 1 Paragraph 1. within the German Banking Act (*Kreditwesengesetz*) Virtual currencies fall into the subcategory of so-called "Units of Measurement" (*Rechnungseinheiten*), which are a special national category of financial instruments and which are not based on EU law.

Observing the surrounding countries, Slovenia has gone the furthest in terms of the legal regulation of this area. Thus, according to the standard classification, the cryptocurrency mining in Slovenia is one of the activities of data processing and related activities, whilst trade in cryptocurrencies is classified among other unclassified supporting business activities. Digital currencies can be purchased over 300 locations through the "Elipay" Platform and they have recently started doing business in Croatia. Also, there are online services in Serbia where you can buy and

---

[10] Tomć, K., 2020, Pravno reguliranje virtualnih valuta u Austriji i ostalim zemljama članicama Uuropske unije, *op. cit.,* str. 370-384.

[11] Arsov, A., 2017, „Bitcoin as an Innovative Payment Currency in Germany: Development of the e-Gold Standard“, *Journal of International Business Research and Marketing,* Volume 2, Issue 2, pp. 33-42.

[12] Čičin-Šain, N., 2017, „Oporezivanje bitcoina“, *Zbornik Pravnog fakulteta Zagreb*, Vol. 67, No. 3-4, str. 655-693.

sell cryptocurrencies, and they also have ATMs in several cities such as Belgrade, Novi Sad, Nis, Subotica and Inđija, where cryptocurrency is bought and sold for cash.

One of the main issues that arise in connection with the use of virtual currencies in everyday life is certainly the issue of paying taxes in the process. It should be noted that in answering this question, the challenge is how to categorize the virtual currencies and specific activities that are related to cryptocurrencies for tax purposes. This is important because profit from mining or selling cryptocurrencies will be categorized as income or capital gain and will affect the type of tax as well as determination of the tax base[13]. For example, some European Union countries have categorized cryptocurrencies differently for tax purposes: Bulgaria – taxed as a financial asset, Denmark – subject to personal income tax, Spain – subject to corporate income tax, United Kingdom – corporations and companies pay corporate income tax, individuals pay capital gain tax etc.

III. Current Situation In Bosnia And Herzegovina

In Bosnia and Herzegovina, i.e. on different authority levels there is no law or any other kind of regulation that specifically regulates cryptocurrencies, nor recognizes their status as money. Also, there is currently no law in the procedure that would specifically regulate this area. Also, there is currently no pending law procedure that would specifically regulate this area. However, trading and possession of cryptocurrencies is not illegal, i.e. the acquisition and holding of cryptocurrencies, as well as their trading, is not prohibited in Bosnia and Herzegovina, but is simply not defined. Therefore, all natural or legal persons who decide to do business with cryptocurrencies in BiH, they operate at their own risk.

At the same time, cryptocurrencies are present in Bosnia and Herzegovina and an increasing number of companies are connecting buyers and sellers of cryptocurrencies precisely due to the lack of legal regulations. In this regard, in 2017, the first non-profit educational forum Crypto.ba was established. On the other hand, the first crypto exchange in Bosnia and Herzegovina was established in mid-2018, and it is BCX *(Balkan Crypto Exchange)* situated in Banja Luka. This is the first platform in Bosnia and Herzegovina for buying, selling, exchanging, trading, storing and managing digital assets i.e. cryptocurrencies[14].

If viewed from a legal angle, cryptocurrency is subject to the division of things as *res in commercio* – a thing that is the subject of legal affairs; *res incorporales* – as a virtual, incorporeal thing, and as *res mobiles* – a movable thing. It is of a financial nature, and by selling / exchanging it on the market, natural and / or legal persons gain a certain financial benefit. Regarding the legal nature of cryptocurrencies, and analyzing the possible accounting treatment of cryptocurrencies, it should be emphasized that in accordance with International Accounting Standards, cryptocurrencies can not

[13] The Law Library of Congress, *Regulation of Cryptocurrency Around the World*, June 2018, pp. 2-3.

[14] It is also interesting to mention is that the largest cryptocurrency dispute in the region, and perhaps beyond, is currently being conducted before the District Commercial Court in Banja Luka. Namely, the company "Bitminer Factory" from Gradiška is demanding from "Unicredit Bank" Banja Luka one hundred million dollars (about 180 million marks) because the company believes that the Bank is the main culprit for the failure of the project based on "blockchain" technology, which this company intended to implement in Republic of Srpska. In the particular case, UniCredit Bank a.d. Banja Luka unilaterally closed the account of the company "Bitminer Factory" with the explanation that in accordance with the business policy they do not do business with companies that deal with cryptocurrencies.

be considered cash (according to IAS 7), can not be considered a financial instrument (according to IAS 32), can not be considered property, plant or equipment (according to IAS 16) and can not be considered inventories (according to IAS 2)[15]. However, cryptocurrencies can be viewed as intangible assets[16]. For example, International Accounting Standard – IAS 38 defines intangible assets as non-monetary assets without identifiable physical substance.

With regards to that, and from the perspective of corporate income tax when disposing of intangible assets or their retirement/decommissioning, the difference between the book value of an asset at the moment of its derecognition and the net inflow resulting from the disposal of the intangible asset, shall be deemed as a gain or loss. Booking is carried out by crediting the corresponding account where the intangible assets are recorded (and possibly debiting the corresponding allowance account) and the corresponding disposal receivables (e.g. domestic trade receivables etc.), and the difference is credited or debited to the other income account group or other expense account group. The Organisation, in accordance with IAS 38, should assess whether the lifetime of an intangible asset is limited or unlimited. Although companies in both FBiH and RS are treated with two different corporate tax laws[17]. there is essentially no tax difference for companies, based on their headquarters.

