Institute of Comparative Law

ISSN 2812-698X

REGIONAL LAW REVIEW

2024

ISSN 2812-698X
ISSN (online) 2812-6998

REGIONAL LAW REVIEW

- ANNUAL EDITION -

BELGRADE, 2024

Održavanje konferencije „Regional Law Review“ i izdavanje ove publikacije podržalo je Ministarstvo nauke, tehnološkog razvoja i inovacija Republike Srbije.

International conference “Regional Law Review” and publishing of this collection of papers were supported by the Ministry of Science, Technological Development and Innovations of the Republic of Serbia.

COLLECTION REGIONAL LAW REVIEW

Publishers
Institute of Comparative Law, Belgrade, Serbia

In Cooperation with
Faculty of Law, University of Pécs, Hungary
Faculty of Law, University of Ljubljana, Slovenia
Faculty of Law, University of Latvia, Riga, Latvia

For the Publisher
Prof. Jelena Ćeranić Perišić, PhD

Editors
Jelena Kostić, PhD, Institute of Comparative Law, Belgrade, Serbia
Prof. Anita Rodina, PhD, Faculty of Law, University of Latvia, Riga, Latvia
Prof. Teresa Russo, PhD, Department of Legal Sciences, University of Salerno, Italy

Secretary
Bogdana Stjepanović, PhD, Institute of Comparative Law, Belgrade, Serbia

Technical editor
Ivana Radomirović, M.A., Institute of Comparative Law, Belgrade, Serbia

Reviewers

Prof. Saša Gajin, PhD, Union University in Belgrade, Serbia
Prof. Nevenko Vranješ, PhD, University of Banja Luka, Bosnia and Herzegovina
Prof. Lucia Mokra, PhD, Comenius University in Bratislava, Slovakia
Milica Matijević, PhD, Institute of Comparative Law, Belgrade, Serbia
Prof. Bojan Urdarević, PhD, University of Kragujevac, Serbia
Prof. Nataša Mrvić Petrović, PhD, Institute of Comparative Law, Belgrade, Serbia
Sanja Jelisavac Trošić, PhD, Institute of International Politics and Economics, Belgrade, Serbia
Prof. Marko Dimitrijević, PhD, University of Niš, Serbia
Ana Knežević Bojović, PhD, Institute of Comparative Law, Belgrade, Serbia
Prof. Ana Đanić Čeko, PhD, "Josip Juraj Strossmayer" University of Osijek, Croatia
Prof. Hana Kovačikova, PhD, Comenius University in Bratislava, Slovakia
Prof. Mina Zirojević, PhD, Institute of Comparative Law, Belgrade, Serbia
Prof. Jelena Ćeranić Perišić, PhD, Institute of Comparative Law, Belgrade, Serbia
Prof. Marko Božić, PhD, Union University in Belgrade, Serbia
Prof. Goran Obradović, PhD, University of Niš, Serbia
Prof. Bojan Spaić, PhD, University of Belgrade, Serbia
Prof. Gordana Gasmi, PhD, Institute of Comparative Law, Belgrade, Serbia
Prof. Jelena Vučković, PhD, University of Kragujevac, Serbia
Prof. Hristina Runcheva Tasev, PhD, Faculty of Law "Iustinianus Primus", North Macedonia
Prof. Miomira Kostić, PhD, University of Niš, Serbia
Prof. Darko Simović, PhD, University of Criminal Investigation and Police Studies in Belgrade, Serbia
Doc. Branka Babović Vuksanović, PhD, University of Belgrade, Serbia
Prof. Bojan Vlaški, PhD, University of Banja Luka, Bosnia and Herzegovina
Sanja Stojković Zlatanović, PhD, Institute of Social Sciences, Serbia
Prof. Ivana Bodrožić, PhD, University of Criminal Investigation and Police Studies in Belgrade, Serbia
Prof. Srđan Golubović, PhD, University of Niš, Serbia
Jelica Gordanić, PhD, Institute of International Politics and Economics, Belgrade, Serbia
Vanja Korać, PhD, Mathematical Institute of the Serbian Academy of Sciences and Arts, Belgrade, Serbia
Doc. Marija Dragićević, PhD, University of Niš, Serbia
Doc. Aleksandar Antić, PhD, University of Kragujevac, Serbia
Doc. Novak Vujičić, PhD, University of Belgrade, Serbia
Mihajlo Vučić, PhD, Institute of International Politics and Economics, Belgrade, Serbia
Marko Novaković, PhD, Institute of International Politics and Economics, Belgrade, Serbia
Dragan Prlja, PhD, Institute of Comparative Law, Belgrade, Serbia
Ranko Sovilj, PhD, Institute of Social Sciences, Belgrade, Serbia
Aleksandra Rabrenović, PhD, Institute of Comparative Law, Belgrade, Serbia

Proofreading
ABC prevodi d.o.o.

Prepress
Branimir Trošić

Print
Birograf Comp doo Beograd

Printed in 150 copies

ISBN 978-86-82582-25-0
ISSN 2812-698X
ISSN (online) 2812-6998
doi: 10.56461/iup_rlrc.2024.5

Indexed in HeinOnline Law Journal Library

Indexed in Directory of Open Access Journals

FOREWORD

In front of you is the fifth volume of RLR collection of papers. This is an attempt for legal science and practice to follow up on the technological innovations, whole new areas of law were created, as well as upgraded many fields of the classical law. Authors not only from the region, but also from other countries dealt with different topics related to technological innovations, both in private and public law. This is one more chance to read about legal topics from the region and beyond.

We aspired as in previous years, for our endeavour to be recognized as current, relevant and conductive for regional cooperation in the area of legal science and practice.

This year Institute of Comparative law have a new partner, the University of Latvia and the guest editors of the collection of papers are from Latvia, Italy and Serbia. As in the previous years, we tried to encompass most of neighbouring countries from the region, as well as from the other countries.

Regional Law Review collection of papers has been indexed in DOAJ, a widely recognized platform among scientific researchers in our region. Inclusion in DOAJ demonstrates our commitment to the best practices in open access publishing. In the coming years, we hope to include the collection of papers in several other research databases. For the third year, we are partnering with HeinOnline Law Jounral Library.

We would like to express our gratitude to the whole organizing crew for making yet another issue of the collection of papers possible, at the highest standards of editing and publishing. Besides the authors, our gratitude goes to our reviewers, all thirty-six of them, who did exceptional work during the summer months, which is always particularly challenging time of the year to perform tasks of this kind.

And the next year we will try to focus thematically on important topics in the current law and practice. We hope that you will remain loyal contributors and readers in the years to come and that we will continue to improve the quality and visibility of our work.

In Belgrade, October 2024

Dr. Jelena Kostić
Prof. Dr. Anita Rodina
Prof. Dr. Teresa Russo
RLR Editors

Contents

UDC: 004.8:341.231.14 DOI: 10.56461/iup_rlrc.2024.5.ch1

Hektor RUCI*
University of New York, Tirana, Albania

LETHAL AUTONOMOUS WEAPON SYSTEMS (LAWS) ENFORCEMENT OF HUMAN RIGHTS BY ALGORITHMS?

The aim of present article is to approach the relatively new field of lethal autonomous robots and weapon systems (LARs or LAWS) from the perspective of international law with a focus on human rights compliance. Initially, the topic became the subject of public awareness and discussions in 2009 and soon acquired both interest and criticism. The development of such weapon systems rises at the same time legal, moral, practical and ethical questions. In the absence of specific sui generis legal provisions regarding them, the article shall try to evaluate to what extent such concepts find legal and moral justification by the existing provisions of humanitarian law. In any case, as LAWS provide for important benefits, they should be considered under serious legal safeguard due to their impact on human rights, out-of-combat units and civilian population. All such benefits must be guided by ethical principles and legal provisions, either those already applied or new ones that would better fit this specific field.

Keywords: LAWS, UN, Geneva Convention, humanitarian law.

1. INTRODUCTION

The aim of the present article is to approach the relatively new field of lethal autonomous robots and weapon systems (LARs or LAWS) from the perspective of international law with a focus on human rights compliance.

Initially, the topic became the subject of public awareness and discussions in 2009. As one of the most important stakeholders in questions of humanitarian intervention it was via the Red Cross that the topic entered the domain of public discussion.

> "Given the rapid pace of development of military robotics and the pressing dangers that these pose to peace and international security and to civilians in war, we call upon the international community to urgently commence a discussion about an arms control regime to reduce the threat posed by these systems. We propose that this discussion should consider the following: The prohibition of the development,

* LLM, Lector, ORCID: 0009-0004-6363-6011, e-mail: *hruci@unyt.edu.al*

deployment and use of armed autonomous unmanned systems; machines should not be allowed to make the decision to kill people."[1]

The next level of such discussion was brought in by the UN through its independent human rights expert Heyns that urged a "pause in progress to 'a world where machines are given the power to kill humans' was" to elaborate "a global moratorium on the development and deployment of lethal autonomous robots" aiming at declaring and implementing "national moratoria on the production, assembly, transfer, acquisition, deployment and use of LARs, until a framework on the future of LARs has been established."[2]

2. PRESENT CHALLENGES

Once a public concern, several members of the UN have addressed the LAWS issue, by specifically considering them as an emerging threat to many established values of humanity. Nevertheless, since this is a relatively new domain at the present stage, it requires further discussion and thought as well as a need to de-lineate clearly what type of systems are included.[3]

The Canadian representative at the preparatory discussions on the Convention on Conventional Weapons as one of the most interested and initial investors on the issue specified: "We hope that a substantial report could be used as basis for further work (…) Canada supports the proposal to organize an informal meeting of experts to discuss emerging technologies in the field of lethal autonomous weapons systems. We have followed discussions closely and think it would be encouraging to look at issues pertaining to the development of these weapons. We're pleased to note that this view is shared by many states to the Convention on Conventional Weapons."[4]

On the other side, the UN Secretary-General "took note of 'killer robots' in his report on the Protection of Civilians in Armed Conflict issued in November 2013, saying important questions have been raised as to the ability of such systems to operate in accordance with international humanitarian and human rights law."[5]

The UN meeting of experts on LAWS took place under the auspices of the United Nations Office in Geneva where: "The Meeting decided to convene under the overall responsibility of the Chairperson an informal meeting of experts of up to five days during the week of 13 to 17 April 2015 to discuss the questions related to emerging

---

1 Asaro, P. 2012. On banning autonomous weapon systems: human rights, automation, and the dehumanization of lethal decision-making. *International Review of the Red Cross,* 94(886), pp. 687-709.

2 United Nations. 2013. UN human rights expert urges global pause in creation of robots with 'power to kill'. Available at: https://news.un.org/en/story/2013/05/440982 (10. 10. 2024).

3 United Nations. 2013.

4 Campaign to Stop Killer Robots. 2014. Country Statements on Killer Robots - Compilation by the Campaign to Stop Killer Robots. Available at: https://www.stopkillerrobots.org/wp-content/uploads/2013/03/KRC_CountryStatus_14Mar2014.pdf (10. 10. 2024).

5 United Nations. 2014. UN meeting targets 'killer robots'. Available at: https://news.un.org/en/story/2014/05/468302-un-meeting-targets-killer-robots (10. 10. 2024).

technologies in the area of lethal autonomous weapons systems, in the context of the objectives and purposes of the Convention."[6]

2.1. Initial Concerns and Human Rights

Among a broad variety of issues discussed during the aforementioned activities, most of them being very specific, human rights have been addressed rather general in point 7:

> "Overarching issues (a) Human rights and ethical issues (i) What would be the impact of the development and deployment of LAWS on human rights, in particular the right to life and the right to dignity?"[7]

In this context point 4 should be read in a more creative form as below: "(b) in what situations are distinctively human traits, such as fear, hate, sense of honour and dignity, compassion and love, desirable in combat? In what situations do machines that lack emotions offer distinct advantages over human combatants? (c) international humanitarian law indicates how a party to a conflict should behave in relation to people at its mercy, how would machines comprehend such situations?"

Summing up, one main question remains: How may an algorithm ensure compliance with human rights? This question entails the sub-question as to application of humanistic concepts in modern warfare.

Apparently, the impacts of human rights on LAWS (and vice versa) are not yet sufficiently analysed and requires a detailed approach. At the same time, it is highly unlikely that LAWS will be subject to a worldwide ban.[8]

However, a producer of intelligent weapon systems in Canada (Clearpath Robotics) stated: "Those who might see business opportunities in this technology to seek other ways to apply their skills and resources for the betterment of humankind (…) despite our continued involvement with Canadian and international military research and development, Clearpath Robotics believes that the development of killer robots is unwise, unethical, and should be banned on an international scale (…) would a robot have the morality, sense, or emotional understanding to intervene against orders that are wrong or inhumane? No. Would computers be able to make the kinds of subjective decisions required for checking the legitimacy of targets and ensuring the proportionate use of force in the foreseeable future? No. (…) In our eyes, no nation in the world is ready for killer robots—technologically, legally, or ethically."[9]

---

[6] United Nations. 2015. Convention on Certain Conventional Weapons – Informal Meeting of Experts. Available at: https://meetings.unoda.org/ccw-ime/convention-certain-conventional-weapons-informal-meeting-experts-2015 (10. 10. 2024).

[7] United Nations. 2015. Meeting of the High Contracting Parties to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects. Available at: https://digitallibrary.un.org/record/3856238/files/CCW_MSP_2015_9-EN.pdf (10. 10. 2024).

[8] Despite the fact that there are some rather political attempts to do so: ICRAC. 2015. Model United Nations urges Ban on Killer Robots. Available at: https://www.icrac.net/model-united-nations-urges-ban-on-killer-robots/ (10. 10. 2024).

[9] ICRAC. 2014. Canada's biggest robot company rejects 'killer robots'. Available at: http://icrac.net/2014/08/canadas-biggest-robot-company-rejects-killer-robots/ (10. 10. 2024).

It can be said with a certain degree of security as we shall try to show below that as far as there is demand there shall also exist supply, without forgetting that in the present discussion, the concept of technical capabilities, which not only exist, but expend every day, also needs to be added to the idea of demand.

As the vast majority of producers will take a different position, such statements cannot substitute the need to find a legal basis for the use of such systems in the future. According to Down: "…limits ensure there is always an element of human decision-making in carrying out lethal force. No matter how advanced the technology, there is always the potential for glitches and malfunctions with technology that could harm soldiers or civilians."[10]

At the same time, an "international coalition of human rights activists, academics and security experts called the Campaign to Stop Killer Robots says that because technology is advancing so rapidly, world leaders must adopt a treaty to ban the weapons. Alex Neve, Secretary General of Amnesty International Canada, said lethal weapons without human control — whether they're used for policing or military purposes — would violate international humanitarian law."[11]

The Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May be Deemed to be Excessively Injurious or to Have Indiscriminate Effects inclusive of its decision and Protocols (as last amended on 21 December 2001) has not yet been amended with regard to LAWS, but "taking a wait-and-see approach could lead to further investment by states in the development of these weapons systems and their rapid proliferation in a new arms race."[12]

However, to-date no comprehensive analysis of the threats and potential solutions to problems has been made publicly available. Therefore, the present article aims at pursuing a detailed investigation in the relevant issues and intends to achieve identification of the aspects justifiably raising concern. In so doing, necessary aspects for future amendments to the said Convention will be outlined. It will contribute to substantiated decision-making at domestic, community and international level. The article will try to give a modest contribution to substantiate the position on the IHL taking into consideration, *inter alia*, the new international situation during the ongoing war between Russia and Ukraine and possible escalations in both warfare tactics and human rights protection.

3. ADVANTAGES OF APPLYING LAWS

3.1. Technology

Technology is taking over more and more parts of our lives. Most of us today are incapable of remembering for example a certain phone number because we have it stored at our smart phone memory, therefore there is no need to use our own. Lethal Autonomous Weapon Systems does not have to be a priori excluded from such application.

[10] Harris, K. 2015. Killer robots pose risk and advantages for military use. CBC. Available at: http://www.cbc.ca/m/news/politics/killer-robots-pose-risks-and-advantages-for-military-use-1.3026963 (10. 10. 2024).

[11] Harris, K.

[12] Axworthy, L. & Walter, D. 2016. New Technology for peace and protection. Walterdorn. Available at: https://walterdorn.net/pub/236/ (10. 10. 2024).

In most of the cases, opinions included some provisions of humanitarian law to justify these weapons. Autonomous weapon systems are in some way a modern and very sophisticated weaponry as well as highly automated weapon systems that are created generally to set up in environments areas such as air, land or sea in which the risk for the civilians is very small.[13]

Moreover, those weapons are limited generally to use in defensive contexts against other machines. In that way, such systems can be considered even more reliable than a human military unit in the heat of battle always assuming that their ultimate control relies on a person or group of persons, highly trained, ethically and morally sound whom have either designed the algorithm or operate the device remotely.[14]

3.2. Accuracy

Therefore, autonomous weapon systems have the privileges to identify and collect targets more easily than a simple soldier, and in this way, it can provide more protection not only of its own personnel, but also of civilians, civilian property and other nonmilitary targets.

3.3. Decision-Making

Another point which needs to be considered as an advantage for the usage of LAWS is that the machines are much faster in decision-making then people. The specific automation in military systems of all kinds, can provide a quicker response than people who need to assess, calculate and respond. Also, they can sometimes be more precise and accurate in responding to a military threat.[15]

Moreover, the use of robots would decrease the level of casualties since no direct impact shall occur between the armed forces and the enemy, and military operation shall be carried out only using a remote operator.[16]

Therefore, the exact and right usage of these machines by well-trained personnel, in addition to the old and standard forms of warfare can provide a safer environment, despite the oxymoron concept of having both war and safety.

4. DISADVANTAGES

The highest risk of such weapon systems relies on the volatile concept of the respect of human rights in the field of battle and even beyond it. Humanitarian law per se, since the Antigone and Polynices, wants to take into account the direct applicability of the person with everything human nature has, such as feelings, compassion, dilemmas, love, hate, etc.

[13] Guizzo, E. 2016. Autonomous weapons 'could be developed for use within years', says arms-control croup. IEEE SPECTRUM. Available at: https://spectrum.ieee.org/autonomous-weapons-could-be-developed-for-use-within-years (10. 10. 2024).