Considering the value added tax, it should be noted that the provisions of Article 3 of the Law on Value Added Tax[18] stipulate that the subject of VAT are supplies of goods and services (hereinafter: supply of goods and services) which a taxpayer, within the performance of his economic activities, makes for consideration within the territory of Bosnia and Herzegovina, as well as the importation of goods into Bosnia and Herzegovina. According to the provision of Article 4, Paragraph 1 of the Law, the supply of goods, within the meaning of this Law, is the transfer of the right to the disposal of items (hereinafter: goods) to the person who may dispose of these goods as owner. According to the provisions of Article 8, Paragraph 1 of the Law, the supply of services, within the meaning of this Law, are any operations and actions carried out within the performance of an economic activity, which does not constitute a supply of goods referred to in Articles 4 – 7 of this Law. Cryptocurrencies, in their essence, represent virtual money, which is not approved by the competent state authorities i.e. do not represent legal tender. Having in mind the above provisions of the Law governing the subject of VAT taxation, as well as the essence of cryptocurrencies, the sale of virtual currency is not subject to taxation, since the fee earned on that basis does not constitute a fee for taxable supply of goods or services. Namely, in its essence, the sale of cryptocurrencies has the same character as the sale of value vouchers, based on which voucher holders can buy goods or receive services. Moreover, the purchase of cryptocurrencies does not represent an advance payment, since the purchase of cryptocurrencies does not represent a fee for certain future turnover of goods and services (when selling cryptocurrency it is not known which

---

[15] https://unija.com/bs/kriptovalute-u-bosni-i-hercegovini/ pristup decembar 2020.godine.

[16] Compare: Bolotaeva O.S., Stepanova, A.A., Alekseeva, S.S., 2019, „The Legal Nature of Cryptocurrency", International science and technology conference Earth and Environmental Science, 272 (2019) 032166, pp. 1-5.

[17] Corporate Income Tax Law of the Republic of Srpska („*Official Gazette of the Republic of Srpska*", No.: 94/ 2015, 1/2017 and 58/2019). Corporate Income Tax Law of the Federation BiH („*Official Gazette of the FBiH*", No.: 15/ 2016 and 15/2020).

[18] Law on Value Added Tax in Bosnia and Herzegovina („Official Gazette of the BiH", No. 9/2005, 35/2005, 100/2008 and 33/2017).

goods or services will be delivered, at what tax rate will be taxed etc.). VAT treatment is not affected by whether the cryptocurrency is sold in Bosnia and Herzegovina or abroad[19].

It is to be stressed that a similar view was taken by the European Court of Justice on October 22, 2015, when answered the question in regard the VAT taxation of the service of exchanging traditional currency for cryptocurrency and vice versa, answering the Swedish court's question whether these transactions can be exempted from the taxation of VAT prescribed by national legislation as well as the exceptions to the EU VAT Directive 2006/112 / EC in which it took the view that certain provisions of Article 135 of the Directive should be interpreted in such a way that such supplies do not fall within the scope of those provisions.

It should be emphasized that a similar understanding was taken by the European Court of Justice when on October 22, 2015 it answered the question of value added tax on the service of exchanging traditional currency for cryptocurrency and vice versa, answering the question of the Swedish court whether these transactions can be classified as exemptions from VAT prescribed by national law and exemptions from the EU VAT Directive 2006/112 / EC in which it took the view that certain provisions of Article 135 of the Directive should be interpreted in such a way that such supplies of services do not fall within the scope of those provisions.

The Personal Income Tax Law, neither in the Federation of BiH, nor in the Republika Srpska, does not explicitly prescribe the method of taxation, and in connection with possible legal and tax treatments and the framework of income from the sale of cryptocurrencies[20]. However, bearing in mind the extent of general provisions of these laws, it is possible that this type of income might be classified under the income most analogous to it.

Thus, for example, according to the provisions of the Personal Income Tax Law in the Federation of BiH, cryptocurrencies can not be considered income from capital because the Law specifies the categories of income that are considered income from capital, and cryptocurrencies can not be classified under any of category. Also, this type of income can not be considered as capital gains. On the other hand, the Personal Income Tax Law in the Republic of Srpska prescribes somewhat more categories of taxation. However, taking into account all of the above, income from the sale of cryptocurrencies, from the aspect of the Law on taxation of personal income of the citizens, could most closely be subject to taxation from non-self-employed activities i.e. other income at a rate of 10%. In that connection, this type of income would be included in the sum of income that is subject to taxation by the annual personal income tax of citizens.

IV. Concluding remarks

The legal system of a country is a system of rules and norms that regulate the behavior of citizens and which seeks to cover the most diverse life situations of its citizens. Therefore, the generality of certain norms in that system guarantees the possibility to bring under them the widest possible number of real events. However,

[19] https://unija.com/bs/kriptovalute-u-bosni-i-hercegovini/ website visited in December 2020..

[20] Personal Income Tax Law of the Republic of Srpska Srpske („*Official Gazette of the Republic of Srpska*“, No.: 60/ 2015, 5/2016, 66/2018 and 105/2019). Personal Income Tax Law of the Federation BiH („*Official Gazette of the FBiH*“, No.: 10/2008, 9/2010, 44/2011, 7/2013 and 65/2013).

the fact that something is not regulated by positive legal regulations does not affect the existence and development of it in the real world. The situation is the same with virtual currencies.

Some research indicates that the response of countries in the world in relation to the appearance of virtual currencies ranges from countries that completely ban their use (Egypt, Iraq, Morocco, Pakistan etc.), through countries that try to through existing tax legislation (e.g. Austria, Germany, Finland, Italy, Poland, Romania, Spain etc.) or legislation in the area of prevention of money laundering and financing of terrorist activities (Czech Republic, Estonia, Luxembourg) resolve this issue, to countries that enact special laws to regulate this area and fully support the use of virtual currencies in everyday life, and even develop their own or regional virtual currencies (e.g. Ireland, Lithuania, China).

Currently in Bosnia and Herzegovina, at all authority levels, there is no special legal framework for regulating transactions made in cryptocurrencies, which define their concept and status. Therefore, due to the lack of regulation, cryptocurrency payment takes place in a market that is in some way beyond the reach of the tax authorities, because the laws on personal and corporate income tax do not regulate this area in a precise way in Bosnia and Herzegovina. Also, the Law on Prevention of Money Laundering and Terrorist Financing is currently not harmonized with the so-called the 5th EU Directive in this area. However, a cross-sectoral working group has been established which in the coming period should, in accordance with commitments arising under Negotiating Chapter 4 in the process of EU integration, propose amendments in line with the Directive or adoption of a new piece of legislation[21].