[14] Guizzo, E.

[15] Van Den Boogaard, J. 2016. Proportionality and autonomous weapons systems. *Journal of International Humanitarian Legal Studies*, 6(2), pp. 247-283.

[16] Van Den Boogaard, J. 2016. Proportionality and autonomous weapons systems. *Journal of International Humanitarian Legal Studies*, 6(2), pp. 247-283.

4.1. The Geneva Convention of 1949

The Geneva Convention of 1949 on its article 22 explicitly mentions, *inter alia*, that:

> "...They shall be treated humanely and cared for by the Party to the conflict in whose power they may be, without any adverse distinction founded on sex, race, nationality, religion, political opinions, or any other similar criteria. Any attempts upon their lives, or violence to their persons, shall be strictly prohibited; in particular, they shall not be murdered or exterminated, subjected to torture or to biological experiments; they shall not wilfully be left without medical assistance and care, nor shall conditions exposing them to contagion or infection be created."[17]

In case we want to see and analyse this article in *stricto sensu,* there is a direct need of "human treatment," therefore comes the question: can a certain machine, despite of being remotely, if so, operated by humans, provide a human treatment? Is human treatment an exclusivity of humans only? At least this is what IHL has been providing us for centuries now, the importance and necessity of humans behind weapons.

4.2. Proportionality

A core element of humanitarian law especially when applied in the battlefield is proportionality, of actions, response and decision-making.[18] Such proportionality must therefore apply the concept of distinction, including civilians, wounded and other hors de combat personnel. Up to now there is no direct evidence that AI, can provide such a distinction.

4.3. Public Conscience

According to the aforementioned Geneva Convention, wherever codified legislation does not apply or has not been developed yet, then the general norms of humanity and the dictates of public conscience shall take their place in being therefore a direct application of the general principles of justice.[19] The development of technology can push humans far away from the battlefield and the application of conscience can become quite relative if applied at a different place and also at different times. The role of humans becomes therefore ethically questionable by transforming the operator from an actor into a spectator of warfare, comparable to a film lover who watches their favourite action movie in a cinema.

---

[17] Geneva Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field. Geneva, 12 August 1949. Available at: https://ihl-databases.icrc.org/en/ihl-treaties/gci-1949?activeTab=1949GCs-APs-and-commentaries (10. 10. 2024).

[18] International Committee of the Red Cross. 2016. Views of the ICRC on autonomous weapon systems - paper submitted to the Convention on Certain Conventional Weapons Meeting of Experts on Lethal Autonomous Weapons Systems (LAWS). Available at: https://www.icrc.org/en/document/views-icrc-autonomous-weapon-system (10. 10. 2024).

[19] International Committee of the Red Cross. The Geneva Conventions of 12 August 1949. Available at: https://www.icrc.org/sites/default/files/external/doc/en/assets/files/publications/icrc-002-0173.pdf (10. 10. 2024).

5. CONCLUSIONS

The use of LAWS on the battlefield is still a new concept in both warfare and its' legal regulatory acts. The core of the debate rests with the dilemma of saving lives on one side and abusing them on the other, if by abusing we would consider the lack of ethics, compassion and judgment which as per today remains an exclusivity of humanity.

In this article, we tried to evaluate and present the advantages and disadvantages of LAWS which concern both human life and dignity either from the attacker's or the defenders' side as such rights make no distinction regarding the side of the battlefield.

Nevertheless, despite the lack of legislation, customary law and practice, the most important element of legality is still there and is immutable: machines and AI are made by humans and humans shall comply with all standards of warfare and be considered responsible for it. It makes absolutely no difference if a soldier or his commander fires an arrow or a smart high-tech bomb, or even if that smart bomb fires itself based on a complicated algorithm. Even in that case the PERSON(S) responsible for that algorithm shall be liable before the humanitarian law and suffer the consequences of their actions.

LIST OF REFERENCES

Asaro, P. 2012. On banning autonomous weapon systems: human rights, automation, and the dehumanization of lethal decision-making. *International Review of the Red Cross*, 94(886), pp. 687-709. https://doi.org/10.1017/S1816383112000768

Axworthy, L. & Walter, D. 2016. New Technology for peace and protection. Walterdorn. Available at: https://walterdorn.net/pub/236/ (10. 10. 2024).

Campaign to Stop Killer Robots. 2014. Country Statements on Killer Robots - Compilation by the Campaign to Stop Killer Robots. Available at: https://www.stopkillerrobots.org/wp-content/uploads/2013/03/KRC_CountryStatus_14Mar2014.pdf (10. 10. 2024).

Geneva Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field. Geneva, 12 August 1949. Available at: https://ihl-databases.icrc.org/en/ihl-treaties/gci-1949?activeTab=1949GCs-APs-and-commentaries (10. 10. 2024).

Guizzo, E. 2016. Autonomous weapons 'could be developed for use within years', says arms-control croup. IEEE SPECTRUM. Available at: https://spectrum.ieee.org/autonomous-weapons-could-be-developed-for-use-within-years (10. 10. 2024).

Harris, K. 2015. Killer robots pose risk and advantages for military use. CBC. Available at: http://www.cbc.ca/m/news/politics/killer-robots-pose-risks-and-advantages-for-military-use-1.3026963 (10. 10. 2024).

ICRAC. 2014. Canada's biggest robot company rejects 'killer robots'. Available at: http://icrac.net/2014/08/canadas-biggest-robot-company-rejects-killer-robots/ (10. 10. 2024).

International Committee of the Red Cross. The Geneva Conventions of 12 August 1949. Available at: https://www.icrc.org/sites/default/files/external/doc/en/assets/files/publications/icrc-002-0173.pdf (10. 10. 2024).

ICRAC. 2015. Model United Nations urges Ban on Killer Robots. Available at: https://www.icrac.net/model-united-nations-urges-ban-on-killer-robots/ (10. 10. 2024).

International Committee of the Red Cross. 2016. Views of the ICRC on autonomous weapon systems - paper submitted to the Convention on Certain Conventional Weapons Meeting of Experts on Lethal Autonomous Weapons Systems (LAWS). Available at: https://www.icrc.org/en/document/views-icrc-autonomous-weapon-system (10. 10. 2024).

United Nations. 2015. Convention on Certain Conventional Weapons – Informal Meeting of Experts. Available at: https://meetings.unoda.org/ccw-ime/convention-certain-conventional-weapons-informal-meeting-experts-2015 (10. 10. 2024).

United Nations. 2015. Meeting of the High Contracting Parties to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects. Available at: https://digitallibrary.un.org/record/3856238/files/CCW_MSP_2015_9-EN.pdf (10. 10. 2024).

United Nations. 2014. UN meeting targets 'killer robots'. Available at: https://news.un.org/en/story/2014/05/468302-un-meeting-targets-killer-robots (10. 10. 2024).

United Nations. 2013. UN human rights expert urges global pause in creation of robots with 'power to kill'. Available at: https://news.un.org/en/story/2013/05/440982 (10. 10. 2024).

Van Den Boogaard, J. 2016. Proportionality and autonomous weapons systems. *Journal of International Humanitarian Legal Studies,* 6(2), pp. 247-283. https://doi.org/10.1163/18781527-00602007

UDC: 316.647.82:004.8:34(4-672EU) DOI: 10.56461/iup_rlrc.2024.5.ch2

Aleksandar MIHAJLOVIĆ*
Institute of Comparative Law, Belgrade, Serbia
Vesna ĆORIĆ**
Institute of Comparative Law, Belgrade, Serbia

ARTIFICIAL INTELLIGENCE AND DISCRIMINATION – STRENGTHS AND WEAKNESSES OF THE CURRENT EUROPEAN ANTI-DISCRIMINATION LEGAL FRAMEWORK***

We are witnessing an enormous development of artificial intelligence (AI) which boosts economic productivity, creates new job opportunities, and gives hope that human life will be more prosperous. On the other side, AI, as a new system, that is undiscovered and unpredictable, creates ethical and legal dilemmas and threats to human rights violations, in the context of the principle of equality, the rule of law, and democratic principles, if it is used in an inappropriate way. The subject of the paper is discrimination in the process of AI application in different fields of people's everyday lives. The aim of this investigation is to analyze provisions in the recently adopted European Union (EU) AI Act and the Council of Europe Framework Convention which are expected to prevent discriminatory treatment through an AI life cycle, and to give a bird-view of the selected cases of AI-related discrimination, as well as of the position of the Serbian national authorities in that regard. On that road, the authors will provide a critical and comparative analysis of these two instruments governing the AI application. Subsequent to that, the paper is focused on the position taken by the Serbian authorities in order to examine the level of its readiness to stay in line with the legal challenges the AI implementation brings, and illustrates a

* LLM, Research Assistant, ORCID: 0000-0001-8309-7896, e-mail: *a.mihajlovic@iup.rs*.

** PhD, Senior Research Associate, ORCID: 0000-0003-4240-7469, e-mail: *v.coric@iup.rs*.

Vesna Ćorić, PhD, was appointed as a mentor to Aleksandar Mihajlović, LLM, research assistant at the Institute of Comparative Law, by the Decision of the Scientific Council of the Institute of Comparative Law No. 771 of 05/10/2023. This paper is one of the results of the mentoring process with the mentee Aleksandar Mihajlović.

*** This paper is a result of the research conducted at the Institute of Comparative Law financed by the Ministry of Science, Technological Development and Innovation of the Republic of Serbia under the Contract on realization and financing of scientific research of SRO in 2024 registered under no. 451-03-66/2024-03/200049.

current example which is related to the implementation of the Social Card Law. The methodological framework includes doctrinal, comparative, and descriptive methods.

Keywords: artificial intelligence, anti-discrimination, European Union AI Act, Council of Europe Framework Convention, Serbia, Social Card Law.

1. INTRODUCTION

We are witnessing an enormous development of artificial intelligence (hereinafter: AI) which looks very promising and pleasurable, especially from an economic perspective, higher productivity, higher salaries and more free time. For instance, there is a prediction that AI could contribute to the global economy up to $15.7 trillion in 2030, where $6.6 trillion is likely to come from increased productivity and $9.1 trillion is likely to come from consumption-side effects (Rao & Verweij, 2017, p. 3). Besides these catchy numbers, AI is still an unknown and unpredictable area, and its implementation can provoke different legal challenges in exercising different rights, and especially in implementing the principles of equality and non-discrimination, as universal values of law.

Although the first impression regarding AI systems can be their objectivity in the decision-making process, different examples support the fact that AI is biased and can provoke discriminatory treatment toward different segments of people's lives. Another challenge is the unpredictability of AI effects throughout its lifecycle. At the moment, the initiative to regulate AI by legally binding instruments has come from the European Union (hereinafter: EU) and the Council of Europe (hereinafter: CoE), which adopted the EU Regulation on Artificial Intelligence[1] (hereinafter: EU AI Act) and the CoE Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law[2] (hereinafter: Framework Convention) in 2024.

The subject of the paper is discrimination in the process of AI application in different fields of people's everyday lives. The aim of this investigation is to analyze provisions in the recently adopted the EU AI Act and the Framework Convention which are expected to prevent discriminatory treatment through an AI life cycle, and to give a bird-view of the selected cases of AI-related discrimination, as well as of the position of the Serbian national authorities in that regard.

Firstly, the authors provide an analysis of definitions of AI and elements of an AI lifecycle. More specifically, the definitions introduced by the Organization for Economic Cooperation and Development (hereinafter: OECD), the CoE and the EU are to be examined. In

[1] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) Text with EEA relevance, OJ L, 2024/1689, 12.7.2024. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401689 (15. 7. 2024).

[2] Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, CM(2024)52-final, 17 May 2024. Available at: https://search.coe.int/cm#{%22CoEIdentifier%22: [%220900001680afb11f%22],%22sort%22:[%22CoEValidationDate%20Descending%22]} (7. 7. 2024).

the subsequent section, the authors will provide an overview of how AI programs are created and what risks are in the process of their implementation along with selected examples of how the AI application can provoke discriminatory treatment to concrete social groups. After that, the authors will have a look on the current anti-discrimination provisions in the EU AI Act and the Framework Convention. Within the last section, it will be shown where Serbia is at the moment regarding the AI development and what should be done to comply with the recently introduced the EU and the CoE framework. It is important to mention that Serbia was among the first countries in the world to adopt the Strategy of Development of Artificial Intelligence 2020-2025[3] (hereinafter: AI Strategy), as well as the Ethical Guidelines for the Development, Application and Usage of Reliable and Responsible Artificial Intelligence[4] (hereinafter: Ethical Guidelines). In this context, the authors will illustrate some current challenges which are related to the implementation of the Serbian Social Card Law[5] (hereinafter: SCL) which applies machine learning in the administrative procedure of exercising the right to social aid. This statute seems particularly important for risk assessment of its impact on indirect algorithmic discrimination before the Serbian national authorities given that the procedure for assessing its constitutionality was initiated before the Serbian Constitutional Court. The methodological framework includes doctrinal, comparative, and descriptive methods.

2. AI DEFINITION AND ELEMENTS OF AN AI LIFECYCLE

In the beginning of this part, the authors briefly elaborate on the definition of AI, starting from a universally accepted definition given by the OECD to the European definitions offered by the EU AI Act and the Framework Convention respectively. Concurrently, the elements of an AI lifecycle are described, aiming to illustrate its complexity. The explanation of an AI lifecycle is given as a theoretical overview which is common for every AI system.

2.1. AI Definition

In the modern world, it is very difficult to distinguish the digital revolution from AI which is becoming an inevitable part of every segment of human life (Miasato & Silva Reis, 2019, p. 193). When talking about AI, Surden (2019, p. 1308) was right when said that "[...], AI systems are not intelligent thinking machines, in any meaningful sense. Rather, [...], they are often able to produce useful, intelligent results without intelligence". In some circumstances related to handling cases in taxation, social insurance, transport tariffs etc, human intelligence can be redundant and not very productive because of the higher possibility of making risks related to manual decision-making, and the development of automation is more than desired in such cases (Sannerholm, 2021, p. 225).

[3] Strategy of Development of Artificial Intelligence in the Republic of Serbia for the period 2020-2025, *Official Gazette RS*, No. 96/2019.

[4] Ethical Guidelines for the Development, Application and Usage of Reliable and Responsible Artificial Intelligence, *Official Gazette RS*, No. 23/2023.

[5] Social Card Law, *Official Gazette RS*, No. 14/2021.

For lawyers, it is not an easy task to predict new technological innovations and their correlation with a legal system, while technological development and inventions will anticipate necessary legal changes very precisely, because the legal environment will be *conditio sine qua non* for their further development (success) or failure (Fornasier Oliveira, 2021, p. 354). Therefore, the urgent need had been identified to regulate the AI system and its elements, and lay down their key definitions on supranational and international levels. An inevitable progress of new technologies cannot be an excuse for violations of human rights, democratic values and the rule of law (Nemitz, 2021, p. 240).[6]

The OECD's revised definition states that "*An AI system is a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment.*" (Grobelnik, Perset & Russell, 2024). It means that AI is a machine system without human elements. It is fed by information, and it can produce different outputs. Although AI is a non-living system, it can affect both physical (living) and virtual environment. The last part of the definition underlines that AI systems have different capacities to produce inputs, which depend on their level of complexity. The same definition was adopted by the Framework Convention[7], and this approach illustrates its character of an international treaty, which tends to create a consensus of an internationally accepted AI definition. The EU AI Act accepted almost an identical definition[8] as the Framework Convention and the OECD, and this approach towards uniformity in defining an AI system is commendable and can be attributed to the fact that these two instruments were drafted at the same period of time.

2.2. Elements of an AI Lifecycle

The complexity of AI systems is attributable to the three types of machine learning where an AI system is applied in different formats. First, *supervised learning* is basic and is based on the dataset, and trained to discover a pattern in the limited framework of concrete data. For example, this is a way how detection of spam emails works. Second, *unsupervised learning* is more complex in comparison to the former, because the program learns how to find a pattern among data and produce a concrete result. For

[6] The development of AI can be seen as a chance for improving the state of fundamental rights, democracy and the rule of law in general, because AI will replace lawyers from doing repetitive jobs, and leave an opportunity to them to use this time to focus on important aspects of concrete areas (Kaur & Puri Gopal, 2021, p. 347).

[7] "For the purposes of this Convention, "artificial intelligence system" means a machine-based system that for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations or decisions that may influence physical or virtual environments. Different artificial intelligence systems vary in their levels of autonomy and adaptiveness after deployment." (Article 2, Framework Convention).

[8] "AI system means a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments." (Article 3 paragraph 1 point (1), EU AI Act).

instance, the program is trained to detect and classify fruits, vegetables and animals based on given criteria such as a colour. Third, *reinforcement learning* represents the most complex system, which uses dataset, interacts with a virtual or real environment, searches for an optimal way to complete a task while implementing steps which maximize a chance to complete the task successfully (Leslie *et al*., 2021, p. 9).[9]

The definition provided by the OECD, the EU and the CoE instruments shows that AI has its *lifecycle*, which amounts to a process of how it is developed and how it works in practice. In general, the literature recognizes 12 stages of an AI lifecycle, which are separated into three levels. The first level is called *design* and it includes the following four steps: 1. project planning when a project team decides if they will apply AI on a concrete task or not; 2. problem formulation which will be addressed by an AI model; 3. data extraction or procurement which should provide necessary data to train an AI model. Data can be extracted from surveys or similar methodologies, or procured which means to obtain existing datasets based on legal agreements; 4. data analysis which starts when all the necessary data is provided (Leslie *et al*., 2021, p. 10). The second level is called *development* and the following four steps are part of it: 1. preprocessing is implemented as a phase of feeding a model and includes among other tasks, data cleaning and data wrangling; 2. model selection and training which depends on a concrete task which should be done; 3. model testing and validation; 4. model reporting where experts can detect if an AI model should be modified based on detected obstacles (Leslie *et al*., 2021, p. 11). The third level is *the deployment of an AI model* which includes the following four steps: 1. model implementation in a real world; 2. user training for AI implementers; 3. monitoring of a model implementation; 4. updating or deprovisioning of an AI model based on results of monitoring and experiences from its implementation (Leslie *et al*., 2021, p. 12).

While the Framework Convention has covered on the surface only the activities related to the AI lifecycle that have the potential to interfere with human rights, democracy, and the rule of law, the EU AI Act has recognized concrete steps in detail which should be followed through the development of high-risk AI systems. The EU AI Act has introduced a *risk management system* that shall be established, implemented, documented and maintained in relation to the development of high-risk AI systems. The elements of this system are: the identification and analysis of the known and reasonably foreseeable risks; the estimation and evaluation of the risks that may emerge when the high-risk AI system is used in accordance with its intended purpose, and under conditions of reasonably foreseeable misuse; the evaluation of other risks possibly arising; and the adoption of appropriate and targeted risk management measures.[10] Concurrently, there are stipulated concrete rules regarding the data and data governance in a way that high-risk AI systems which make use of techniques involving the training of AI models with data shall be developed on the basis of training, validation, and testing data sets that meet the quality criteria referred to in paragraphs 2 to 5 of Article 10 whenever such

[9] In the literature, we can find a classification of the three waves of AI: first, "*handcraft knowledge*", as the most primitive category of AI; second, "*statistical learning*" also known as "*machine learning*"; third, "*deep learning*" as the most complex type of AI (see more at: Rejeski, Reynolds & Wright, 2018, pp. 6-7).

[10] Article 9, the EU AI Act.

data sets are used.[11] Special attention is placed to the detection of possible biases which can produce discriminatory treatment. The EU AI Act requires also that high-risk AI systems shall be designed and developed in such a way as to ensure that their operation is sufficiently transparent to enable deployers to interpret a system's output and use it appropriately.[12] High-risk AI systems during the process of their development shall be effectively overseen by natural persons during the period in which they are in use.[13] Prior to deploying a high-risk AI system, deployers shall perform an assessment of the impact on fundamental rights that the use of such system may produce.[14] The EU AI Act has also recognized the importance of monitoring the implementation of AI systems through the notifying authority, and each Member State shall designate or establish at least one notifying authority.[15] As a way to stimulate the AI development as well as to prevent possible negative effects through its development, the EU AI Act has introduced the AI regulatory sandbox.[16] Its aim is to provide conditions for an innovative AI system development, training, validation and testing, where appropriate in real-world conditions, for a limited time and under regulatory supervision.

3. DISCRIMINATION BASED ON AI APPLICATION – FROM UNKNOWN TO PREDICTABLE CONSEQUENCES OF AI

AI models apply different datasets which are used for their training and based on them they are ready to make content, predictions, recommendations and conclusions. This kind of data is called "*big data*" which are large in their complexity and interrelationships, and AI models discover previously unknown connections between data elements (Schmidt & Stephens, 2019, p. 134). The opposite is "*alternative data*" which are used for decision-making or model building, but they do not have *a historical background*[17] of their application

[11] Article 10, the EU AI Act. Prescribed practices in accordance with the paragraph 2 of the Article 10 from the EU AI Act include the following: the relevant design choices; data collection processes and the origin of data, and in the case of personal data, the original purpose of the data collection; relevant data-preparation processing operations, such as annotation, labelling, cleaning, updating, enrichment and aggregation; the formulation of assumptions, in particular with respect to the information that the data are supposed to measure and represent; an assessment of the availability, quantity and suitability of the data sets that are needed; examination in view of possible biases that are likely to affect the health and safety of persons, have a negative impact on fundamental rights or lead to discrimination prohibited under Union law, especially where data outputs influence inputs for future operations; appropriate measures to detect, prevent and mitigate possible biases; the identification of relevant data gaps or shortcomings that prevent compliance with this Regulation, and how those gaps and shortcomings can be addressed.

[12] Article 13, the EU AI Act.

[13] This is called human oversight and is regulated by Article 14, the EU AI Act.

[14] Fundamental Rights Impact Assessment for High-Risk AI Systems is regulated by the Article 27, the EU AI Act.

[15] Article 28, the EU AI Act.

[16] Article 57, the EU AI Act.

[17] This kind of data is called "*historical data*", because they are coming from some records, such as medical records, Internet search done by concrete population, criminal records etc (Huq, 2021, p. 3). This

in the decision-making process (Schmidt & Stephens, 2019, p. 134). An example can be a credit decision by a bank based on data such as the occupation of a client, rental payments, utility payments, and their educational background, where this data had not been used for a concrete credit decision or any other decision before (Schmidt & Stephens, 2019, p. 134).

AI models use machine learning algorithms which rely on different data, and based on the complexity of AI programs, it is not always possible to predict effects which AI can provoke. In the context of supervised and unsupervised machine learning it is easier to make accurate predictions, but, in case of reinforcement or so-called deep learning, it is very hard to predict all possible consequences. That is the reason why this kind of unpredictability creates AI as a "black box". In the literature, there are two types of AI "black boxes": strong and weak "black boxes". First, effects of strong "black boxes" can be very severe for humans, and there is no way to determine how the AI makes decisions or predictions, what kind of information influences an AI decision, and what is the rank of importance of variables processed by the AI. On the other hand, weak "black boxes" refer to AI where engineers can predict to some extent its accuracy effects although it can still be "opaque" to humans (Bathaee, 2018, p. 906). For this reason, the EU AI Act adopted the risk-based approach in the classification of AI systems (Korać, Prlja & Gasmi, 2021, p. 163) following the principle – the higher risk, the stricter rules will be applied to an AI model. It is noteworthy that the Framework Convention has not adopted the risk-based classification of AI systems, because it presumes that every AI system constitutes a risk for people and their environment.

A greater amount of data, which is used for training of an AI model, provides stronger processing power and advances a mathematical algorithm[18] which helps AI to operate autonomously (Greenstein, 2022, p. 299). Algorithms rely on statistical inferences which can discover discriminatory correlations (Xenidis, 2020, p. 745). Although we can perceive algorithms as objective, they are biased[19] because AI models are trained by humans who have a taste for discrimination and the dataset has "historical records" of discrimination. It is important to mention that not every bias is associated with protected characteristics such as sex, age, ethnicity, and religion. Instead, such a feature can be an algorithm which classifies people based on a fact if they have cats or not (European Union Agency for Fundamental Rights, 2022, p. 24). In another case, an algorithm can contain biases related to a protected characteristic, but the final result may not be discriminatory if it does not lead to a less favourable treatment (European Union Agency for Fundamental Rights, 2022, p. 24).

There are different examples of how AI models can discriminate, for instance, in the field of a labour market it is interesting to mention the case of *the Amazon Company* when

---

data has some historical background where it was used for making concrete decisions and deciding about someone's rights and/or obligations. That is the reason why this data is seen as biased.

[18] In the simplest way, an algorithm can be explained as a program which gives concrete instructions to a computer in which order and how concrete task should be done (Prlja, Gasmi & Korać, 2022, p. 84).

[19] There are different forms of biases: *historical bias*, *representation bias*, *measurement bias*, *aggregation bias*, *evaluation bias*, *deployment bias*, *automation and confirmation biases* etc. (see more in: Bartoletti & Xenidis, 2023, pp. 16-19).

the created automated hiring tool discriminated against women who applied for software engineering positions (Goodman, 2018; Dastin, 2018).[20] The program was trained by the data from CVs of male engineers who were dominant employees in these positions. The program scored female's resumes with lower points because it marked words such as "women's" or "women's rugby team" as less worthy. Concurrently, some colleges and schools were ranked with lower points as well, because the program recognized as more valuable concrete schools attended dominantly by male engineers, and which were used as data to feed the program. The Amazon Company has tried to fix this problem and modified the algorithm, but at the end it stopped using it in 2018. This example of algorithmic discrimination in the hiring process supports *the statistical discrimination theory* (Chen, 2023, pp. 2-3) which means that individual characteristics of an applicant are observed in the context of his/her membership of a concrete group of people. For instance, an employer may not have a taste for discrimination, but high economic costs of discovering the true potential of a candidate will lead him to put all female applicants in a group of less productive than male applicants because based on the statistical data female employees are often absent from job because of the pregnancy and child care obligations than males.

In Finland, the National Non-Discrimination and Equality Tribunal found that a company discriminated against a client when he applied for a credit loan (Bartoletti & Xenidis, 2023, p. 21; *Algorithms in credit scoring: Discrimination based on use of statistical data in Finland*, 2021). This example is related to the algorithm which was used to assess the credit capability of a client and took into account data related to age, gender, language and place of residence, but did not include the applicant's actual credit history. The person in this case was a Finnish male speaker and came from a rural area, and the statistical model assessed these characteristics as disadvantages. Cases of discrimination can occur also in the housing market when landlords use AI programs to assess applicants as potential tenants. Using addresses, names and ages of applicants can lead to discriminatory treatment toward people of colour, elderly people, or people who live in some areas which are associated with higher levels of committed crimes (*Housing Discrimination: Big Data, AI, and Algorithmic Models*, 2023). The last example includes the Dutch Government which faced a huge scandal when the Tax authorities used an algorithm that detected incorrect applications for child benefits and potential fraud, based on the data related to race and ethnicity of applicants (*Dutch childcare benefit scandal an urgent wake-up call to ban racist algorithms*, 2021). This program affected primarily disadvantaged families who did not have Dutch nationality and who received higher risk scores (*Dutch childcare benefit scandal an urgent wake-up call to ban racist algorithms*, 2021).

From concrete examples, we can conclude that in algorithmic discrimination, *indirect discrimination* often occurs, because *seemingly neutral datasets*, which are used to feed AI programs, contain hidden biases, which in the end have discriminatory effects (Korać, Prlja & Gasmi, 2022, p. 287). Discrimination can be based on one, two or several protected grounds, in other words, it can occur as multiple discrimination, depending on an AI program and variables which are used. There is a view that discrimination can be proved easily

[20] See more in: Weerts *et al*., 2023, pp. 809-811.

when an algorithm is involved and that anti-discrimination principle must be respected before, when an AI model is designed (Kleinberg *et al*., 2018, p. 114). Although this in fact sounds absolutely true and makes sense, the problem also occurs because AI companies lack transparency of how an algorithm is trained, which data is used, etc. (Heinrichs, 2022, pp. 143, 150-153). This problem of transparency will be presented in the part of the paper related to the implementation of the Serbian Social Card Law.

All the presented examples show that rooted discriminatory patterns are transported from humans to datasets which are used to train mathematical algorithms. The huge risk of applying AI is the violation of the principle of equality which leads to discriminatory treatment. In many cases, it is not predictable at all how an AI model will work in practice. Such a kind of unpredictability provokes a phenomenon which has been called a "black box". The selected cases further prove that the current European anti-discrimination legal framework is significantly challenged by the AI development. Such a challenge was recognized and addressed by the EU and the CoE. A part of their response to the spreading AI application to different areas of human life has led to the creation of specific legal instruments regulating AI along with focusing on human rights protection and anti-discrimination measures.

4. THE ANTI-DISCRIMINATION PROVISIONS WITHIN THE EU AI ACT AND THE FRAMEWORK CONVENTION

The EU AI Act and the Framework Convention represent a pioneering achievement of AI regulation. Although their legal natures as well as the institutional framework under which they have been developed differ among each other, their common aim is the regulation of AI in a way which prevents negative effects on people. Both acts contain anti-discriminatory norms which have strengthened the implementation of existing anti-discriminatory provisions and introduced new rules. First, it will be analysed the impact of these two acts on the national legislative frameworks of Member States, and, after that, anti-discriminatory rules from these acts will be compared.

4.1. A Different Approach of Implementing the EU AI Act and the Framework Convention and Their Impact on National Legislation

As a response to the growing development of AI and to different risks that it brings, the EU and the CoE recently adopted two legal documents, the EU AI Act and the Framework Convention. Both legal acts represent a revolutionary step to regulate the AI application on the regional and international level. They contain provisions governing the anti-discrimination matters in the AI context and are important for both the EU member states and its candidate countries.

The EU AI Act is a regulation, and, as a binding secondary law of the EU, it will be applied uniformly toward all EU member states. Since regulations are directly applicable, they are *legally binding without any action from an individual member state, and they* take effect as soon as they are published in the Official Journal of the EU. *Although EU*

regulations require no implementing legislation within individual member states, there has been a widespread practice among candidate countries to align their national regulatory frameworks with provisions of EU regulations to the highest possible extent in the accession process. Therefore, it is expected that aspiring candidate countries, such as Serbia, harmonize their legislation with the EU AI Act provisions in short run (Korać, Prlja & Gasmi, 2023, p. 213).

On the other side, the Framework Convention is an international treaty that will be opened for signatories on 5 September 2024 to all interested states, including Serbia, as well as to the EU as an entity, irrespectively of its member states. Every state party shall incorporate it as a part of its national law and it is important for both the EU Member States and candidate countries to interpret the provisions of the EU AI Act and the Framework Convention jointly, paying equal and close attention to both of them. However, it is noteworthy that the enforcement of the Framework Convention is "multifaceted" (Güçlütürk Gazi, 2024) and it goes beyond national implementation and includes the establishment of at least one effective oversight mechanism, regular consultations, and discussions among the State Parties and international cooperation (Articles 23 and 26, the Framework Convention).

4.2. The EU AI Act and the Framework Convention – A Comparison of Their Anti-Discriminatory Rules

While both legal instruments contain provisions governing anti-discrimination matters in the AI context, the Framework Convention is less detailed in comparison to the EU AI Act since it sets forth a set of general obligations and principles for its state parties, and leaves specific details to domestic legislation.[21] For that reason, the Framework Convention belongs to the category of so-called "framework agreements" (Lück-Matz, 2011).

As it appears from its title and the preamble, the Framework Convention's purpose is to ensure that all elements of an AI lifecycle are fully consistent with *human rights*, *democracy* and *the rule of law*. On the other hand, it seems that the EU AI Act focuses primarily on *the EU internal market* and AI's effects on it.[22] However, Article 1 along with improving the functioning of the internal market, also underlines the need to "promote the uptake of human-centric […] artificial intelligence" and to ensure *inter alia* a high level of fundamental rights (enshrined in the EU Charter of Fundamental Rights), including democracy and the rule of law. Therefore, the purposes of both legal instruments are compatible as the three European fundamental values are put at the forefront of protection, and are all inseparably treated as a "holy trinity".

Even though the EU and the CoE are not directly and organically linked since there are structural differences between them, those fundamental values have almost identical content within both organizations (Güçlütürk Gazi, 2024). On the road to developing

[21] The EU AI Act has 113 articles and XIII Annexes, while the Framework Convention has 36 articles. See also: Güçlütürk Gazi,2024.

[22] In that light, Lütz states that the purpose of the EU AI Act is not to ensure gender equality and non-discrimination as such. However, the author admits that "a flavour of gender equality" can be felt throughout its provisions (Lütz, 2024, p. 79).

a coherent system of human rights protection in Europe, relevant steps were taken. An illustration of such an approach may serve the provision introduced by the Lisbon Treaty stipulating that the EU shall access the European Convention for the Protection of Human Rights and Fundamental Freedoms (Ćorić & Knežević Bojović, 2020, p. 27).

Since both instruments follow the same values, they are not mutually contradictory, but rather complementing. They also underline the need to comply with provisions of other international human rights treaties. Most of those human rights instruments also contain relevant anti-discrimination norms. In that light, the Framework Convention refers *inter alia* to the necessity of application of the Universal Declaration of Human Rights, the European Convention for the Protection of Human Rights and Fundamental Freedoms, the International Covenant on Civil and Political Rights, the International Covenant on Economic, Social and Cultural Rights, and the European Social Charter. In a similar vein, the EU AI Act underlines the importance of the following human rights instruments: the United Nations (hereinafter: UN) Convention on the Rights of Persons with Disabilities, the UN Convention relating to the Status of Refugees, and the UN Convention on the Rights of the Child, as well the UNCRC General Comment No. 25 as regards the digital environment.

In addition to this body of the UN human rights instruments, the EU AI Act also gives due regard to the applicable EU regulatory framework and holds that provisions of the EU treaties, the Charter of Fundamental Rights of the EU (hereinafter: EU Charter of Fundamental Rights) and the EU secondary legislation shall be respected. When it comes to combating discrimination, the EU AI Act particularly stipulates that it does not affect the practices that are prohibited by the EU anti-discrimination law (Preamble, point 45, EU AI Act).

The approach of extensive referral to various international and supranational human rights instruments in the texts of the EU AI Act and the Framework Convention is not surprising. Namely, all the EU member states are state parties to the European Convention for the Protection of Human Rights and Fundamental Freedoms, as well as to the above UN human rights treaties. Therefore, the EU Member States are reminded through the texts of the EU AI Act and the Framework Convention of their obligation to interpret the EU AI Act in conjunction with the existing UN human rights framework, the Framework Convention, and the other relevant pieces of the European human rights' supranational framework (the EU and the CoE) in the process of development and implementation of AI lifecycles.

Considering that AI can provoke different risks, it is important that both instruments adopt *the risk-based approach* regarding the AI application. The difference is that the EU AI Act stipulates *categories of risk-systems*,[23] And the Framework Convention despite its reference to the risk-based approach, does not classify specific use of AI systems as prohibited or high-risk systems (Güçlütürk Gazi, 2024).

The EU AI Act clearly defines conditions which have to be fulfilled for one AI system to be considered a high-risk.[24] In addition, it contains a list of prohibited AI practices and

[23] Unacceptable, high, limited and minimal risk.

[24] See Article 6, EU AI Act.

a detailed classification of high-risk AI systems, which are listed in Annex III. It is argued that adequate protection against gender biases and discrimination can be only achieved in cases where AI systems are classified as a "high-risk" since the EU AI Act is of a horizontal nature and its priority is not the reduction of discrimination (Lütz, 2024, p. 81).[25] Therefore, an adequate identification of AI systems as high-risk systems is of key importance for ensuring fundamental rights protection in the non-discrimination realm.