Firstly, in this regard, it would be good to define the concept of blockchain technology and cryptocurrencies at various levels of government in Bosnia and Herzegovina and then specifically regulate them since they represent this new fact in the real world, that is, our everyday life that should be covered by the legal system. Until then, the existing tax legislation should certainly be applied.

In the event of future standardization, issues related to decentralization and anonymity should certainly be taken into consideration, in the sense that there are no intermediaries in transactions related to virtual currencies, that transactions do not contain personal data, and that the competent authorities cannot currently monitor transactions or stop the conclusion of transaction. In this regard, it is necessary to regulate this area in accordance with the adopted standards of the European Union for the prevention of money laundering and financing of terrorist activities, in a way that the identity of traders is known, and that trading platforms exercise due supervision over their clients.

References

1. Arsov, A., 2017, „Bitcoin as an Innovative Payment Currency in Germany: Development of the e-Gold Standard“, *Journal of International Business Research and Marketing,* Volume 2, Issue 2, pp. 33-42.

2. Bolotaeva O.S., Stepanova, A.A., Alekseeva, S.S., 2019, „The Legal Nature of Cryptocurrency“, *International science and technology conference Earth and Environmental Science*, 272 (2019) 032166, pp. 1-5.

[21] Law on money laundering and financing of terrorist activities („Official Gazette of the BiH“ No. 47/14 and 67/16)

3. Ehrenfeld, J., Gallagher, R., Lyon, M., Potter, T., Rosenblatt, J., 2019, „Panel: Legal issues surrounding blockchain, cryptocurrency, & bitcoin“, *Transactions: The Tennessee Journal of Business law*, Vol. 20, pp. 1135-1168.

4. Turudić, D.A, Milić, J., Štulina, K., 2017, „Korištenje kriptovaluta u medjunarodnom poslovanju“, *Zbornik sveučilišta Libertas*, Br.1-2, str 191-210.

5. Radivojević, A., 2018, *Virtuelne valute razvoj i regulacija*, Fondacija za razvoj ekonomske nauke, br. 29.

6. The Law Library of Congress, *Regulation of Cryptocurrency Around the World*, June 2018.

7. Tomć, K., 2020, „Pravno reguliranje virtualnih valuta u Austriji i ostalim zemljama članicama Uuropske unije“, *Zbornik radova Usaglašavanje pravne regulative sa pravnim tekovinama Evropske unije*, godina 4, broj 4, str. 370-384.

8. Tomić, K., 2018, „Blockchain tehnologija, pametni ugovori i njihova implementacija u industriji osiguranja“, *Zbornik radova Pravo i praksa osiguranja –izazovi, nove tehnologije i korporativno upravljanje*, str.133-144.

9. Čičin-Šain, N., 2017, „Oporezivanje bitcoina“, *Zbornik Pravnog fakulteta Zagreb*, Vol. 67, No. 3-4, str. 655-693.

10. Directive (EU) 2018/843 of the European Parliament and the Council since May,30 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purpose of money laundering or terrorist financing and on amending Directives 2009/138 / EC and 2013/36 / EU, Official Journal of the European Union L 156/43.

11. Corporate Income Tax Law of the Republic of Srpska („*Official Gazette of the Republic of Srpska*“, No.: 94/ 2015, 1/2017 and 58/2019). 11. Corporate Income Tax Law of the Federation BiH („*Official Gazette of the Federation of BiH*“, No.: 15/ 2016 and 15/2020).

12. Law on Value Added Tax in Bosnia and Herzegovina („*Official Gazette of the BiH*“, No. 9/2005, 35/2005, 100/2008 and 33/2017).

13. Personal Income Tax Law of the Republic of Srpska („*Official Gazette of the Republic of Srpska*“, No.: 60/ 2015, 5/2016, 66/2018 and 105/2019).

14. Personal Income Tax Law of the Federation BiH („*Official Gazette of the Federation of BiH*“, No.: 10/2008, 9/2010, 44/2011, 7/2013 and 65/2013).

15. Law on money laundering and financing of terrorist activities („*Official Gazette of the BiH*“ No. 47/14 and 67/16).

16. https://www.loc.gov/law/help/cryptocurrency/cryptocurrency-world-survey.pdf

17. https://www.fma.gv.at/en/cross-sectoral-topics/fintech-navigator/bitcoin-co/

18. https://unija.com/bs/kriptovalute-u-bosni-i-hercegovini/ website visited in December 2020.

Implications of New Technologies on Criminal Justice System

Marina Matic Boskovic*

Abstract

The crime landscape has changed tremendously in the past years due to advancement in technology. The technological innovations from the end of XX century have transformed nearly every component of the criminal justice system. Technology has become a key component of most criminal activities and enables significant level of flexibility for criminals. Technology also significantly supports law enforcement authorities in prevention, detection, investigation, prosecution and enforcement of criminal sanctions. The author in the paper analysis the key benefits of the new technology for efficiency of the criminal justice system, as well as areas of human rights concern. Special area of concern is use of artificial intelligence and predictive models in the policing, investigation and enforcement of criminal sanctions. Some of the new technology were already part of the European Court of Human Rights jurisprudence and developed standards should be embedded in the legislation. The needed balance between human rights protection and efficiency of criminal investigations could be established through comprehensive assessment of the new technology prior to its adoption by policy makers. In addition, the evaluation system has to be established to monitor application of the new instruments in practice and enable timely review of instruments in case of human rights infringement.

Keywords: *technology, human rights, cybercrime, predictive models, internet, criminal justice*

I. Introduction

The development and extensive use of information and communication technologies has generated new forms of crime or new forms of perpetrating crimes and consequently new types of evidence[1]. Starting in the 1980s, personal computers became available for home use, and as of 2019, 83 percent of households in the European Union had access to a personal computer, while in Serbia 73 percent of household had at least one computer[2]. As a consequence of advancement of computer technology today we have global banking, in which complex transactions can be

* Research Fellow, Institute for Criminological and Sociological Research, Belgrade, Republic of Serbia. Contact: m.m.boskovic@roldevelopmentlab.com.