Nevertheless, in the scholarly literature, it was rightly indicated that the EU AI Act does not provide sufficiently clear guidance on what falls under the scope of "high-risk" AI systems and that it is expected from the Court of Justice of the European Union to provide clarifications through its further interpretations in order to increase the legal security in the given field (Lütz, 2024, p. 82). As it was mentioned earlier, the classification of high-risk AI systems is based on Annex III's list of use cases which are determined in a rather clear manner. They *inter alia* include employment, workers management and access to self-employment, education and vocational training, as well as access to and the enjoyment of essential private services and essential public services and benefits. The above cases are selected as important considering that gender bias and discrimination frequently occur in one of those categories (Lütz, 2024, pp. 82-83).

However, the Annex III list is subject to two types of uncertainties. First refers to the derogations which are foreseen in Article 6 paragraph 3 for the use cases and which can be introduced if one of four specified criteria is fulfilled. If one of those criteria is fulfilled and the AI system referred to in Annex III does not pose a significant risk of harm to the fundamental rights of natural persons, it will not be considered as a high risk.[26] In the legal doctrine, it was rightly claimed that those four criteria are not clearly determined what may seriously undermine the envisaged system of protecting fundamental rights linked to the (high-risk) AI systems. The second point that can be brought up with regard to the flexibility of the scope of high-risk AI systems relates to the option envisaged by the EU AI Act according to which the Annex III list can be amended by delegated acts if some AI system, in particular, poses a risk or an adverse impact on fundamental rights.[27] The reference in Article 7(1) (b) shows the importance of negative impacts on fundamental rights including the right to non-discrimination, which enables the Commission to add new AI systems to Annex III, for instance when the principle of equality between women and men is adversely affected. This opportunity for the Commission to review Annex III by delegated act, as well as its general obligation to review the AI Act on a regular basis (after three years and thereafter every four years), leads to fluidity of the exact scope of application of the notion of high-risk AI system and

[25] See more in: Renard-Castets & Eynard, 2023, p. 613.

[26] These are: (a) the AI system is intended to perform a narrow procedural task; (b) the AI system is intended to improve the result of a previously completed human activity; (c) the AI system is intended to detect decision-making patterns or deviations from prior decision-making patterns and is not meant to replace or influence the previously completed human assessment, without proper human review; or (d) the AI system is intended to perform a preparatory task to an assessment relevant for the purpose of the use cases listed in Annex III.

[27] Beside this condition, it is also necessary that AI systems are intended to be used in any of the areas listed in Annex III (Article 7(1) (a).

as such may endanger achieved level of legal security within the EU regulatory framework. However, the benefits of such a flexible approach prevail over its limitations since this opportunity leaves room for further upgrades of the EU AI Act to reflect contemporary AI developments.

The Framework Convention does not contain any kind of classifications neither in the form of risk classes nor lists for high-risk AI systems. Instead, it presumes that every kind of AI can pose a potential risk to human rights, democracy, and the rule of law. It provides high-level obligations and offers a framework for the risk assessment and mitigation of its adverse impacts (Güçlütürk Gazi, 2024). In Article 10, the Framework Convention stipulates the importance of respecting *the principle of equality and non-discrimination*, including *gender equality*, as provided under applicable international and domestic law, within the lifecycle of AI systems. Concurrently, this instrument calls for the implementation of its provisions by the State Parties *without discrimination* on any ground, in accordance with their international human rights obligations (Article 17, Framework Convention).

The Framework Convention does not stipulate any kind of penalties or fines for individuals or firms in cases of not complying with the norms. It is up to every State Party to introduce a mechanism for monitoring the implementation and compliance with national legal frameworks. The EU AI Act provides concrete penalties in cases of breach of the rules, and every party can introduce concrete warnings and non-monetary measures. The difference in sanctioning approach can be explained by the fact that the Framework Convention belongs to the category of "framework agreements" which sets forth only broad commitments while leaving more detailed rules to national legislation. Moreover, considering the applicable anti-discriminatory framework which has been established through the European Convention for the Protection of Human Rights and Fundamental Freedoms and its Protocol No. 12 to this Convention, it can be expected that the European Court of Human Rights will develop in the near future relevant case-law on sanctioning violations of anti-discrimination provisions triggered by the AI system.

The European Commission established the AI Office.[28] Which will have a key role in the process of implementation of the EU AI Act, and every EU member state shall establish a public authority which will monitor the implementation of the EU AI Act. In Article 77 paragraph 1, the EU AI Act stipulates that "national public authorities or bodies which supervise or enforce the respect of obligations under the EU law protecting fundamental rights, including *the right to non-discrimination*, in relation to the use of high-risk AI systems referred to in Annex III shall have the power to request and access any documentation created or maintained under this EU AI Act in accessible language and format when access to that documentation is necessary for effectively fulfilling their mandates within the limits of their jurisdiction." The AI Office through its role is expected to further clarify and develop the provisions of the EU AI Act pertaining to anti-discrimination.

[28] Commission decision of establishing the European Artificial Intelligence Office, Brussels, 24. 01. 2024 C(2024) 390 final. Available at: https://digital-strategy.ec.europa.eu/en/library/commission-decision-establishing-european-ai-office (16. 7. 2024).

5. THE SERBIAN APPROACH TO AI REGULATION AND CURRENT CHALLENGES IN THE FIELD OF DISCRIMINATION

The Republic of Serbia was among the first countries in the world to adopt the AI Strategy for the period 2020-2025, which introduced aims and measures necessary for the development of AI. The Strategy recognized the importance of regulating the relationship between the individual and the society, and targeted challenges such as the representativeness of data used for machine learning, redefinition or elimination of the need for certain professions due to the introduction of AI, the need for additional qualification of the population for future jobs and issues concerning the responsibility for consequences of autonomous system decisions based on AI, etc.

As to overcome a possible problem which is experienced in practice, the AI Strategy has recognized the importance of prevention from *discrimination based on machine learning*. Besides the general objective of the AI Strategy which is to use AI in favour of economic growth, employment and improvement of the quality of life, there are five specific objectives. The fifth specific objective which is called the *Ethical and safe application of artificial intelligence* is dedicated to *discrimination based on AI*. The AI Strategy describes that algorithmic discrimination occurs based on data which are used for the training model, such as "historic" data, gender/sex unbalanced data, or lack of the inclusiveness of all relevant data sources necessary for the development of an AI lifecycle. It is recognized that individuals who are subject to decisions made by the AI model must have *the right to an explanation* and *the right to transparency* in connection with the algorithm. For this reason, it is necessary to enable the prevention of discrimination as well as early understanding and interpretation of the model and enable explanation of the decision.

The AI Strategy recognized the necessity of adopting the Ethical Guidelines. This document was introduced in 2023 and its aim is to enable necessary conditions for science, especially in the field of AI, to develop and progress, but not to allow people, as the central figures of all processes that affect them and of which they are indirect or direct agents, to be endangered and neglected. Concurrently, AI systems that are developed must be in line with the well-being of humans, animals and the environment.

The Ethical Guidelines have reflected to some extent the EU AI Act approach and recognized as a high-risk AI system a system that is part of the safety component of a product, or is a product in itself that has a function and behaves as a safety system and as such requires an assessment of compliance with legislative norms on putting AI systems into use, by a third party. Concurrently, the Ethical Guidelines have envisaged that a high-risk AI system is a system that is listed and marked as a high-risk system in the Ethical Guidelines. The high-risk AI systems are recognized in the numerous specified fields which are not exhaustively listed. Instead, this list is an open list which leaves room for more flexible interpretation and detection of new high-risk systems if a concrete AI system shows this kind of risk. The Ethical Guidelines do not apply to systems that are prohibited under the law governing AI systems.

The following *principles* are recognized as a starting point for the creation, application, and use of AI systems that will be worthy of human trust due to their reliability

and responsibility towards humans: explainability and verifiability; dignity; prohibition of damages; and, equity. The Ethical Guidelines introduce the following *conditions* of reliable and responsible AI which are based on the above-mentioned principles: action (mediation, control, and participation) and supervision; technical reliability and safety; privacy, personal data protection, and data management; transparency; *diversity*, *non-discrimination and equality*; social and environmental well-being; and responsibility.

For each of the conditions, there are AI System Assessment Questionnaires which help individuals and/or organizations to identify areas for improvement and encourage them to take action to overcome perceived challenges. By filling out the Questionnaires, one gets an insight into the established measures and identifies the measures that should still be implemented for the purpose of building a reliable AI. The Questionnaires do not exclude the application of other tools and methods for assessing the fulfilment of the AI system requirements in terms of the adopted Ethical Guidelines and/or laws. They are not a guide through the legal system of the Republic of Serbia and filling them out does not release responsible subjects from legal obligations and responsibilities. The conditions related to *diversity*, *non-discrimination and equality* are covered by a questionnaire regarding these three values and help to identify possible negative effects of an AI model on these fields. The principles and conditions specified by the examined Serbian documents (the Strategy and the Ethical Guidelines) reflect the spirit and the provisions of the recently introduced European supranational regulatory framework. However, they lack binding character and effective enforcement, because both documents, the strategy, as a policy document, and the Ethical Guidelines constitute "soft law" instruments.

The current case of alleged algorithmic discrimination in Serbia is related to the implementation of the Social Card Law (hereinafter: SCL) which was introduced in 2021 and whose main objective is to create a more effective realization of social protection rights and services, fairer distribution of social assistance, improvement of the efficient and proactive work of authorities in the field of social protection, provision of support in defining and shaping social policy and monitoring the overall effects of social protection measures, as well as provision of up-to-date data on beneficiaries in the event of emergencies.

Based on the SCL, the social card is a unique register that contains data on the individual and related persons on social and economic status, data on the type of rights and services from social protection that a person uses or has used, as well as data on the officials who led, that is, decided on individual rights. There are around 135 personal processed data of every social aid user or applicant, and the Centre for Social Work uses the data from the system to make a decision if a person has or does not have a right to receive social aid. The Initiative for Economic and Social Rights (hereinafter: Initiative A11), as a Serbian NGO, notified complaints from people who lost the right to social aid because the centres for social work use primarily the algorithm which processes their personal data and data of related persons to make a final decision about a concrete applicant. Initiative A11 asked the responsible Ministry of Labor, Employment, Veterans and Social Affairs to publish the structure of the algorithm and the lifecycle of the program, but

this request was refused. At the moment, there is a case before the Constitutional Court of the Republic of Serbia because Initiative A11 has initiated the procedure for assessing the constitutionality of the SCL. This is the first case of possible indirect algorithmic discrimination before a Serbian authority and it remains to be seen in the following period how the Constitutional Court will adjudicate and to which extent it will take into account the recently adopted EU and the CoE framework governing the operation of AI systems.[29]

In general, the existing Law on the Prohibition of Discrimination can be applied, as an umbrella anti-discrimination act, to cases including algorithmic discrimination, because Article 4 Paragraph 2 stipulates that "*everyone*[30] *shall be obligated to respect the principle of equality, that is to say, the prohibition of discrimination*". It is also important to underline that, although the current AI Strategy has recognized discrimination which can occur in the process of AI implementation, it does not mention anywhere in the text the Law on the Prohibition of Discrimination in the context of the existing legal framework in Serbia (for instance, it mentions the Law on Personal Data Protection). We expect that this approach will be changed in a new strategy and that the Law on the Prohibition of Discrimination will be placed as a starting point in the part related to the recognition of preventing algorithmic discrimination.

As an EU candidate country, Serbia should follow the future development of the EU AI Act and improve its legal framework on AI (Prlja, Gasmi & Korać, 2021, p. 126), which includes also the update of the Ethical Guidelines in accordance with the further development and implementation of the analyzed the EU and the CoE legal instruments. In the case of ratification of the Framework Convention, the Serbian authorities will be obliged to further improve the current legislation. At the moment, the AI Strategy and the Ethical Guidelines as soft law instruments provide only a vision and a framework for safe AI development without having any legally binding force.

6. CONCLUSION

AI systems have a lifecycle in which effects on people and the environment are not predictable at all. That is the reason why AI can provoke risk for violations of human rights, democracy and the rule of law. The level of the risk depends on the complexity of an AI system. The accelerating development of AI initiated the adoption of two legal instruments, the EU AI Act and the Framework Convention, under the auspice of the EU and the CoE. Although there are some differences between these two acts, they share the common aim of regulating the AI application in a safe manner and limiting its negative effects to the minimum possible extent.

Although the regulatory approach of these two instruments seems to look different, their shared value is the protection of fundamental human rights, the rule of law

[29] See more about this case on: (Anti) Social Card. Available at: https://antisocijalnekarte.org/en (17. 7. 2024).

[30] Based on the Law on the Prohibition of Discrimination, everyone means also any legal entity registered or operating on the territory of the Republic of Serbia.

and democracy, and they both call on the substantive application of international and domestic human rights norms. While the EU AI Act will be implemented directly by the EU member states, the Framework Convention creates a foundation for how State Parties to this international treaty should adapt their national legislative frameworks. Furthermore, these two instruments supplement each other and support the overall idea of creating a safe environment for the AI application. At this stage, because the EU AI Act has just entered into force and the Framework Convention was recently adopted and will be opened for signature in Vilnius (Lithuania) on 5 September 2024 on the occasion of a conference of Ministers of Justice, we cannot predict at all possible challenges which will occur during its application, but it is absolutely clear that the anticipated interpretation of the EU AI Act by the Court of Justice of the European Union through its case-law will additionally show the relevance, efficiency and effectiveness of this instrument. Although supranational courts already dealt with issues deriving from the use of AI, it seems that throughout the implementation of the recently adopted legal instruments, both courts will clarify and strengthen the given protection, particularly in the field of combating discrimination. Among others, it is expected that the Court of Justice of the European Union will bring needed clarification when it comes to the interpretation of when an AI system should be classified as a high-risk system.

Discrimination based on AI applications, the so-called algorithmic discrimination, can occur in different spheres of everyday life, and this usually happens in an indirect form. This is because algorithms seem to be neutral and bias-free, but in reality, they reflect the biases which exist around us and which are just incorporated by humans into the AI lifecycle. Current international and European supranational human rights instruments, together with the EU AI Act and the Framework Convention, create a strong and secure base for protection from discrimination in the context of AI applications.

The Republic of Serbia was among the first countries in the world to adopt the AI Strategy and the Ethical Guidelines. By doing so, it has recognized the importance and necessity of regulating safe AI development and application. Although these two national instruments are not legally binding, they provide a solid base for the self-assessment of safe AI development and its application. Serbia, as an EU candidate country, should start the harmonization of domestic law with the EU AI Act. At least, it is expected that a new strategy and the Ethical Guidelines are to be carefully reviewed in order to determine to which extent they have to be amended to comply with both instruments, the EU AI Act and the Framework Convention. If Serbia ratifies the Framework Convention, this will introduce a concrete obligation to adapt the domestic law in accordance with the Framework Convention's provisions. At this moment, it is important to underline, that the AI Strategy has not mentioned anywhere in the text the Law on the Prohibition of Discrimination, as the main anti-discrimination legal act, although it has recognized a problem of algorithmic discrimination. The authors are looking forward to the new strategy and the revised Ethical Guidelines which will place in the centre the proper application of the Law on the Prohibition of Discrimination and will hopefully reflect the spirit and wording of two recently adopted European legal instruments.

LIST OF REFERENCES

Monographs

Bartoletti, I. & Xenidis, R. 2023. *Study on the impact of artificial intelligence systems, their potential for promoting equality, including gender equality, and the risks they may cause in relation to non-discrimination*. Strasbourg: The Council of Europe. Available at: https://rm.coe.int/study-on-the-impact-of-artificial-intelligence-systems-their-potential/1680ac99e3 (10. 7. 2024).

European Union Agency for Fundamental Rights. 2022. *Bias in Algorithms – Artificial Intelligence and Discrimination – Report*. Luxembourg: Publications Office of the European Union. Available at: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2022-bias-in-algorithms_en.pdf (10. 7. 2024).

Leslie, D. *et. al*. 2021. *Artificial intelligence, human rights, democracy, and the rule of law: a primer.* The Council of Europe. Available at: https://rm.coe.int/primer-en-new-cover-pages-coe-english-compressed-2754-7186-0228-v-1/1680a2fd4a (7. 7. 2024). https://doi.org/10.2139/ssrn.3817999

Prlja, D. Gasmi, G. & Korać, V. 2021. *Veštačka inteligencija u pravnom sistemu EU*. Beograd: Institut za uporedno pravo. Available at: https://iup.rs/wp-content/uploads/2021/05/2021-Ve%C5%A1ta%C4%8Dka-inteligencija-u-pravnom-sistemu.pdf (22. 9. 2024).

Prlja, D. Gasmi, G. & Korać, V. 2022. *Ljudska prava i veštačka inteligencija*. Beograd: Institut za uporedno pravo. Available at: https://iup.rs/wp-content/uploads/2022/09/Ljudska-prava-i-ve%C5%A1ta%C4%8Dka-inteligencija-Prlja-Gasmi-Korac.pdf (10. 7. 2024).

Rao, S. A. & Verweij, G. 2017. *Sizing the prize – PwC's Global Artificial Intelligence Study: Exploiting the AI Revolution – What's the real value of AI for your business and how can you capitalize?* PwC. Available at: https://www.pwc.com/gx/en/issues/analytics/assets/pwc-ai-analysis-sizing-the-prize-report.pdf (7. 7. 2024).

Rejeski, D., Reynolds, L. & Wright, S. 2018. *When Software Rules: Rule of Law in the Age of Artificial Intelligence*. Washington, D. C: Environmental Law Institute. Available at: https://www.eli.org/sites/default/files/eli-pubs/when-software-rules-web.pdf (8. 7. 2024).

Renard-Castets, C. & Eynard, J. 2023. *Un Droit de L'intelligence Artificielle: Entre Règles Sectorielles et Régime Général: Perspectives Comparées*. Belgium: Bruylant.