[1] Evidence – European Informatics Data Exchange Framework for Courts and Evidence – Overview of existing legal framework in the EU Member States, 2015, available at: http://s.evidenceproject.eu/p/e/v/evidence-ga-608185-d3-1-411.pdf 26.12.2020.

[2] Proportion of households having access to a personal computer 2014-2019, (2020) Eurostat, available at: https://ec.europa.eu/eurostat/statistics-explained/index.php? title=File:Proportion_of_households_having_access_to_a_personal_computer,_2014_and_2019_(%25)_CPC20.png 25.12.2020.

completed electronically. Information is also available to us more quickly due to development of internet. By 2019, the share of EU households with internet access had raisin to 90 percent and in Serbia to 80 percent[3]. Certainly, these advances in technology have changed the life.

Offenders very quickly integrate new technologies in their operations. The use of new technologies is especially spread among organized criminal groups and includes cybercrime, online trade of illicit goods and services, use of encrypted communication channels by criminals for impediment of detection, investigation and prosecution of crime, new forms of payment such as crypto currencies etc.[4].

Advancement of technology also put in the risk consumers who are exposed to online scams and fraud, which can affect consumer confidence and could lead to a reduction in consumer expenditure and function of digital market. Recently conducted survey in EU on Scams and Fraud Experience by Consumers, showed that slightly more than half of Europeans personally experienced one of the types of scams and fraud[5] in the last two years, when purchasing goods or services[6]. As a consequence there is substantial level of concern among online consumers about potential misuse of their personal data or theft of their credit card details[7]. It is estimated that in the EU adult population incurred 24 billion EUR of financial losses resulting from scams and fraud over a two-year period[8].

Technologies also facilitated prevention, detection, investigation, prosecution and enforcement of sanctions[9]. With most of lives organized online, especially in time of COVID-19 pandemic and introduced restrictions, people are using latest technologies to communicate with friends, families and colleagues. Many countries introduced e-government to more efficiently interact with citizens and businesses. Spread of the technology has a consequence creation of digital traces. Criminal activities are also conducted using ICT and evidence in criminal cases nowadays are very often in electronic form. The electronic evidence has to be handled by using specific methods to secure its authenticity and integrity, since it can be easily modified, overwritten or deleted[10].

Recent decades have seen the emergence of closed-circuit television (CCTV) surveillance as a mainstream crime prevention measure used around the world. Use of CCTV is based on the crime prevention strategy by reducing criminal opportunities and increasing the perceived risk of offending through modification of the physical

---

[3] Digital economy and society statistics – households and individuals, (2020) Eurostat, available at: https://ec.europa.eu/eurostat/statistics-explained/index.php/Digital_economy_and_society_statistics_-_households_ and_individuals#Internet_access 25.12.2020.

[4] Crime in the age of technology, (2017) Europol, 3.

[5] Types of scams and fraud that were included in the survey includes buying scams, identity thefts and monetary fraud.

[6] Survey on Scams and Fraud Experienced by Consumers – Final Report, January 2020, European Commission, 10.

[7] The 2015 DG JUST study on "Perceived and actual barriers with online (cross-border) purchases" found that 30% of online consumers were concerned that personal data may be misused and 25% that payment card details may be stolen while shopping online domestically.

[8] Survey on Scams and Fraud Experienced by Consumers – Final Report, 15.

[9] Smith, G. R, (2007) Crime Control in the Digital Age: An exploration of Human Rights Implications, *International Journal of Cyber Criminology*, Vol. 1, Issue 2, 167-179.

[10] United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime, draft February 2013, 157.

environment[11]. Findings of the assessment show that CCTV is associated with a significant and modest decrease in crime[12]. Surveillance technology can also enhance the investigation of crime.

Computers will offer nearly unlimited possibilities for aggregating information and sharing it with other criminal justice agencies. Due to development of technology within the European Union the Prüm Decision allows the exchange of basic fingerprints, DNA and vehicle registration data[13].

New technologies are also used in trials and in judicial decision making-for example, computer models based on social science research are used in assessing the likelihood of recidivism. The Correctional Offender Management Profiling for Alternative Sanctions (COMPAS) tool produces a risk score that predicts a person's likelihood of committing a crime in the next two years and is widely used by courts across the USA[14].

COVID-19 pandemic and measures of social distancing have impact on court operations. Majority of countries were looking for solutions that would limit interaction with courts and suspension of non-urgent cases was one of the applied measures. To enable functioning of the courts, countries where level of information technology development allowed introduced modalities of online hearings and/or other use of modern technologies during proceedings like electronic filing[15].

The new technologies such as electronic bracelets are being used in corrections. Electronic monitoring has been used in Europe since the 1990s and continues to expand[16]. It is predominantly been used to enforce curfews and home detention, but newer technologies are emerging and can help create and monitor exclusion zones.

Although technologies enabled criminal justice authorities to prevent and investigate crimes and offered many protections for suspects and accused persons, risks of violation of human rights have arisen from the modalities of law response to cybercrime.

The policy makers sometimes include novelties attracted by development and efficiency of technology without thorough assessment of influence on human rights. Fundamental rights, democracy and the rule of law need to be protected in cyberspace while protecting against incidents, malicious activities and misuse[17]. These rights and freedoms also include the right to a fair trial, in particular when preparing a defense case where electronic evidence is included.

---

[11] Clarke, R.V. (1995) Situation crime prevention, *Crime and Justice*, Vol. 19, 90-160.

[12] Piza, E., Welsh, B., Farrington, D. and Thomas, A. (2019) CCTV Surveillance for Crime Prevention: A 40-Year Systematic Review with Meta-Analysis, *Criminology and Public Policy,* Vol 18, Issue 1, 135-159.

[13] Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime; Council Decision 2008/616/JHA of 23 June 2008 on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime.

[14] Brennan, T., Dieterich, W., Ehret, B., (2009) Evaluating the predictive validity of the COMPAS Risk and Needs Assessment System, *Criminal Justice and Behavior,* Vol. 36, Issue 1, 21-40.