Sannerholm, R. 2021. Responsibility and Accountability: AI, Governance, and the Rule of Law. In: Collona, L. & Greenstein, S. (eds.), *Law in the Era of Artificial Intelligence*. Stockholm: Stiftelsen Juridisk Fakultetslitteratur (SJF) and The Swedish Law and Informatics Research Institute (IRI)and Law Faculty, Stockholm University, pp. 223-246. Available at: https://irilaw.org/2022/02/16/new-publication-nordic-yearbook-of-law-and-informatics-2020-2021/ (8. 7. 2024). https://doi.org/10.53292/208f5901.40d940a1

Weerts, H. *et al*. 2023. Algorithmic Unfairness through the Lens of EU Non-Discrimination Law: Or Why the Law is not a Decision Tree. In: *2023 ACM Conference on Fairness, Accountability, and Transparency (FAccT'23)*, June 12–15, 2023, Chicago, IL, USA. New York : ACM, pp. 805-816. https://doi.org/10.1145/3593013.3594044

Scholarly Articles

Bathaee, Y. 2018. The Artificial Intelligence Black Box and the Failure of Intent and Causation. *Harvard Journal of Law & Technology*, 31(2), pp. 889-938. Available at: https://jolt.law.harvard.edu/assets/articlePDFs/v31/The-Artificial-Intelligence-Black-Box-and-the-Failure-of-Intent-and-Causation-Yavar-Bathaee.pdf (8. 7. 2024).

Chen, Z. 2023. Ethics and discrimination in artificial intelligence-enabled recruitment practices. *Humanities and Social Sciences Communications*, 10(567), pp. 1-12. Available at: https://www.nature.com/articles/s41599-023-02079-x (10. 7. 2024). https://doi.org/10.1057/s41599-023-02079-x

Fornasier Oliveira de, M. 2021. Artificial Intelligence and Democratic Rule of Law. *Revista de Estudos Constitucionais*, *Hermenêutica e Teoria do Direito (RECHTD)*, 13(3), pp. 351-369. https://doi.org/10.4013/rechtd.2021.133.06

Ćorić, V. & Knežević Bojović, A. 2020. Autonomous Concepts and Status Quo Method: Quest for Coherent Protection of Human Rights before European Supranational Courts. *Strani pravni život*, 64(4), pp. 27-40. https://doi.org/10.5937/spz64-30165

Greenstein, S. 2022. Preserving the rule of law in the era of artificial intelligence (AI). *Artificial Intelligence and Law*, 30, pp. 291-323. https://doi.org/10.1007/s10506-021-09294-4

Heinrichs, B. 2022. Discrimination in the age of artificial intelligence. *AI & Society*, 37(1), pp. 143-154. https://doi.org/10.1007/s00146-021-01192-2

Huq, Z. A. 2021. Artificial Intelligence and the Rule of Law. *Public Law and Legal Theory Working Paper Series*, No. 764, pp. 1-14. Available at: https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=2194&context=public_law_and_legal_theory (8. 7. 2024).

Kaur, I. & Puri Gopal, C. 2021. Impact of Artificial Intelligence on Legal Industry. *International Journal of Law Management & Humanities*, 4(2), pp. 346-354.

Kleinberg, J. *et al*. 2018. Discrimination in the Age of Algorithms. *Journal of Legal Analysis*, 10, pp. 113-174. https://doi.org/10.1093/jla/laz001

Korać, V., Prlja, D. & Gasmi, G. 2021. Challenges brought on by Artificial Intelligence. *Archaeology and Science*, 17, pp. 159-165. https://doi.org/10.18485/arhe_apn.2021.17.10

Korać, V., Prlja, D. & Gasmi, G. 2022. Influence of Artificial Intelligence on Human Rights. *Archaeology and Science*, 18, pp. 279-292. https://doi.org/10.18485/arhe_apn.2022.18.19

Korać, V., Prlja, D. & Gasmi, G. 2023. European Approach to Artificial Intelligence. *Archaeology and Science*, 19, pp. 209-216. https://doi.org/10.18485/arhe_apn.2023.19.14

Lütz, F. 2024. The AI Act, gender equality and non-discrimination: what role for the AI office? *ERA Forum*, 25, pp. 79-95. https://doi.org/10.1007/s12027-024-00785-w

Miasato, A. & Silva Reis, F. 2019. Artificial Intelligence as an Instrument of Discrimination in Workforce Recruitment. *Acta Universitatis Sapientiae*, *Legal Studies*, 8(2), pp. 191-212. https://doi.org/10.47745/AUSLEG.2019.8.2.04

Nemitz, P. 2021. Democracy through law The Transatlantic Reflection Group and its manifesto in defence of democracy and the rule of law in the age of "artificial intelligence". *European Law Journal*, 29(1-2), pp. 237-248. https://doi.org/10.1111/eulj.12407

Schmidt, N. & Stephens, B. 2019. An Introduction to Artificial Intelligence and Solutions to the Problem of Algorithmic Discrimination. *Conference on Consumer Finance Law (CCFL) Quarterly Report*, 73(2), pp. 130-144.

Surden, H. 2019. Artificial Intelligence and Law: An Overview. *Georgia State University Law Review*, 35(4), pp. 1305-1337.

Xenidis, R. 2020. Tuning EU equality law to algorithmic discrimination: Three pathways to resilience. *Maastricht Journal of European and Comparative Law*, 27(6), pp. 736–758. https://doi.org/10.1177/1023263X20982173

Legal Sources

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)Text with EEA relevance, *OJ* L, 2024/1689, 12.7.2024 Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401689 (15. 7. 2024).

Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, CM(2024)52-final, 17 May 2024. Available at: https://search.coe.int/cm#{%22CoEIdentifier%22:[%220900001680afb11f%22],%22sort%22:[%22CoEValidationDate%20Descending%22]} (7. 7. 2024).

Strategy of Development of Artificial Intelligence in the Republic of Serbia for the period 2020-2025, *Official Gazette RS*, No. 96/2019.

Ethical Guidelines for the Development, Application and Usage of Reliable and Responsible Artificial Intelligence, *Official Gazette RS*, No. 23/2023.

Social Card Law, *Official Gazette RS*, No. 14/2021.

Law on the Prohibition of Discrimination, *Official Gazette RS*, No. 22/2009 and 52/2021.

Commission decision of establishing the European Artificial Intelligence Office, Brussels, 24. 01. 2024 C(2024) 390 final. Available at: https://digital-strategy.ec.europa.eu/en/library/commission-decision-establishing-european-ai-office (16. 7. 2024).

Online Sources

Algorithms in credit scoring: Discrimination based on use of statistical data in Finland. Equinet. 8 July 2021. Available at: https://ai.equineteurope.org/library/algorithms-credit-scoring-discrimination-based-use-statistical-data-finland (10. 7. 2024).

(Anti) Social Card. Available at: https://antisocijalnekarte.org/en (17. 7. 2024).

Dasti, J. *Insight* – Amazon scraps secret AI recruiting tool that showed bias against women. 11 October 2018. Available at: https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G/ (10. 7. 2024).

Dutch childcare benefit scandal an urgent wake-up call to ban racist algorithms. Amnesty International. 25 October 2021. Available at: https://www.amnesty.org/

en/latest/news/2021/10/xenophobic-machines-dutch-child-benefit-scandal/ (10. 7. 2024).

Goodman, R. *Why Amazon's Automated Hiring Tool Discriminated Against Women*. 12 October 2018. Available at: https://www.aclu.org/news/womens-rights/why-amazons-automated-hiring-tool-discriminated-against (10. 7. 2024).

Grobelnik, M., Perset, K. & Russell S. 2024. *What is AI? Can you make a clear distinction between AI and non-AI systems?* 6 March 2024. Available at: https://oecd.ai/en/wonk/definition (7. 7. 2024).

Güçlütürk Gazi, O. *Understanding Council of Europe's Draft Framework Convention on AI, Human Rights, Democracy, and Rule of Law*. 17 January 2024. Available at: https://www.holisticai.com/blog/europe-committee-artificial-intelligence-draft-framework-convention (25. 7. 2024).

Lück-Matz, N. 2011. *Framework Agreements*. In: Oxford Public International Law. Available at: https://opil.ouplaw.com/display/10.1093/law:epil/9780199231690/law-9780199231690-e703#:~:text=A%20framework%20agreement%20can%20be,agreements%20between%20the%20parties%2C%20usually (16. 8. 2024).

Smith NMTC Associates. Housing Discrimination: Big Data, AI, and Algorithmic Models. SMITH NMTC ASSOCIATES, LLC. 10 October 2023. Available at: https://smithnmtc.com/housing-discrimination-big-data-ai-and-algorithmic-models/ (10. 7. 2024).

UDC: 004.9:35 DOI: 10.56461/iup_rlrc.2024.5.ch3

Plarent RUKA*
Faculty of Law and Social Science, University of New York, Tirana, Albania

THE LEGAL CHALLENGES RELATED TO THE DIGITALIZATION OF PUBLIC SERVICES: A PRINCIPLES PERSPECTIVE

The digitalization of public services has revolutionized the way governments interact with their citizens, offering efficiency, accessibility, and convenience. The legal principles of the administrative procedures endorsing active administrative support to public entities provide opportunity to such entities to promote the use of digital means for ensuring access to public services. In light of this, public entities have gone even further by digitizing the majority of governmental services. Certainly, there are numerous benefits, such as the improvement of efficiency in delivering public services with limited resources. This is certainly a plausible transformation of traditional governance into e-government. This could serve as a premise for further application of innovative solutions provided by artificial intelligence modules, that could "substitute" instead of "merely supporting" the human capital in public administration.

However, this transformation also brings forth a myriad of legal challenges that need to be addressed to ensure the effective and equitable delivery of services. This paper explores the key legal challenges faced in the digitalization of public services, including but not limited to data privacy and security concerns, digital inclusion and accessibility issues, regulatory compliance, jurisdictional complexities, the need for robust legal frameworks to govern emerging technologies, and internationalization of marginal economic cost. By examining these challenges, this paper aims to contribute to the ongoing discourse on how to navigate the legal landscape of digital public services to promote transparency, accountability, and trust between governments and citizens. Relevant legal principles shall be employed in order to elaborate on such legal challenges the e-revolution is bringing in the area of governance, with the ultimate question that remains open: Is this what citizens need?

Keywords: digital transformation, accountability, administrative law, public administration, cybersecurity risks.

* PhD, Lecturer, ORCID: 0009-0009-0144-685X, e-mail: *plarentruka@unyt.edu.al*

1. INTRODUCTION

Public services are undergoing a transformation from a traditional to a digital modus in most countries in the world, notwithstanding their level of development. This transformation could be explained by political reasons as much as by economic ones related to the accomplishment of cost efficiency, improvement of quality of services, increase in transparency and reduction in corruptive practices. Quantitative research is needed to observe the real impacts of digitalization in these directions. However, this paper is based on the assumption that the digitalization of public services is beneficial for society, without judging the proper effects it has in the quality and quantity of services. Rather, this paper addresses some concerns related to the legitimacy of the digitalization processes, including the Artificial Intelligence ("AI") systems, in terms of constitutional and legal principles regulating the public administration.

At the outset, the paper shall bring some notes on the most important legal and constitutional principles of administrative law and procedure permeating the traditional modus of public administration. These principles are mainly explored within the European Union jurisdiction, as an exemplary legal framework that has well combined treaty law with domestic law, and where the administrative law principles can be traced very clearly with the support of the jurisprudence of the European Court of Justice. In the third section we shall shed light on the main understanding of the digitalization processes of public services, to continue with some threats and benefits of the transformation process of the traditional public services into digitalized modus. Here, the concept of AI shall be also highlighted. In the third section, the process of the digitalization of public services shall be discussed in view of the constitutional and legal principles and institutions, before reaching some conclusion on this discourse.

2. PUBLIC SERVICES AND THEIR ANCHOR IN CONSTITUTIONAL AND ADMINISTRATIVE LEGAL PRINCIPLES

Public services can be referred to as services provided or facilitated by the governments for the general public´s convenience and benefit.[1] Such services are expected to be delivered by a public entity that has the capacity to act and can be provided to the public directly or indirectly, by means of government's subcontractors. In any case, the process for delivering such services, whether performed through a governmental body or a specialized corporation organized on a commercial basis, the public service should be delivered in conformity with legal principles governing the activities of public services or public administration. Indeed, administration of public services is based on administrative law to a wide extent and should be delivered as such in compliance with administrative procedures.

[1] See for example: Garner, B. A. 2004. *Black's Law Dictionary.* USA: Thomson West Publishing Co.

Developed in a national legislation context since the late medieval states and more furiously after the Enlightenment Movements, administrative law has expanded its frontiers under the pressure of comparative law to inspire even the law of the European Union since the early days of the Communities, the latter being depicted as a *sui generis* legal order with supranational features.[2] The main principles of administrative law inspire the administrative action from a substantive perspective. Such principles include:

- The general principle of administration through law, in that the administrative action should be in full compliance with the norms of general application provided in the primary and secondary legislation;[3]
- The principle of non-discrimination requiring an equal and non-discriminatory administrative conduct of the decision-making authority;[4]
- The principle of proportionality, requiring an administrative action to be proportionate to the objectives sought by the measure, by adopting the less radical means;[5]
- The principle of legal certainty[6] and of protection of legitimate expectations[7] by which the confidence of persons concerned deserves to be protected;
- The right to a hearing before an adverse decision is taken by a public authority;[8]
- The maintenance of a balanced and fair administrative process.

In addition to these substantive law principles governing the content of a certain decision-making, the administrative action should also comply with the principles of administrative procedure, which govern the way how the administrative body should act under the imperative of the rule of law.[9] Such principles and institutions include the duty to act with the granted powers (competencies), the right of the administrative entities to make investigations within the limitations thereof, right of defense of the affected or interested parties, respect of formal requirements of the decision-making process, such as the formulation of the decision, the duty to give reasons, notification to parties, etc.

All these principles are inherently vested in the administrative entities delivering any public services.

---

[2] On a more detailed analysis of the European Union law as a community of administrative law see: Schwarze, J. 1992. *European Administrative Law*. London: Office for Official Publications of the European Communities, pp. 11 *et seq*.

[3] See for example ECJ Case C-113/77 *NTN Toyo Bearing v Council* [1979], E.C.R. 1985, at 1209, para. 21.

[4] See for example ECJ Joined cases 117-76 and 16-77 *Ruckdeschel and Others v Hauptzollamt Hamburg-St. Annen* and *Diamalt AG v Hauptzollamt Intzenhoe* [1977], E.C.R. 1753, at 1770, para. 8.

[5] See for example ECJ C-11/70 *Internationale Handelsgesellschaft mbH v Einfuhr- und Vorratsstelle für Getreide und Futtermittel* [1970], E.C.R. 1125, at 1137

[6] See for example Case C-111/63 *Lemmerz Werke v High Authority* [1965], E.C.R. 677, at 690.

[7] See for example ECJ Case C-1/73 *Westzucker GmbH v Einfuhr- und Vorratsstelle für Zucker* [1973], E.C.R. 723, at 729, para. 6.

[8] See for example ECJ Case C-17/74 *Transocean Marine Paint Association v Commission* [1974], 1073, at 1080, para. 20.

[9] See for a detailed comparative view on the matter: Schwarze, 1992, p. 1173 *et seq*.

3. PUBLIC SERVICES IN THE ERA OF DIGITALIZATION

The concept of digitalization refers to the transformation of analog processes into digital processes by revising these processes and introducing new organizational models.[10] Since their invention, the governments have been the primary customers of the digital technology market. As of the '60s, the public sector organizations have felt the need to adopt new technologies to organize their work in a more effective and efficient manner, such as storing and retrieving citizens' data in shared databases.[11]

Such technology has been used for decades to support and improve productivity in delivering public services. Digital technology and the data revolution offer countries significant potential to increase public service efficiency and delivery, and to boost transparency and citizen trust.[12] In this view, the technology was not delivering the service, but was used as tool for storing and processing information and data management. Hence, since the late '70s the introduction of technology in the public services has been seen as a tool for improving the interaction between government and citizens.[13]

With the expansion of digital technology in the wide society, governments are relying more on digital products and services. A new potential is being created for bringing services closer to citizens by creating a direct digital link between the government as a service provider and the citizen as its client. The pandemic caused by the Coronavirus in 2019 can well be regarded as a trigger for shifting most of the public services from paper-based to digitalized products. This shift brought a different perspective in the perception of the systemic relationship between governments and citizens. Accessing public services remotely from any place in the world via the internet by means of various devices, from personal computers to mobile phones, is certainly more than just a convenient tool for reaching the services. Digitalization served in this way as a communication channel between the government and any citizen in an isolation period, thus turning into a tool for crisis management.[14] After the crisis, this platform was transformed into a great potential for de-bureaucratization of governance and the improvement of quality of services allowing for reallocation of human resources in a more efficient way. In this view, digital technology is regarded as a medium for interaction between the public official and the citizen, without eliminating the decision-making capabilities from the human actor. Hence, most services are still dependent on human resources, and this fades most of the advantages of the technology in terms of the time for delivering the services.[15]

[10] Fischer, C., Heuberger, M. & Heine, M. 2021. The impact of digitalization in the public sector: A systematic literature review. *Zeitschrift für Public Policy, Recht und Management,* 14(1), pp. 3-23.

[11] Mina-Raiu, L. & Melenciuc, M. 2022. The role of digitalisation in the process of improving the quality of urban public services. *Theoretical and Empirical Researches in Urban Management*, 17(4), pp. 22–35.

[12] Bjerde, A. & Demirgüç-Kunt, A. 2024. Digitalization and data can vastly improve public service delivery for citizens. World Bank blogs. Available at: https://blogs.worldbank.org/en/europeandcentralasia/digitalization-and-data-can-vastly-improve-public-service-delivery-citizens (4. 8. 2024).

[13] Lynn, T. *et al*. 2022. Digital Public Services. In: Lynn, T. (ed.): *Digital Towns*. Cham: Springer International Publishing, p. 50.

[14] Lynn *et al*., 2022, p. 50.

[15] Lynn *et al*., 2022, pp. 50–51.

Indeed, while the governments are still working on developing, enabling and improving the platform for delivering public services, they are at the same time preparing to adopt AI products for their needs, as tools that promise to deliver many more benefits in terms of productivity, cost-effectiveness, customer satisfaction and quality.

The focus of the digitalization process is mainly set on the capacity building of the public administration. As Bjerde and Demirgüç-Kunt put it: "Governments must encourage the adoption and development of robust data systems within the civil service. This will require recruitment and capacity building of staff to improve the use of data for evidence-based decision-making. Enhancing digitalization of public services and improving coordination of decentralized data systems across institutions are also necessary".[16]

Digitalization of public services brings significant benefits both from a quantitative and qualitative perspective. Automated systems certainly allow for a significant increase in the number of services by utilizing the same or even a lower number of human resources. Any citizen can communicate with the office 24/7 without being restricted by the opening hours. Considering that the majority of public services can be delivered remotely, the organizations may allocate their personnel in those areas where the work overload is higher, without having to increase personnel. The statistical information is easily managed and, in this way, it allows for adaptation strategies over time.

However, the provision of public services in a digitalized mode is based on several assumptions in order to work properly. First and foremost, it is based on the assumption that the system works perfectly well from an operational perspective. This means that the system shall not be interrupted for any reason and that the hardware, as well as software elements, are duly protected from security threats or unauthorized access. Secondly, it is based on the assumption that the citizens own both the digital devices and the necessary literacy to operate the systems or platforms for accessing the desired public services.[17] If these preconditions are not met, various threats of a legal nature may emerge.

Digitalization is criticized for detaching public services from the traditional places of government.[18] This is certainly not merely a physical problem. A citizen that is unable to access a digitally provided service, for various reasons, is essentially denied that service. Hence, although digitalization has increased the outreach of public services from the majority of society, essentially it constitutes a safe premise for denying access to a certain number of citizens. It is for this reason that alternative channels of communication should remain available and easily accessible by any citizen, in order to be able to obtain the relevant services.

Another downside of digitalization is the vulnerability of data to externally or internally driven cybersecurity threats. Such threats may cause a leak of sensitive data related to citizens or even a blackout of digital services for significant amounts of time. This would expose the governmental bodies to a significant civil liability towards citizens, and most

[16] Bjerde, A. & Demirgüç-Kunt, A. 2024. Digitalization and data can vastly improve public service delivery for citizens. World Bank blogs. Available at: https://blogs.worldbank.org/en/europeandcentralasia/digitalization-and-data-can-vastly-improve-public-service-delivery-citizens (4. 8. 2024).

[17] See also: Lynn *et al.*, 2022, p. 51.

[18] Lynn *et al.*, 2022, p. 51.

probably, the possibility of redressing could be impossible as there is no adequate policing force to enforce criminal offences in the global virtual environment. Therefore, amid these risks, the due level of care that the government should exercise could be prohibitively high.

Amid these drawbacks, by digitalizing public services, governments have established a new model for delivering the outputs of public administration. In this new paradigm, platforms of communication, such as e-governments, are more than a medium for facilitating the exchange of information between the government and its citizens by means of self-service tools. E-government, consisting of the use of digital technologies in government to promote efficiency and cost-effectiveness, has managed to facilitate public access to information for citizens and businesses, has favoured economic development, and made governments more accountable.[19] These platforms operating electronic governmental services, initially designed as a medium for the exchange of information, have modified the models of organizations in public entities, requiring further specialization in the use of technology for almost every member of the organization.

In terms of the actors involved, further intermediates are most likely to be involved in facilitating the communication between the classic actors, namely the public body and the citizens. Hence, the services now are more dependent on third parties acting as service providers for creating, maintaining and operating the platform of communication between the main actors. In terms of the initiation of public services, digitalization allows for 24/7 access to public services, and this certainly might change the expectations of citizens for the government response time in general.[20]

However, this new model is the basis for inseminating a future model of providing services through AI programs. Such programs shall overtake the human role in many directions and might well interact with the citizens in the name of the public administration during the delivery of services. Algorithms may lead to proactive delivery of services based on constant incoming data flow.[21] The European Union is among the first entities regulating the development, placing on the market, putting into service and use of AI systems, with the aim to classify and mitigate, prevent or prohibit potential risks these systems could cause to the public.[22] The AI Act is introduced on the premises that: "AI is a fast-evolving family of technologies that contributes to a wide array of economic, environmental and societal benefits across the entire spectrum of industries and social activities. By improving prediction, optimising operations and resource allocation, and personalising digital solutions available for individuals and organisations, the use of AI can provide key competitive advantages to undertakings and support socially and environmentally beneficial outcomes, for example in healthcare, agriculture, food safety,

[19] Terlizzi, A. 2021. The Digitalization of the Public Sector: A Systematic Literature Review. *Rivista Italiana di Politiche Pubbliche*, 1, pp. 5–38.

[20] Lynn *et al*., 2022, p. 50.

[21] Lynn *et al*., 2022, p. 51.

[22] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act).

education and training, media, sports, culture, infrastructure management, energy, transport and logistics, public services, security, justice, resource and energy efficiency, environmental monitoring, the conservation and restoration of biodiversity and ecosystems and climate change mitigation and adaptation".[23]

The digitalization of public services has changed significantly the concept of government for offering public services. This is not a mere transformation from paper to digits, but a transformation modus of communication of service providers with citizens.[24] Digital transformation implies change at the core of the organization, its processes and routines, as well as in its environment, business models, products, and services, and in the interaction between users and the organization itself.[25] Governments believe that this transformation is a game changer in terms of the amelioration of service quality as well as an opportunity to reduce corruption practices. The entire society needs to be prepared to respond adequately to this transformation, but the governments have also to adapt to a new reality. They need to reconceptualize their roles and functions in a digitalized society, where the threats could be as high as the benefits of this digitalization. Governments have to achieve greater trust in the system, including through responsiveness and transparency, and by providing opportunities for greater outreach among citizens.[26] In essence, governments need to redesign themselves into digital modus, and this requires a systemic reconceptualization of the public administration and the public sector in general. According to the OECD: "Becoming digital by design requires: 1) setting a strategic vision and clear mandate for digital government; 2) securing solid organizational leadership to steer digital government policies and actions, and 3) establishing effective coordination and collaboration within and outside the public sector for government-wide digital transformation in a coherent and inclusive manner".[27]

4. NORMATIVE PROPOSITIONS FROM THE PERSPECTIVE OF LEGAL PRINCIPLES

The above overview as well as the review of the main literature of recent years on the topic shows that the process of transformation of the public service to digital form is mainly seen as an infrastructural process, in which the governments have to establish institutions to develop and implement digitalization programs across the governmental institutions at all levels. Certainly, the benefits of this process could be enormous for society at large from an economic perspective. Nevertheless, the concerns associated with this process should not be neglected.

---

[23] Regulation (EU) 2024/1689, para. 4 Preamble.

[24] See also: Mina-Raiu & Melenciuc, 2022.

[25] Haug, N., Dan, S. & Mergel, I. 2024. Digitally-induced change in the public sector: a systematic review and research agenda. *Public Management Review*, 26 (7), pp. 1963–1987.

[26] Mishra, M. K. 2020. *Digital Transformation of Public Service and Administration*. Kiel, Hamburg: ZBW – Leibniz Information Centre for Economics.

[27] OECD. 2023a. Government at a Glance 2023. Available at: https://www.oecd.org/en/publications/government-at-a-glance-2023_3d5c5d31-en.html (10. 10. 2024).

The bureaucracy, with all its deficiencies in terms of delivering services in due course and quality, operates on the basis of constitutional principles and legal institutions. Many of these principles are usually implemented during the administration of public services as well as in the course of administrative procedures. In case of failures, administrative and/or judicial review stands as a guarantee for the protection of citizens' rights. The question raised in the context of digitalization of the public services, and particularly in their delivery through AI, is whether the algorithms are able to adhere to the general principles of the constitution and the legal principles to the same extent as public officials are.

The general principle of administration through law requires that the administrative action should be in full compliance with the norms of general application provided in the primary and secondary legislation. The primary and secondary legislation could be easily digitalized and as such, the machines could use the databases to generate automatic answers to many legal questions. Nonetheless, legal thinking in the application of law could barely be taught to machines. This process is inseminated to law students in universities and continues to be enriched throughout their careers. It barely ends, as long as human knowledge is endless. The application of law is everything but a mechanical process of norm application to a certain problem. In between, one could only imagine the challenges of teaching the art of legal analysis and interpretation to an AI machine, in order to obtain the necessary tools for decision-making.

Exercising administrative power is often associated with the duty of the public entity to refrain from discriminative practices. Often, the courts are overloaded with administrative claims related or amounting to discrimination for many written or unwritten grounds. It is for the courts to interpret the law in very sensitive yet narrow trials distinguishing right from wrong in deciding the fate of citizens.

Another core principle of public administration, the principle of accountability, means that the public administration is held accountable to the public for the proper implementation of its duties and responsibilities. The concept of accountability is quite complex and not easily absorbed by all institutions equally. Other stakeholders can also play a role in enhancing or confirming the accountability of the administration, and this makes the adherence to this principle, inasmuch as they may interact with the bureaucracy in various stages of a certain administrative process. While it could seem relatively possible to transform a certain workflow or administrative process into digital processes and programs, it is reasonably very challenging to expect the machines using algorithms to judge the moral values of principles in making decisions that could influence the lives of citizens. It is often the discretion of public officials that determines the veracity of the statements of various stakeholders in a certain administrative process.[28] Similarly, the principle of proportionality provides also for a certain margin of appreciation in exercising public power in particular cases. Hence, it remains unclear whether this discretion, which often could be based on, or determined by, psycho-emotional and cultural factors permeating the public discourse in a given society, could be vested in machines by any sort of digitalization transformation.

[28] Lindgren, I. & van Veenstra, A. F. 2018. Digital government transformation. In: Janssen, M. (ed.), *Proceedings of the 19th Annual International Conference on Digital Government Research Governance in the Data Age*. New York: ACM, pp. 1–6.

It is the duty of the public administration to guarantee the confidence of people involved in a particular administrative process, or obtaining a certain service. Yet, the principles of legal certainty and of protection of legitimate expectations, as provided in constitutional documents, laws and confirmed by jurisprudence, are quite complex to automatize. Similarly, one could hardly imagine the digitalized administrative bodies observing a fair balance between public and private interests in a certain administrative procedure, or even to exercise public authority within the granted powers (competencies), or to exercise the right to make investigations within the limitations thereof, or observing in an adequate manner other procedural rights, such as the right of defence of the affected or interested parties, to respect the formal requirements of the decision-making process, such as the formulation of the decision, the duty to give reasons, notification to parties. All these principles interact in a very complex way with each other, and this makes the administrative process quite unpredictable. Indeed, although the purpose of the law is to enhance predictability, the automatization or digitalization of the law does not necessarily serve that aim. The nature of law, inasmuch as the predictability is concerned, aims to strike a fair balance under the "regulatory dilemma." If the lawmaker regulates every human behaviour, the law becomes impossible to implement as the transaction costs in society will increase prohibitively high. In case the lawmaker chooses not to regulate, the trials in the implementation of the law might endanger the legal certainty itself. The art of legislative policy is then to strike the proper balance between these two ends, none of which is purely desired. While the legislators regulate, through a minimalistic approach, the most common and indispensable interests of the society, the principles put some barriers both to citizens and public officials in the conduct of their everyday activities. Here, the question is to what extent would digitalization really guarantee a proper transformation of the public from human to digital modus. Alignment and adherence to shared ethical values and principles for the management of algorithms are essential when using AI in the public sector.[29]

The discourse with the introduction of AI takes another dimension. AI systems are still under development and the mere fact that their adherence to constitutional and legal principles and institutions is quite complex, it should be required that such systems do not get introduced into service providers unless they pass the tests for fundamental rights impact assessment.[30] In addition, AI systems should be programmed to respect the rule of law, human rights, and democratic and human-centred values, including the principles of non-discrimination and equality, freedom, dignity, the autonomy of individuals, privacy and data protection, diversity, fairness, social justice, and internationally recognized labour rights. To this end, AI actors should implement mechanisms and safeguards, such as capacity for human agency and oversight, including addressing risks arising from uses outside of the intended purpose, intentional misuse, or unintentional misuse in a manner appropriate to the context and consistent with the state of the art.[31]

[29] OECD, 2023a.

[30] Regulation (EU) 2024/1689, Art. 27.

[31] OECD. 2023b. Recommendation of the Council on Artificial Intelligence. Available at: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449 (10. 10. 2024).

Notwithstanding the above, it should be expected that jurisdictional questions should often arise. AI systems are developed in particular jurisdictions, and their implantation in foreign countries should not be easily adapted from a jurisdictional perspective. This is due to the fact that legal systems and families remain extremely diverse in almost every discipline of law, even in the areas and regions where legal unification has produced a significant degree of legal integration, such as the European Union.

5. CONCLUSION

From the moral perspective, the reduction of the human role in the decision-making processes needs to be judged upon the ability of the machines to fully substitute the humans in such roles. It should be noted that the human dimension inherent in traditional public administration and public service, in general, is not a material value that can be convertible to digital products by means of algorithms. Before surrendering our institutions and elected governments to machines, human society should make sure that such algorithms are aligned and adhere to shared ethical values, principles constitutional principles and other legal institutions.

One should not neglect the fact that cyberthreats could have a severe impact on human rights, inasmuch as such impacts could be significantly large and extended in time. Hence, as far as digitalization is concerned, if the central servers of a government are attacked, besides the leaking of information, the services could be denied to the public for a significant amount of time. For governments, it is quite impossible to return to a paper-based administration in a short period of time. Hence, the denial of public services is unavoidable and could amount to a less costly solution.

It is for the above reasons that the digitalization of public services should be taken very carefully from the government, not as a race to the bottom, but as a process of self-development of the public administration into a new system of governance, where the constitutional and legal principles and institutions are also adapted to the new concept of digitalization of public administration.

LIST OF REFERENCES

Bjerde, A. & Demirgüç-Kunt, A. 2024. Digitalization and data can vastly improve public service delivery for citizens. World Bank blogs. Available at: https://blogs.worldbank.org/en/europeandcentralasia/digitalization-and-data-can-vastly-improve-public-service-delivery-citizens (4. 8. 2024).

Fischer, C., Heuberger, M. & Heine, M. 2021. The impact of digitalization in the public sector: A systematic literature review. *Zeitschrift für Public Policy, Recht und Management*, 14(1), pp. 3-23. https://doi.org/10.3224/dms.v14i1.13

Garner, B. A. 2004. *Black's Law Dictionary.* USA: Thomson West Publishing Co.

Haug, N., Dan, S. & Mergel, I. 2024. Digitally-induced change in the public sector: a systematic review and research agenda. *Public Management Review*, 26 (7), pp. 1963–1987. https://doi.org/10.1080/14719037.2023.2234917

Lindgren, I. & van Veenstra, A. F. 2018. Digital government transformation. In: Janssen, M. (ed.), *Proceedings of the 19th Annual International Conference on Digital Government Research Governance in the Data Age*. New York: ACM, pp. 1–6. https://doi.org/10.1145/3209281.3209302

Lynn, T. *et al.* 2022. Digital Public Services. In: Lynn, T. (ed.): *Digital Towns*. Cham: Springer International Publishing, pp. 49–68. https://doi.org/10.1007/978-3-030-91247-5_3

Mina-Raiu, L. & Melenciuc, M. 2022. The role of digitalisation in the process of improving the quality of urban public services. *Theoretical and Empirical Researches in Urban Management,* 17(4), pp. 22–35.

Mishra, M. K. 2020. *Digital Transformation of Public Service and Administration*. Kiel, Hamburg: ZBW – Leibniz Information Centre for Economics.

OECD. 2023a. Government at a Glance 2023. Available at: https://www.oecd.org/en/publications/government-at-a-glance-2023_3d5c5d31-en.html (10. 10. 2024).

OECD. 2023b. Recommendation of the Council on Artificial Intelligence. Available at: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449 (10. 10. 2024).

Schwarze, J. 1992. *European Administrative Law*. London: Office for Official Publications of the European Communities.

Terlizzi, A. 2021. The Digitalization of the Public Sector: A Systematic Literature Review. *Rivista Italiana di Politiche Pubbliche,* 1, pp. 5–38.

Legal Sources and Case Law

Case C-111/63 Lemmerz Werke v High Authority [1965], E.C.R. 677.

ECJ Case C-113/77 NTN Toyo Bearing v Council [1979], E.C.R. 1985.

ECJ Joined cases 117-76 and 16-77 Ruckdeschel and Others v Hauptzollamt Hamburg-St. Annen and Diamalt AG v Hauptzollamt Intzenhoe [1977], E.C.R. 1753.

ECJ C-11/70 Internationale Handelsgesellschaft mbH v Einfuhr- und Vorratsstelle für Getreide und Futtermittel [1970], E.C.R. 1125.

ECJ Case C-1/73 Westzucker GmbH v Einfuhr- und Vorratsstelle für Zucker [1973], E.C.R. 723.

ECJ Case C-17/74 Transocean Marine Paint Association v Commission [1974], 1073.

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act).

UDC: 004.738.5:343 DOI: 10.56461/iup_rlrc.2024.5.ch4

*Ajna JODANOVIĆ**
Faculty of Law, University of Bihać, Bosnia and Herzegovina

THE DIGITAL SERVICES ACT PACKAGE: PROTECTION OF THE FUNDAMENTAL RIGHTS OF DIGITAL SERVICE USERS IN THE EUROPEAN UNION

In recent years, the European Union has been trying to adequately respond to constant technological progress and changes in the digital world by establishing a legislative and legal framework aimed at protecting users in the online environment. The Digital Services Act (DSA) and the Digital Markets Act (DMA) as a single set of rules are applied throughout the European Union with the aim of creating a safer digital space in which the fundamental rights of all users of digital services are protected. In addition to the protection of fundamental rights, the aim of these rules is to establish equal conditions for encouraging innovation, growth and competitiveness, both in the single European market and globally. The aim of the paper is to present the fundamental differences between the DMA and the DSA in the context of separate regulatory measures and obligations they impose on digital platforms. Summarily observing, the main goal of the research is the analysis of the legislative and legal framework of the European Union aimed at creating a safer and more open digital space. The results of the research will present the importance of EU regulations as part of the Digital Services Package in the context of the adoption of significant new rules aimed at strengthening the rights of users in the online environment and increasing transparency in the operation of internet platforms.

Keywords: European Union, legislative and legal framework, digital space, protection of rights.