[15] Kostic, J., Matic Boskovic, M., (2020) How COVID-19 Pandemic influences Rule of Law backsliding in Europe? In. M. Reljanović (ed.) Regional Law Review, Institute of Comparative Law, Belgrade, 77-91.

[16] Nellis, M., (2014) Understanding the electronic monitoring of offenders in Europe: expansion, regulation and prospects, *Crime, Law and Social Change*, Vol. 62, Issue 4, 489–510.

[17] Joint communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace [2013] JOIN(2013) 1 final, p. 2.

In the article benefits of use of new technologies will be briefly assessed as well as challenges in using technologies in regard to human rights protection.

II. Benefits of use of new technologies

The benefits of the new technologies for prevention, detection, prosecution and enforcement of criminal sanctions are without doubts. Several analyses confirmed that use of technology contributed to all segments of the criminal justice system.

The new technology and tools are used for the prevention of crime, through predictive models that use geospatial modeling for predicting future crime concentrations[18]. The police in USA are using tools of data mining, machine learning and artificial intelligence to make accurate predictions and applied it to human resource management[19].

Police across the world are using artificial intelligence tools to detect the preparatory phase of crime. Technology tools are using large amount of data that are collected and supposed to excavate planners of crimes which are yet to be committed. The tools are also used to detected already committed crimes based on database that contain information on victims, perpetrator, risky places, or other items, such as background noise in the video[20].

The new technologies are also used by courts to assess the likelihood of recidivism and the likelihood of those awaiting trial to escape, or of offenders in bail and parole procedures. The courts in the USA are using different software for analysis of likelihood and predictions.

The use of CCTV as tool for prevention of corruption resulted in the decrease of crime rate, dure to increase offender hesitate to commit crimes at places covered by surveillance. Furthermore, CCTV has the potential to assist police after crimes are committed to identify offender[21] and to provide visual evidence for use in criminal investigations[22]. In addition, accused persons are more willing to plea guilty when there is visual evidence[23]. The CCTV also has potential to have impact on increase of reported crime, since CCTV can detect crimes that would have otherwise gone unreported[24].

Advancement of technology, both computer and medical have impact on the criminal justice system. Arguably the most important advance has been the DNA testing and their effect on legal outcomes by providing certainty about identity in a wat that has not been possible before. Cross-border crimes and establishment of

---

[18] McClendon, L., Meghanathan, N., (2015) Using Machine Learning Algorithms to Analyze Crime Data, *Machine Learning and Applications: An International Journal*, Vol. 2, No. 1, 1-12.

[19] Eck, J.E., Chainey, S., Cameron, J.G., Leitner, M., Wilson, R.E., (2005) Mapping Crime: Understanding Hot Spots, U.S. Department of Justice, Office of Justice Programs, National Institute of Justice. Available at: https://www.ncjrs.gov/pdffiles1/nij/209393.pdf 28.12.2020.

[20] Završnik, A., (2020) Criminal justice, artificial intelligence systems, and human rights, *ERA Forum* 20**,** Springer, 567-583.

[21] Ratcliffe, J., (2006) Video surveillance of public places, Problem-Oriented Guides for Police – Response Guide Series, Guide No. 4, U.S. Department of Justice Office of Community Oriented Policing Services, Center for Problem-Oriented Policing.

[22] Ashby, M. P. J., (2017) The value of CCTV surveillance cameras as an invstigative tool: An empirical analysis, *European Journal on Criminal Policy and Research,* Vol. 23, Issue 3, 441-459.

[23] Piza, E., Welsh, B., Farrington, D. and Thomas, A., 139.

[24] Winge, S., Knutsson, J., (2003) An evaluation of the CCTV scheme at Oslo central railway station. *Crime Prevention and Community Safety,* Vol. 5: 49- 59.

national DNA databases incentivize exchange of DNA profiles among countries, but also development of international database. At the international level Interpol established DNA Gateway database that provides member states with the opportunity to load DNA profiles and access to submitted profiles through 24/7 communication system[25]. While in the EU, article 4 of the Council Decision 2008/615/JHA allows direct access to other countries database to compare unidentified DNA profiles from one EU Member State with all DNA profiles from another national DNA database for the investigation of criminal offences.

Although technology is advancing the fingerprints identification continuous to form an integral part of the detection of a wide range of crime types, especially volume crime such car thefts and burglary[26]. Due to development of computer many law enforcement agencies have abandoned the practice of taking ink fingerprints of those arrested and have purchased technologies that instead allow them to take digital fingerprints, which can then be instantly transmitted to database to search for a match. Technology enables faster and more accurate searches. Automatic fingerprint matching can perform fingerprint comparison at the rate of tens of thousands of times each second, and the result can be sorted according to the degree of similarity and combined with any other criteria that may be available to further filter the candidates, all without human intervention[27].

Another technology assisting law enforcement as the effective means of criminal investigation is the Global Positioning System (GPS) tracking devices. Electronic tracing can be distinguished from electronic surveillance equipment in that the location of the subject is the primary goal of tracking. The GPS tracking devices are used in investigation of crimes, but also in enforcement of criminal sanctions. In USA GPS is used for enforcing more complicated supervision orders[28]. As an investigation tool, the GPS devices and technology got public interest with the Scott Peterson trial in 2004, when police attached GPS devices to a number of Peterson's vehicles to track his movement after disappearance of his wife[29]. The Peterson trial was the first case in USA when judge allowed the GPS evidence into trial.

III. Challenges for human rights

Although new technology contributes to the efficiency of the criminal justice system, there should be stressed that the same rights that people have offline must also be protected online[30]. The focus on the relationship between new technology and

[25] Matić Bošković, M., (2019) DNA profiles and database – relevance and ethical dilemmas in criminal justice, In: Stevanović, I., Vujičić, N. (ed.), *Kazneno pravo i medicina*, Institute for Criminological and Sociological Research, Belgrade, 337-351.

[26] Adderley R., Bond J. (2008) Police Forensic science performance indicators – a new approach to data validation. In: Ellis R., Allen T., Petridis M. (ed.) Applications and Innovations in Intelligent Systems XV, SGAI 2007, Springer, London, 163-174.