1. INTRODUCTORY REMARKS

For many years, the European Union (hereafter: EU) has been pursuing a digital strategy by developing a modern legal framework to protect online users' fundamental rights while facilitating business expansion and access to new markets.[1] The

* PhD, Associate Professor, ORCID: 0000-0002-0146-411X, e-mail: *ajna_x@hotmail.com*

[1] Turillazzi, A. *et al.* 2023. The digital services act: an analysis of its ethical, legal, and social implications. *Law, Innovation and Technology*, 15(1), p. 83.

goal of the EU is to create a digital single market and to govern the digital transition underway. As part of the digital single market strategy, the European Commission has recently developed the "Digital Service Act Package," consisting of the Digital Service Act (DSA) and the Digital Market Act (DMA). It sets out a first comprehensive rulebook for the online platforms with the specific purpose of creating a safer digital space where the fundamental rights of users are protected and to establish a level playing field for businesses.[2] On 16 December 2020, the European Commission delivered on the plans proposed in the European Digital Strategy[3] by publishing two proposals related to the governance of digital services in the European Union: the Digital Services Act (DSA) and the Digital Markets Act (DMA). The much-awaited regulatory reform is often mentioned in the context of content moderation and freedom of expression, market power and competition. It is, however, important to bear in mind the contractual nature of the relationship between users and platforms and the additional contracts concluded on the platform between the users, in particular traders and consumers. Moreover, the monetisation offered by digital platforms has led to new dynamics and economic interests.[4]

Taking into account that in the past 20 years, online platforms have emerged, grown and become sources of both benefits and risks for citizens, including exposure to illegal contents, the DMA and DSA strike a balance between fostering innovation and competition while working to ensure consumer protection and a secure online environment. The introduction of these regulations reflects the growing recognition of the need to regulate the digital sector and bring it in line with societal values and market principles.[5] Both legislative acts were adopted by the Council and the European Parliament in 2022. Since 17 February 2024, the full implementation of the DSA rules has come into effect. From this date forward, all digital service providers are expected to comply with the new regulations.

The goal of the research is to contribute to the better understanding of the relevance of EU regulations, which make up the Digital Services Package, vis-à-vis the need to strengthen the rights of users in the online environment and increase transparency in the operation of internet platforms. In an effort to pursue the set research goals, the paper will analyse the impact of the DSA Package on citizens and platforms, and will determine differences in regulatory measures and obligations between the DSA and the DMA. In the final part of the paper, we will analyse the Commission's enforcement powers under the DSA.

---

2 Chiarell, M. L. 2023. Digital Markets Act (DMA) and Digital Services Act (DSA): New Rules for the EU Digital Environment. *Athens Journal of Law*, 9(1), p. 34.

3 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A Digital Single Market Strategy for Europe, Brussels, 06/05/2015, COM (2015) 192 final

4 Cauffman, C. & Goanta, C. 2021. A New Order: The Digital Services Act and Consumer Protection. *European Journal of Risk Regulation*, 12, p. 758.

5 See: Usercentrics. 2023. Key differences between the Digital Markets Act (DMA) and the Digital Services Act (DSA). Available at: https://usercentrics.com/knowledge-hub/differences-between-digital-markets-act-and-digital-services-act/ (10. 10. 2024).

2. THE DIGITAL SERVICES ACT PACKAGE

Since the adoption of the e-commerce Directive[6] two decades ago, online platforms have evolved into key intermediaries in the digital economy, as well as essential sources and shapers of information. They have developed from passive, neutral intermediaries to active co-creators of the digital sphere. In the attention economy, digital services and content are optimised to benefit online platforms' advertising-driven business models.[7] The COVID-19 crisis has made it obvious that the digital economy is and will remain central to the lives of many, and that numerous individuals, companies and states rely on e-commerce and digital services in many aspects of their lives. Beyond e-commerce, e-education, e-health or e-work, perhaps the time has come to talk about e-life? In this context, the Digital Services Act Package appears to be a landmark piece of legislation, intended to update a legal framework that has remained unchanged since the adoption of the e-Commerce Directive in 2000. In the past 20 years, online platforms have emerged, grown and become sources of both benefits and risks for citizens, including exposure to illegal contents. Some of these platforms have also gradually built up the ability to control huge parts of the digital ecosystems in which citizens now live and work.[8]

Navigating the nuanced landscape of platform liability regimes and fundamental rights demands a comprehensive look at key legislative frameworks. Originating in the 1990s, early limited liability regimes aimed for a precarious balance between user rights and the operational freedoms of DSPs. This ethos has been enshrined in the E-Commerce Directive, which stands as a landmark in shaping the responsibilities of online platforms in the European Union. However, with the advent of the Digital Single Market Strategy and the impending Digital Services Act, the policy equilibrium is being recalibrated.[9]

---

[6] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), *OJ* L 178, 17/07/2000.

[7] A central component of this business model is the moderation of content in order to encourage users to spend more time on the platform and share more personal data. Today's search engines, social media networks and e-commerce platforms determine not only which users can participate in the ecosystem or the way transactions are to be carried out via the platform but also what information corresponding users will receive. See: Buiten, M. C. 2021. The Digital Services Act from Intermediary Liability to Platform Regulation. *Journal of Intellectual Property. Information Technology and E-Commerce Law*, 12(5), p. 361.

[8] Ponce Del Castillo, A. 2020. The Digital Services Act package: Reflections on the EU Commission's policy options. *ETUI Policy Brief*, 12, p. 1.

[9] The new legislative thrust appears to retain some of the foundational principles while introducing more stringent obligations on platforms, thereby sparking debates about rights, responsibilities, and the overarching role of digital intermediaries in society. As the European Union seeks to harmonise and deepen its digital single market, this evolving legal framework continues to stir contentious dialogues around balancing corporate interests, user freedoms and the rule of law. See more in: Frosio, G. & Geiger, C. 2023. Taking fundamental rights seriously in the Digital Services Act's platform liability regime. *European Law Journal*, 29(1-2), pp. 36-67.

On 15 December 2020, the European Commission submitted its legislative proposal for digital service to the European Council and the European Parliament. The proposal has two components, the Digital Services Act (DSA) and the Digital Market Act (DMA). Together, these constitute the DSA Package.[10] The DMA and DSA were enacted by the European Commission under one regulation package, the Digital Services Act Package (DSA Package), but they are in fact separate and independent laws.[11]

Digital services impact our lives in many different ways. We use them to communicate with each other, shop, order food, find information, watch films, listen to music and more. Digital services also make it easier for companies to trade across borders and access new markets. While these are some examples of the many benefits of the digital transformation, there are also problems. Despite a range of targeted, sector-specific interventions at EU level, there are still significant gaps and legal burdens to address at the dawn of the 2030 Digital Decade.[12] The Digital Services Act (DSA) and the Digital Market Act (DMA) form a single set of rules that apply across the whole European Union (EU). They have 2 main goals: 1) to create a safer digital space in which the fundamental rights of all users of digital services are protected; 2) to establish a level playing field to foster innovation, growth, and competitiveness, both in the European Single Market and globally.[13]

The first part of the Package is the Digital Services Act (DSA), which addresses platform practices in terms of content management and distribution. The DSA requires companies to take a more active role in monitoring and responding to issues such as political disinformation campaigns or hate speech and applies financial penalties if platforms are in breach. These fines can be up to 6% of the company's global revenue. The DSA also requires that platforms provide more transparency to users; for example, more information about advert microtargeting will be provided so users understand why a particular ad appears on their feeds. The DSA aims to introduce more accountability for platforms and their practices around content removal. This mainly concerns very large platforms, which are required to proactively mitigate systemic risks that enable disinformation or other harmful contents to spread. In this, the DSA

[10] UCD Centre for Digital Policy. *The Digital Services Act Package: A Primer.* Available at: https://digitalpolicy.ie/the-digital-services-act-package-a-primer/ (10. 10. 2024).

[11] See: Usercentrics, 2023.

[12] For example, some large platforms control important ecosystems in the digital economy. They have emerged as gatekeepers in digital markets, with the power to act as private rule-makers. Their rules sometimes result in unfair conditions for businesses using these platforms and less choice for consumers. Another concern is the trade and exchange of illegal goods, services and content online. And, online services are being misused by manipulative algorithmic systems to amplify the spread of disinformation, and for other harmful purposes. These challenges and the way platforms address them have a significant impact on fundamental rights online. Therefore, the European Union adopted a modern legal framework that ensures the safety of users online, establishes governance with the protection of fundamental rights at its forefront, and maintains fair and open online platform environment. See: European Commission. f. The Digital Services Act Package. Available at: https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package (10. 10. 2024).

[13] European Commission. f. The Digital Services Act Package. Available at: https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package (10. 10. 2024).

complements the updated Code of Practice on Disinformation[14] which is part of the European Democracy Action Plan.[15], [16]

The second part of the Package is the Digital Markets Act (DMA) which focuses on companies' roles as "gatekeepers" between businesses and consumers.[17]

2.1. The DSA Package: Implications for Platforms

For platforms, the implementation of the DSA Package means that they have to adjust their practices in ways that enhance rather than stifle competitiveness and innovation and that allow smaller companies to grow (DMA). Secondly, they have to operate with clear and transparent rules and be accountable to their users (DSA). Additionally, the DSA Package aims to harmonise platforms' responsibilities across the EU and improve transparency for users and researchers. The new rules apply differently to different size platforms. Very large platforms, defined as those with a user base that reaches at least 10% of the EU population, or 45 million people, are addressed as "Gatekeepers" because they have "a central role in facilitating the public debate and economic transactions." Very large platforms are considered to pose a higher risk than smaller, more niche platforms and would be subject to specific obligations regarding risk management. This means Google, Facebook and Twitter have to ramp up their reporting and open some more windows into their operations. They need to become more transparent and provide information on recommender algorithms that select and present information

[14] The new Code aims to achieve the objectives of the Commission's Guidance presented in May 2021, by setting a broader range of commitments and measures to counter online disinformation. The strengthened Code of Practice on Disinformation has been signed and presented on the 16 June 2022 by 34 signatories who have joined the revision process of the 2018 Code. The 2022 Code of Practice is the result of the work carried out by the signatories. It is for the signatories to decide which commitments they sign up to and it is their responsibility to ensure the effectiveness of their commitments' implementation. The Code is not endorsed by the Commission, while the Commission set out its expectations in the Guidance and considers that, as a whole, the Code fulfils these expectations. European Commission. The 2022 Code of Practice on Disinformation. Available at: https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation (10. 10. 2024).

[15] On 3 December 2020, the European Commission presented its Democracy Action Plan to empower citizens and build more resilient democracies across the EU. It is a non-legislative initiative announcing further steps, including legislative ones. Protecting and strengthening European democracy and in particular European elections and the threat of disinformation raise challenges that cannot be addressed by national or local action alone. The Plan is centred around the individual rights and freedoms, transparency and accountability. European Parliament. 2024. European Democracy Action Plan In "A New Push for European Democracy". Available at: https://www.europarl.europa.eu/legislative-train/theme-a-new-push-for-european-democracy/file-european-democracy-action-plan (10. 10. 2024).

[16] See: UCD Centre for Digital Policy.

[17] Here the focus is on "levelling the playing field" and countering the oligopolies set up by large platforms. This is accomplished mainly by setting up stiff fines for anti-competitive practices, which can be up to 10% of the company's global revenue. For example, a search engine like Google cannot prioritise their own services ahead of a third-party business in search results. In online marketplaces, "own brand" items cannot be prioritised ahead of third-party products. A second important stipulation of the DMA is to counter illegal trade and increase business transparency. For example, new online businesses will be required to provide much more detailed information which can help authorities identify and prevent sales of illegal goods. See: UCD Centre for Digital Policy.

on search and social media feeds to users. Very large platforms also have to arrange for independent investigators and auditors to access and examine algorithms, recommender systems, and content moderation practices to verify compliance. Compliance officers and cooperation with authorities in the case of crises are also required. Further, the obligations under the DSA require enhanced measures to address illegal content, such as working with "trusted flaggers" to identify and report content. Micro and small companies still have some obligations under the DSA, but they will not be as extensive as those of big tech with its bigger resources. Rather, obligations are proportionate to platforms' ability and size.[18]

2.2. The DSA Package: Implications for Citizens

These enhanced obligations of digital service providers aim to improve the digital environment for users. The DSA attempts to crack down on illegal activities online and protect citizens from harm while protecting fundamental rights, including freedom of expression, and the right to privacy. It is a challenging balancing act. Currently, the platforms make decisions on what types of content or accounts to take down. Companies such as Facebook or YouTube can remove communities and individuals without any accountability or need to offer information on who was removed and why. The Act requires digital platforms to be more transparent about what they take down and why, as well as to allow users to challenge any content moderation decisions such as takedowns. But how does it address illegal or harmful content such as hate speech and disinformation? The DSA retains the exemption from liability for online platforms for content posted by users. However, there are certain obligations regarding risk management and due diligence that must be adhered to. Under the DSA users should have enhanced mechanisms to report illegal content on social media. The platforms have requirements to respond within set timeframes and are subject to penalties if they fail to meet targets. In this respect, the main provisions are to strengthen the Code of Practice on Disinformation and the Code of Conduct on illegal contents. In other words, the DSA does not go so far as to define what illegal and harmful content is; these rules are contained in other EU and national legislations.[19]

3. THE DIGITAL SERVICES ACT (DSA)

Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022, on a Single Market for Digital Services, commonly known as the Digital Services Act ("DSA"), is another important milestone in the European Union's ("EU") regulation of the digital sector.[20]

---

[18] UCD Centre for Digital Policy.

[19] See: UCD Centre for Digital Policy.

[20] See: Cuatrecasas. Digital Services Act: New regime for intermediary services. Available at: https://www.cuatrecasas.com/en/portugal/intellectual-property/art/digital-services-act-new-regime-for-intermediary-services (10. 10. 2024).

Since the adoption of Directive 2000/31/EC (the "e-Commerce Directive"), epochal changes have occurred that have transformed society and the market, giving rise to a "digital revolution."[21] New and innovative digital services have emerged, changing our daily lives, shaping how we communicate, connect, consume goods, and do business. This transformation is defined as the new digital revolution, which is as fundamental as that caused by the industrial revolution. At the same time, the use of digital services has also become the source of new risks and challenges, both for society as a whole and for individuals.[22]

The DSA was originally announced by *Ursula von der Leyen* in her political guidelines in July 2019, and forms part of a legislative package for regulating the online environment in the EU and beyond. It is an element of the European Digital Strategy "Shaping Europe's Digital Future," and was subject to public consultation from June to September 2020.[23]

The Digital Services Act is the most important and most ambitious regulation in the world in the field of the protection of the digital space against the spread of illegal content, and the protection of users' fundamental rights.[24] The goal of the DSA rules is that online platforms must implement ways to prevent and remove posts containing illegal goods, services, or content while simultaneously giving users the means to report this type of content. End users should enjoy a safer online experience and the companies operating these services have a more clearly defined set of rules they need to follow.[25]

On 15 December 2020, the European Commission submitted a proposal for a Regulation on a Single Market for Digital Services (Digital Services Act, DSA) and amending Directive 2000/31/EC.[26] In November 2021, the Council of the European Union reached agreement on an amended version of this proposal,[27] and on 20 December 2021 the

---

[21] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ("Directive on Electronic Commerce"), *OJ* L 178, 17.7.2000.

[22] This situation has been exacerbated by the pandemic emergency which has dramatically increased the use of online bargaining and the use of digital services. In the meantime, digitalisation has become one of the pillars of post-pandemic transformation of the EU. For this reason, given the immense importance of online platforms and digital services, European Institutions feel the need to introduce specific rules for the sector to improve online access to goods and services for consumers, to prohibit the dissemination of illegal content and products, as well as to facilitate innovation, competition and growth of the European digital ecosystem. See: Chiarell, 2023, pp. 33–34.

[23] See: Herbert Smith Freehills. 2022. The Digital Services Act: Europe's new framework for online regulation to come into force next month. Available at: https://www.herbertsmithfreehills.com/notes/tmt/2022-10/the-digital-services-act-europes-new-framework-for-online-regulation-to-come-into-force-next-month (10. 10. 2024).

[24] See: The Digital Services Act (DSA) Regulation (EU) 2022/2065. Available at: https://www.eu-digital-services-act.com/ (10. 10. 2024).

[25] See: Alorica. EU Digital Services Act. Ensuring Online Safety and Fairness. Available at: https://www.alorica.com/insights/resource/eu-digital-services-act-ensuring-online-safety-and-fairness (10. 10. 2024).

[26] COM (2020) 825: Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC.

[27] Council of the European Union, Proposal for a Digital Services Act and amending Directive 2000/31/EC – General approach, 18/11/2021, Council Document 13203/21.

European Parliament's Committee on the Internal Market and Consumer Protection (IMCO) released a draft for an EP legislative resolution.[28] The legislative project "seeks to ensure the best conditions for the provision of innovative digital services in the internal market, to contribute to online safety and the protection of fundamental rights, and to set a robust and durable governance structure for the effective supervision of providers of intermediary services."[29] To achieve these aims, the DSA sets out numerous due diligence obligations for intermediaries concerning any type of illegal information, including copyright-infringing content.[30, 31]

The Digital Services Act was formally adopted by the European Parliament on 5 July 2022, and by the Council of the European Union on 18 July 2022. It was published in the Official Journal of the European Union on 27 October 2022. It came into effect gradually in 2023 and 2024.[32] The DSA governs online intermediaries through a set of horizontal rules and a continuation of the intermediary liability regime in the European Union. The liability rules are restated for all intermediaries while due diligence obligations are created, and a new governance regime is established to oversee implementation, reporting, compliance, and enforcement. The DSA is said to provide legal certainty, remove disincentives for platforms to take voluntary measures and keep their services safe, preserve a fair balance of fundamental rights and prohibition of general monitoring obligations.[33] The DSA is more comprehensive than any previous legislation of the dig-

---

[28] Report on the proposal for a regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC, 20/12/2021 – (COM(2020)0825 – C9-0418/2020 – 2020/0361(COD))

[29] COM (2020) 825: Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC.