[27] Moses, K. R., (2011) Automated Fingerprint Identification System, In: Fingerprint Sourcebook, National Institute of Justice, Washington DC.

[28] Roman, J. K., Liberman, A. M., Taxy, Sm., Downey, P. M. (2012) The Costs and Benefits of Electronic Monitoring for Washington D.C, Urban Institute, Washington D.C.

[29] Elmes, G.A., Roedl, G., Conley, J., (2014) Forensic GIS: The Role of Geospatial Technologies for Investigating Crime and Providing Evidence, Springer.

[30] United Nations, Human Right Council, Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development, A/HRC/21/L.6 (21 September

human rights is relatively new. The debate on the issue was initiated in 1968, during the International Conference on Human Rights in Teheran, which resulted in adoption of Resolution 2450 (XXIII) which invited the Secretary General to begin a process of interdisciplinary studies to define appropriate standards of protection of human rights and fundamental freedoms against the potential impact of new technologies[31].

Use of the technology in the detection, investigation and prosecution of crime, as well as in the enforcement of criminal sanctions impose risks of infringement of human rights. Information technologies, for example, can lead to gross violation of individual privacy. The ability to monitor computer usage creates a number of potential human rights concerns including infringements of human freedom, freedom of thought and expression, and the right to privacy, but also right to fair trial and presumption of innocence.

To ensure human rights protection in investigation of cybercrime different international and regional instruments are adopted. The Council of Europe's Convention on Cyber crime (2001) incorporates various provisions designed to safeguard human rights norms and privileges in connection with cyber crime investigations, such as requirements for judicial or other independent supervision, proportionality, and respect for and consideration of the rights of third parties. Given the strength of the provisions allowing search, seizure and surveillance, however, these have been criticized by some privacy advocates as being inadequate.

The key instruments within the Council of Europe are the Ethical Charter on the use of artificial intelligence in judicial systems that the European Commission for the Efficiency of Justice (CEPEJ) has adopted and the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. The case-law of the European Court of Human Rights is also crucial when it comes to respecting private life, liberty, security and providing effective remedies to challenge intrusions into private life and to protect individuals from unlawful surveillance, including surveillance conducted through using of the new technology.

a. Discrimination

Inclusion of artificial intelligence to help police determine where the next crime spot might be or to determine the risk that a person awaiting criminal trial poses to society was followed by explanation that decisions are impartial, objective and based on facts[32]. However, the critics of the artificial intelligence and prediction models have demonstrated that these neutral systems replicate biases inherent in the data they are trained on or translate the particular ways of thinking into code[33]. If a system is fed with human biases, even unconscious, the result will inevitably be bias, thus reinforcing discrimination and prejudices.

2012), available at: http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session21/A.HRC.21.L.6_en.doc 25.12.2020.

[31] Coccoli, J., (2017) The Challenges of New Technologies in the Implementation of Human Rights: an Analysis of Some Critical Issues in the Digital Era, *Peace Human Rights Governance*, Vol. 1, Issue 2, 223-250.

[32] Miller, AP. (2018) Want less-biased decisions? Use algorithms. *Harvard Business Review*, July 26. https://hbr.org/2018/07/want-less-biased-decisions-use-algorithms 28.12.2020.

[33] O'Neil, C., (2016) Weapons of Math Destruction – How Big Data Increases Inequality and Threatens Democracy, New York, Crown Publishers.

Predictive policing has raised concern, since this became the predominant model of policing[34]. Country specific studies of predictive policing implemented in Germany[35], and UK[36] raised question of objectivity of the model, since inputs for automated calculation of future crime are given by police. As a consequence, a police choices, priorities and omissions become the inputs algorithms use[37].

In the USA tools for assessing criminality have been used in criminal justice for decades. However, the recent studies around bail, sentencing, policing and parole from criminal justice system demonstrated that racial and ethnic profiling leads to harsher criminal sentences for certain groups. Assessment of COMPAS, a predictive model of the risk of criminal recidivism, used until recently by various courts in the USA to support judges' decisions on release request, showed that model has strong racist bias. The model assigned a double risk to backs who will not actually commit a crime compare to whites in the same conditions[38]. The model, presumably inherited the bias present in the historical sentences and is affected by the fact that the American prisons population over-represents blacks.

Due to restricted budget resources and increase caseload, the European countries are also looking into predictive models as solution to improve efficiency of criminal justice systems. However, the policy makers in Europe are cautious and adopted several instruments to mitigate possible risks. The European Union Fundamental Right Agency warns that decision making based on predictive models and other related methods is relatively new and there is need to develop further safeguards in this area[39]. Also, European Parliament warned that maximum caution is required in order to prevent unlawful discrimination and the targeting of certain individuals or groups by reference of race, color, ethnic or social origin, or any other characteristic[40]. In addition, CEPEJ adopted in 2018 already mentioned Charter on the Use of Artificial Intelligence in Judicial Systems.

b. Right to privacy

Police investigative techniques exploiting new technologies ensures more efficiency in investigation and prosecuting crime, but their high degree of intrusiveness affects upon right to privacy. Some of new technologies, such as interception of communication, silent video surveillance of the home interior, enables policy to bypass physical barriers.

To respond appropriately to new types of offences related to technology use

---

[34] Wilson, D., (2018) Algorithmic patrol: The futures of predictive policing, In. Završnik, A., (ed.) Big Data, Crime and Social Control, London, Routledge, 108-127.

[35] Egbert, S., (2018) About discursive storylines and techno-fixes: The political framing of the implementation of predictive policing in Germany, *European Journal for Security Research*, Vol. 3, Issue 2, 95-114.

[36]Stainer, I., (2016) Enhancing Intelligence-Led Policing: Law Enforcement's Big Data Revolution, In. Bunnik, A., Cawley, A., Mulqueen, M., Zwitter, A., (ed.) Big Data Challenges: Society, Security, Innovation and Ethics, London, Palgrave, 97-113.

[37] Joh, E.E., (2017) Feeding the machine: Policing, crime data and algorithms, *William and Mary Bill of Rights Journal,* Vo. 26, Issue 2, 287-302.

[38] Pedreschi, D., Miliou I., (2020) Artificial Intelligence (AI): New developments and innovations applied to e-commerce, European Parliament, PE 648.791.

[39] European Union Agency for Fundamental Rights (2018) #Big Data: Discrimination in data-supported decision making, FRA Focus.

[40] European Parliament (2017), Fundamental rights implications of big data, P8_TAPROV (2017)0076.

authorities across the Europe introduced specific rules on use of undercover agents in online communication, interception of electronic communication, remote searches of computer system, preservation of stored computer data etc.[41]. Use of those specific rules should be in line with safeguards introduced for implementation of special investigation techniques and rules governing their gathering should be applied. European Court of Human Rights in several cases identified that implementation of special investigation techniques violates article 8, right to privacy, of the European Convention of Human Rights. In the case *Klass v Germany* the European Court of Human Rights stated that whatever system of surveillance is adopted, there should be adequate and effective guarantees against abuse[42]. The assessment has a relative character and depends on all the circumstances of the case, including nature, scope and duration of the possible measures, the grounds required for ordering such measures, the authorities competent to permit etc.[43].

Establishment of the national and supranational databases with DNA profiles, fingerprints and vehicle registration data raised question how to ensure proper balance between individual rights, including right to privacy and public safety[44]. DNA sample collection, retention, access and use of DNA samples are linked to fundamental rights. DNA data base contain DNA profile and collected DNA samples (cellular material). The issue of storage is usually under discussion and critics. Even the European Court of Human Rights stated in the case *S and Marper v United Kingdom*[45] that there had been a violation of article 8, right to respect for private life of the European Convention of Human Rights. The Court considered in particular that the use of modern scientific techniques in the criminal- justice system could not be allowed at any cost and without carefully balancing the potential benefits of the extensive use of such techniques against important private-life interests. Any State claiming a pioneer role in the development of new technologies bore special responsibility for "striking the right balance". The Court concluded that the blanket and indiscriminate nature of the powers of retention of the fingerprints, cellular samples and DNA profiles of persons suspected but not convicted of offences, as applied in this particular case, failed to strike a fair balance between the competing public and private interests[46].

Use of new technology for surveillance purposes may violate right to privacy. The European Court of Human Rights in the case *Shimovolos v Russia* held there had been violation of article 8 of the Convention in the case concerned the registration of a human rights activist in the surveillance database, which collected information on activist's movements[47]. The creation and maintenance of the database and the

---

[41] Ortiz-Pradillo, J.C., (2017) The new regulation of technology-related investigative measures in Spain, *ERA Forum*, Springer, 425-435.

[42] Case *Klass v Germany*, Application No. 5029/71. See: Deployment of special investigative means, Council of Europe, 2013, 14-43.

[43] Case *Malone v UK*, Application No. 8691/79; case *Leander v Switzerland*, Application No 9248/81; *Huvig v France*, Application No. 11105/84.

[44] Vervaele, J.A.E., (2008) *Information sharing between intelligence and law enforcement authorities in combating international terrorism*, In. Becker, S. Derenčinović, D., (ed.) *International Terrorism: the Future Unchained?,* Zagreb, 49-82

[45] Application No. 30562/04 and 30566/04 *S and Marper v United Kingdom*.

[46] Matić Bošković, M., (2019) DNA profiles and database – relevance and ethical dilemmas in criminal justice, 345.

[47] Case *Shimovolos v Russia*, Application No. 30194/09.

procedures for its operations were governed by a ministerial order which had never been published and there we no indication of the minimum safeguards against abuse of the database. Similar position on the secret surveillance for national security purposes the Court had in the case *Szabo and Vissy v Hungary*[48] due to lack of safeguards to avoid abuse.

IV. Conclusions

The new technologies are transforming every segment of the criminal justice system, from prevention to enforcement of criminal sanctions. It is inevitable that the criminal justice system follows trends to be in line with technology used by offenders, however rules for its use should be clear, transparent and in line with rule of law standards.

The presented analysis confirmed that application of new technology has as a result more efficient and more effective law enforcement agencies as well as investigation and prosecution. However, the criminal justice system must ensure balance between the protection of fundamental rights and efficient criminal justice. The jurisprudence of the European Court of Human Rights confirmed that same standards of human rights protection have to be followed when country introduce new technologies in the legislation and when law enforcement authorities apply new technologies.

Prior to introduction of the new technologies in the criminal justice system the policy makers in cooperation with researchers should conduct thorough assessment and analyze implications on human rights protection. Standards and principles for inclusion of the new technology should be set to guide its use, especially if there is discussion on introduction of predictive models and artificial intelligence.

Once when new technologies are introduced the comprehensive evaluation system should be established to monitor their potential for violation of human rights and to take necessary measures for improvement. The ex-post analysis of predictive model showed that algorithms incorporated all bias that exists and there is a need to introduce mechanism for prevention of such challenges.

References

1. Adderley R., Bond J. (2008) Police Forensic science performance indicators – a new approach to data validation. In: Ellis R., Allen T., Petridis M. (ed.) Applications and Innovations in Intelligent Systems XV, SGAI 2007, Springer, London, 163-174.

2. Ashby, M. P. J., (2017) The value of CCTV surveillance cameras as an invstigative tool: An empirical analysis, *European Journal on Criminal Policy and Research,* Vol. 23, Issue 3, 441-459.

3. Brennan, T., Dieterich, W., Ehret, B., (2009) Evaluating the predictive validity of the COMPAS Risk and Needs Assessment System, *Criminal Justice and Behavior,* Vol. 36, Issue 1, 21-40.

4. Clarke, R.V. (1995) Situation crime prevention, *Crime and Justice*, Vol. 19, 90-160.

[48] Case *Szabo and Vissy v Hungary,* Application No. 37138/14.

5. Coccoli, J., (2017) The Challenges of New Technologies in the Implementation of Human Rights: an Analysis of Some Critical Issues in the Digital Era, *Peace Human Rights Governance*, Vol. 1, Issue 2, 223-250.

6. Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime.

7. Council Decision 2008/616/JHA of 23 June 2008 on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime.

8. Eck, J.E., Chainey, S., Cameron, J.G., Leitner, M., Wilson, R.E., (2005) Mapping Crime: Understanding Hot Spots, U.S. Department of Justice, Office of Justice Programs, National Institute of Justice. Available at: https://www.ncjrs.gov/pdffiles1/nij/209393.pdf 28.12.2020.

9. Egbert, S., (2018) About discursive storylines and techno-fixes: The political framing of the implementation of predictive policing in Germany, *European Journal for Security Research*, Vol. 3, Issue 2, 95-114.

10. Elmes, G.A., Roedl, G., Conley, J., (2014) Forensic GIS: The Role of Geospatial Technologies for Investigating Crime and Providing Evidence, Springer.

11. European Commission Survey on Scams and Fraud Experienced by Consumers – Final Report, January 2020.

12. European Informatics Data Exchange Framework for Courts and Evidence – Overview of existing legal framework in the EU Member States, 2015, available at: http://s.evidenceproject.eu/p/e/v/evidence-ga-608185-d3-1-411.pdf 26.12.2020.

13. European Parliament (2017), Fundamental rights implications of big data, P8_TAPROV(2017)0076.

14. European Union Agency for Fundamental Rights (2018) #Big Data: Discrimination in data-supported decision making, FRA Focus.

15. Europol, Crime in the age of technology, (2017).

16. Eurostat, Digital economy and society statistics – households and individuals (2020), available at: https://ec.europa.eu/eurostat/statistics-explained/index.php/Digital_economy_and_society_statistics_-_households_and_individuals#Internet_accessed 25.12.2020.

17. Eurostat, Proportion of households having access to a personal computer 2014-2019 (2020), available at: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=File:Proportion_of_households_having_access_to_a_personal_computer,_2014_and_2019_(%25)_CPC20.png 25.12.2020.

18. Joh, E.E., (2017) Feeding the machine: Policing, crime data and algorithms, *William and Mary Bill of Rights Journal,* Vol. 26, Issue 2, 287-302.

19. Joint communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace [2013] JOIN(2013) 1 final, p. 2.

20. Kostic, J., Matic Boskovic, M., (2020) How COVID-19 Pandemic influences Rule of Law backsliding in Europe? In. M. Reljanović (ed.) Regional Law Review, Institute of Comparative Law, Belgrade, 77-91.

21. Matić Bošković, M., (2019) DNA profiles and database – relevance and ethical dilemmas in criminal justice, In: Stevanović, I., Vujičić, N. (ed.), *Kazneno pravo i medicina*, Institute for Criminological and Sociological Research, Belgrade, 337-351.

22. Matić Bošković, M., (2019) DNA profiles and database – relevance and ethical dilemmas in criminal justice.

23. McClendon, L., Meghanathan, N., (2015) Using Machine Learning Algorithms to Analyze Crime Data, *Machine Learning and Applications: An International Journal*, Vol. 2, No. 1, 1-12.

24. Miller, AP. (2018) Want less-biased decisions? Use algorithms. *Harvard Business Review*, July 26. https://hbr.org/2018/07/want-less-biased-decisions-use-algorithms 28.12.2020.

25. Moses, K. R., (2011) Automated Fingerprint Identification System, In: Fingerprint Sourcebook, National Institute of Justice, Washington DC.

26. Nellis, M., (2014) Understanding the electronic monitoring of offenders in Europe: expansion, regulation and prospects, *Crime, Law and Social Change*, Vol. 62, Issue 4, 489–510.

27. O'Neil, C., (2016) Weapons of Math Destruction – How Big Data Increases Inequality and Threatens Democracy, New York, Crown Publishers.

28. Ortiz-Pradillo, J.C., (2017) The new regulation of technology-related investigative measures in Spain, *ERA Forum*, Springer, 425-435.

29. Pedreschi, D., Miliou I., (2020) Artificial Intelligence (AI): New developments and innovations applied to e-commerce, European Parliament, PE 648.791.

30. Piza, E., Welsh, B., Farrington, D. and Thomas, A. (2019) CCTV Surveillance for Crime Prevention: A 40-Year Systematic Review with Meta-Analysis, *Criminology and Public Policy,* Vol 18, Issue 1, 135-159.

31. Piza, E., Welsh, B., Farrington, D. and Thomas, A., 139.

32. Ratcliffe, J., (2006) Video surveillance of public places, Problem-Oriented Guides for Police – Response Guide Series, Guide No. 4, U.S. Department of Justice Office of Community Oriented Policing Services, Center for Problem-Oriented Policing.

33. Roman, J. K., Liberman, A. M., Taxy, Sm., Downey, P. M. (2012) The Costs and Benefits of Electronic Monitoring for Washington D.C, Urban Institute, Washington D.C.

34. Smith, G. R, (2007) Crime Control in the Digital Age: An exploration of Human Rights Implications, *International Journal of Cyber Criminology*, Vol. 1, Issue 2, 167-179.

35. Stainer, I., (2016) Enhancing Intelligence-Led Policing: Law Enforcement's Big Data Revolution, In. Bunnik, A., Cawley, A., Mulqueen, M., Zwitter, A., (ed.) Big Data Challenges: Society, Security, Innovation and Ethics, London, Palgrave, 97-113.

36. United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime, draft February 2013.

37. United Nations, Human Right Council, Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development, A/HRC/21/L.6 (21 September 2012), available at: http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session21/A.HRC.21.L.6_en.doc 25.12.2020.

38. Vervaele, J.A.E., (2008) *Information sharing between intelligence and law enforcement authorities in combating international terrorism*, In. Becker, S. Derenčinović, D., (ed.) *International Terrorism: the Future Unchained?,* Zagreb, 49-82.

39. Wilson, D., (2018) Algorithmic patrol: The futures of predictive policing, In. Završnik, A., (ed.) Big Data, Crime and Social Control, London, Routledge, 108-127.

40. Winge, S., Knutsson, J., (2003) An evaluation of the CCTV scheme at Oslo central railway station. *Crime Prevention and Community Safety,* Vol. 5: 49- 59.

41. Završnik, A., (2020) Criminal justice, artificial intelligence systems, and human rights, *ERA Forum* 20, Springer, 567-583.