[30] See Recital 12 of the Digital Services Act (DSA) of the European Union: In order to achieve the objective of ensuring a safe, predictable and trustworthy online environment, for the purpose of this Regulation the concept of "illegal content" should broadly reflect the existing rules in the offline environment. In particular, the concept of "illegal content" should be defined broadly to cover information relating to illegal content, products, services and activities. In particular, that concept should be understood to refer to information, irrespective of its form, that under the applicable law is either itself illegal, such as illegal hate speech or terrorist content and unlawful discriminatory content, or that the applicable rules render illegal in view of the fact that it relates to illegal activities. Illustrative examples include the sharing of images depicting child sexual abuse, the unlawful non-consensual sharing of private images, online stalking, the sale of non-compliant or counterfeit products, the sale of products or the provision of services in infringement of consumer protection law, the non-authorised use of copyright protected material, the illegal offer of accommodation services or the illegal sale of live animals. In contrast, an eyewitness video of a potential crime should not be considered to constitute illegal content, merely because it depicts an illegal act, where recording or disseminating such a video to the public is not illegal under national or Union law. In this regard, it is immaterial whether the illegality of the information or activity results from Union law or from national law that is in compliance with Union law and what the precise nature or subject matter is of the law in question.

[31] Peukert, A. *et al*. 2022. European Copyright Society – Comment on Copyright and the Digital Services Act Proposal. *IIC - International Review of Intellectual Property and Competition Law,* 53, p. 359.

[32] See: Secure Privacy. 2024. Digital Services Act (DSA) of the European Union Explained. Available at: https://secureprivacy.ai/blog/eu-digital-services-act-explained (10. 10. 2024).

[33] See more in: Leiser, M. 2023. Analysing the European Union's Digital Services Act Provisions for the Curtailment of Fake News: Disinformation, & Online Manipulation. pp. 1-13. Available at: https://osf.io/

ital world in the European Union and addresses a range of issues, such as content moderation, monetisation, competition and accountability.[34]

The DSA revamps the principle of the limitation of liability for online intermediaries contained in the e-Commerce Directive, but its core innovation is a new chapter on standards for transparency, and the accountability of all providers of "intermediary services" regarding illegal and harmful content.[35] The DSA's general date of applicability was 17 February 2024. However, the DSA applies to providers of online platforms and of online search engines whose services have been designated as Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs) as from four months following notification of the decision designating those services as such.[36] The DSA establishes a notice-and-action regime, a legal framework that requires intermediaries to restrict content that violates their own terms of service or the laws of an EU Member State. In turn, people have the right to appeal decisions to remove or alter their content.[37] The DSA regulates online intermediaries and platforms such as marketplaces, social networks, content-sharing platforms, app stores, and online travel and accommodation platforms. Its main goal is to prevent illegal and harmful activities online and the spread of disinformation. It ensures user safety, protects fundamental rights, and creates a fair and open online platform environment.

---

preprints/socarxiv/rkhx4 (10. 10. 2024).

[34] The European Commission under *Ursula von der Leyen* has made the digital world a priority with the "A Europe Fit for the Digital Age" initiative and its dual purpose: to assert and strengthen Europe's digital sovereignty, that is, its capacity to develop innovative new technologies; and to set up its own standards, which derive from Europe's commitment to fundamental rights for citizens and a competitive free market. The DSA Package constitutes an example of co-regulation, where the regulatory body (the EU in this instance), sets the framework for the operation of the tech industry, but the industry itself is responsible for developing rules for implementation and enforcement mechanisms and for delivering self-assessment reports to regulators. It is, in this sense, a light touch approach. See: UCD Centre for Digital Policy.

[35] See: Crowell. 2022. The Digital Services Act: EU Regulation of Intermediary Service Providers Imminent. Available at: https://www.crowell.com/en/insights/client-alerts/the-digital-services-act-eu-regulation-of-intermediary-service-providers-imminent (10. 10. 2024).

[36] On 25 April 2023, the Commission designated 17 online platforms as VLOPs and 2 online search engines as VLOSEs. Consequently, the DSA already applies to the providers of those VLOPs and VLOSEs, for which the Commission enjoys the competence to supervise and enforce. If VLOPs and VLOSEs fail to comply with DSA requirements to moderate content or address systemic risks, they can be fined up to 6 percent of their annual global revenue. The European Commission has yet to issue any fines, but it has opened formal proceedings against a host of platforms, including TikTok and X. Freedom House. 2022. The EU Digital Services Act: A Win for Transparency, New tech regulations are poised to help civil society foster a more democratic online experience. Available at: https://freedomhouse.org/article/eu-digital-services-act-win-transparency (10. 10. 2024).

[37] Under the law, regulators from each EU member state will help to implement the law and appoint "trusted flaggers," to point out content that is illegal or violates intermediaries' terms of services. The act also requires that intermediaries identify risks that are inherent to their platform's design, known as systemic risks, including features that negatively impact civic discourse, electoral processes, and fundamental rights. It empowers independent auditors to assess how well intermediaries are mitigating these risks, which is crucial to understanding how platforms behave ahead of high-stakes events like elections. See: Freedom House, 2022.

3.1. The EU Framework for Fundamental Rights Online: The Role of the DSA

In response to the challenges connected to the proliferation of illegal content, goods, and services, the EU has adopted over the past years a variety of initiatives, including sector- specific legislation, non-binding guidelines for platforms to tackle illegal content online and measures based on self-regulatory cooperation. These initiatives have to a certain extent complemented the e-Commerce Directive and have increased awareness on the risk and harms brought by the digital transformations, including as regards the implications for the protection of fundamental rights. However, as acknowledged by the Commission, such interventions inevitably fail to address the systemic societal risks posed by digital services and online platforms in particular. Crucially, the lack of updated and harmonized rules hinders appropriate levels of protection for fundamental rights, adding legal uncertainty and fragmentation to an already complex regulatory landscape.[38]

In order to guarantee proportional balancing of fundamental rights in the DSA, reference must be primarily made to the legal framework set up both by the Charter of Fundamental Rights of the European Union (EU Charter)[39] and the European Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention of Human Rights or ECHR),[40] as construed respectively by the CJEU and the ECtHR. Only the strict application of the fundamental rights that can be extracted from this legal framework which binds Member States can help secure a coherent legislative framework and a horizontal, fundamental rights compliant approach in the different legislative interventions.[41]

The DSA protects consumers and their fundamental rights online by setting clear and proportionate rules. It fosters innovation, growth and competitiveness, and facilitates the scaling up of smaller platforms, SMEs and start-ups. The roles of users, platforms, and public authorities are rebalanced according to European values, placing citizens at the centre.[42]

---

[38] Buri, I. & Van Hoboken, J. 2021. *The Digital Services Act (DSA) proposal: a critical overview.* Amsterdam: Faculty of Law University of Amsterdam, p. 5.

[39] See: Charter of Fundamental Rights of the European Union, 2012 OJ (C 326) 391. See also See Article 6 (1) of the Treaty on the European Union (TEU): "The Union recognises the rights, freedoms and principles set out in the Charter of Fundamental Rights of the European Union of 7 December 2000, as adapted at Strasbourg, on 12 December 2007, which shall have the same legal value as the Treaties. The provisions of the Charter shall not extend in any way the competences of the Union as defined in the Treaties."

[40] See Article 6 (2) and (3) of the Treaty on the European Union (TEU): "The Union shall accede to the European Convention for the Protection of Human Rights and Fundamental Freedoms. Such accession shall not affect the Union's competences as defined in the Treaties. Fundamental rights, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms and as they result from the constitutional traditions common to the Member States, shall constitute general principles of the Union's law."

[41] Frosio & Geiger, 2023, pp. 44–45.

[42] See: European Commission. Digital Services Act (DSA) overview. Available at: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en (10. 10. 2024).

Recital 3 of the DSA stresses that a responsible behaviour of DSPs is essential for allowing the exercise of the fundamental rights guaranteed in the EU Charter, "in particular the freedom of expression and information and the freedom to conduct a business, and the right to non-discrimination."[43] The DSA should be interpreted and applied in accordance with the fundamental rights recognised by the EU Charter with an obligations for public authorities exercising the powers provided by the DSA to achieve a fair balance of the conflicting fundamental rights, in accordance with the principle of proportionality. However, the DSA also includes some specific prescriptive obligations for DSPs to enforce fundamental rights. First, by defining its scope, the DSA states that the aim of the Regulation is to regulate an online environment "where fundamental rights enshrined in the Charter are effectively protected." Secondly, the DSA has included the impact of digital services on the exercise of fundamental rights protected by the EU Charter as a category of systemic risks that should be assessed in depth by very large online platforms (VLOPs) and very large online search engines (VLOSEs), a new category of online platform to which special obligations apply. VLOPs and VLOSEs must also take mitigating measures as a result of the systemic risk assessment they carry out in connection to the functioning of their services. In particular, the risk assessment of platforms' services must regard the impact of digital services on (i) human dignity (ii) the freedom of expression and information, (iii) personal data, (iv) the right to private life, (v) the right to non-discrimination and (vi) the rights of the child and (vii) consumer protection. Finally, the DSA highlights the role of fundamental rights in conjunction with the emerging sensitive issues of the extra territorial enforcement of DSPs' obligations, which has been recently debated before the CJEU and other international courts. Fundamental rights must be taken into consideration among the conditions to define the territorial scope of "orders to act against illegal content," which should "not exceed what is strictly necessary to achieve its objective". On one side, the territorial—and extraterritorial scope—will be determined by EU and national law but also by the proportional balancing of fundamental rights that emerges from the EU Charter. On the other side, the territorial scope should be, however, limited by international law principles, including comity, according to what the CJEU established in *Glawischnig-Piesczek*[44] *and CNIL*[45].

[43] See Recital 3 of Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act): "Responsible and diligent behaviour by providers of intermediary services is essential for a safe, predictable and trustworthy online environment and for allowing Union citizens and other persons to exercise their fundamental rights guaranteed in the Charter of Fundamental Rights of the European Union (the "Charter"), in particular the freedom of expression and of information, the freedom to conduct a business, the right to non-discrimination and the attainment of a high level of consumer protection."

[44] See: Case *Glawischnig-Piesczek*, ECLI:EU:C:2019:821, see n. 60, para 48–52. See also: Frosio & Geiger, 2023, pp. 36–67.

[45] In 2015, the CNIL informed Google that it must remove links from all versions of its search engine throughout the world when implementing an erasure request from a data subject. Google declined to comply, limiting its de-referencing of links obtained via its search engines with domain extensions inside the EU only (e.g., google.de or google.fr), as well as using geo-blocking techniques, which prohibits links from appearing in searches performed in France regardless of the version used. As a consequence, the CNIL imposed a fine of EUR 100,000 on Google due to non-compliance with the data protection legislation. Google filed a request

Only strict application of the fundamental principles that can be extracted by this constitutional framework can help secure a coherent legislative framework and a horizontal, fundamental-rights compliant approach in the different legislative interventions.[46]

Some inappropriate online services, content, and people can potentially be dangerous or harmful to children. Therefore, the DSA aims to provide a list of measures platforms and search engines can follow to create a digital environment where children feel safe. The DSA specifically aims to provide: a) the "best interest of the child" principle;[47] b) the right to protection for the child; c) the right to freedom of expression; d) the right not to face discrimination; d) the right to protection of personal data; e) a high level of consumer protection.[48] Platforms need to ensure that their online services focus on safety, security, and privacy for children. Some measures that are enforced to protect children are: a) prevent ads targeting children based on profiling; b) ensure terms and conditions are understandable to children; c) interfaces designed with privacy, security, and safety measures in mind. Specifically, DSA forbids dark patterns, which are interfaces that trick users into making decisions they didn't intend to make; d) availability of parental control to help parents limit access to online services; e) simple methods of reporting illegal or harmful content; f) systems that securely verify a user's age before granting access to a service.[49]

---

with the Conseil d'État to have the fine annulled. The Conseil d'État subsequently submitted concerns to the Court of Justice, citing "many severe challenges" surrounding the interpretation of the directive. In its decision, the CJEU ruled that the territorial scope of the right to be forgotten in the context of search engines is limited to the borders of the EU Member States, since under EU law no obligation to do so exists. However, while reading paragraph 72, we notice that the Court tries to embed a global application and scope of the right to be forgotten as a general principle. Stating that, although EU law does not provide for an obligation, when granting a request for removal of links, to carry out such removal for all versions of the search engine in question, it does not prohibit it either. Consequently, a supervisory authority or a court of a Member State still has jurisdiction, in the light of national standards for the protection of fundamental rights, to balance the rights of the data subject against the freedom of information of the public and to instruct the operator of the relevant search engine, where appropriate, to remove the links for all versions of that search engine after such consideration. So it remains to be seen whether the court will uphold this case law in the future. See: Case 507/17 *Google LLC v Commission nationale de l'informatique et des libertés (CNIL),* ECLI:EU:C:2019:772, para 64–72; GDPR Hub. CJEU - C-507/17 - Google (Territorial scope of de-referencing). Available at: https://gdprhub.eu/index.php?title=CJEU_-_C-507/17_-_Google_(Territorial_scope_of_de-referencing) (10. 10. 2024).

[46] Case *Glawischnig-Piesczek*, ECLI:EU:C:2019:821, see n. 60, para 48–52; Frosio & Geiger, 2023, pp. 36–67.

[47] The principle of the best interests of the child is one of the four overarching guiding principles on children's rights (right to non-discrimination, best interests, the right to life, survival and development, and the right to participation or right to express views and have them taken into account). It is anchored in Art. 3 (1) of the Convention on the Rights of the Child and in Art. 24 (2) of the Charter of Fundamental Rights of the European Union. Both instruments give children the right to have their best interests taken into account as a primary consideration in all actions or decisions that concern or affect children. In addition, Art. 24 (3) of the Charter further addresses the need to take into account the child's right to maintain a relationship with both parents. This has also been underlined in the case law of the Court of Justice of the European Union (CJEU), e.g., in the Case C-230/21. See: European Commission. Best interests of the child (BIC). Available at: https://home-affairs.ec.europa.eu/networks/european-migration-network-emn/emn-asylum-and-migration-glossary/glossary/best-interests-child-bic_en (10. 10. 2024).

[48] Marshall-Heyman, T. 2024. Digital Services Act: Age Verification and Protecting Children Online. Available at: https://www.criipto.com/blog/digital-services-act (10. 10. 2024).

[49] Marshall-Heyman, 2024.

Protection of user rights does not only depend on dispute resolution mechanisms. Legislation should provide for safeguards that allow users to effectively complain about decisions, actions, or inaction of DSPs. First, a notification about actions to be undertaken would be an essential tool to guarantee users' right to a legal remedy. According to Mostert, the "digital due process" should be based on the following principles: (1) a fair and public review by an independent and impartial panel or competent court within a reasonable time; (2) a proper prior notification of the review; (3) an opportunity for a user or notifier to respond and present evidence in respect of a takedown or a stay-up inaction by a platform; (4) the right to legal representation; (5) the right to appeal to an appeals panel, alternative dispute resolution tribunal or competent court; (6) notifiers may at any stage in the process seek access to competent courts; (7) the right to receive a decision which clearly articulates the reason for that decision; and (8) the right to an effective remedy including, for example, stay-up or takedown of the content.[50] These principles adapt safeguards and guarantees developed by the CJEU and the ECtHR to the digital world.

In summary, a robust platform liability regime should be anchored in the principles of due process, ensuring fair and impartial dispute resolution with practical access to justice. It must foster transparency, accountability, and contestability, particularly in algorithmic decision-making, with the implementation of "digital due process" principles, including a fair public review, proper prior notification, the opportunity for users to present evidence, the right to legal representation, the right to appeal, and the right to an effective remedy.[51]

3.2. Commission's Enforcement Powers Under the Digital Services Act (DSA)

The Digital Services Act (DSA) provides a framework for cooperation between the Commission, EU and national authorities to ensure platforms meet its obligations. To ensure an efficient enforcement of the DSA, the Commission is building an enforcement network of relevant European entities, national authorities and leading experts in the field covered by the Digital Services Act (DSA). This cooperation framework supports the Commission and Digital Services Coordinators (DSCs) in the supervision, enforcement and monitoring of the Regulation together with the Commission.[52] Under the DSA, the Commission has both investigative and sanctioning powers.

---

[50] See: Mostert, F. 2020. 'Digital due process': a need for online justice. *Journal of Intellectual Property Law & Practice*, 15(5), pp. 378–389.

[51] To address power imbalances, the system should advocate for the "equality of arms" between platforms and users, so that any significant advantage in terms of access to relevant information should be balanced. Both state-based and non-state grievance mechanisms have roles to play, provided they meet standards of impartiality and effectiveness. Legislative safeguards and independent oversight are also crucial to ensure that these principles are not just theoretical but are effectively implemented in practice. Emphasising its role as a cornerstone in this context, the DSA has already laid down the essential legal norms that serve as a blueprint for actualising these guiding principles. See: Frosio & Geiger, 2023, pp. 57–58.

[52] See: European Commission. The cooperation framework under the Digital Services Act. Available at: https://digital-strategy.ec.europa.eu/en/policies/dsa-cooperation (10. 10. 2024).

a) When it comes to *investigative powers*, the Commission can: 1) send a request for information (RFI) to verify platforms' compliance with the DSA. The RFI can be sent also upon decision of the Commission. Fines* can be imposed if a reply is incorrect, misleading or incomplete; 2) order access to the VLOPS' data and algorithms, e.g., to assess how the algorithm/recommender system of a platform promotes illegal content. Fines can be imposed if the provider does not comply; 3) conduct interviews of any person who might have information on the subject matter of an investigation. Interviews can be conducted only with the person's consent and cannot be forced; 4) conduct inspections at the VLOP's premises. Inspections can be conducted only after consultation of the DSC of the Member State of establishment. The DSC may need to request an authorisation issued by the judge in the Member State of establishment. Fines can be imposed if the provider refuses to submit to inspection.[53]
b) When it comes to the sanctioning powers, starting from 17 February 2024, the Commission can:
    1) Apply fines up to 6% of the worldwide annual turnover in case of: a) breach of DSA obligations; b) failure to comply with interim measures; c) breach of commitments.
    2) Apply periodic penalties up to 5% of the average daily worldwide turnover for each day of delay in complying with remedies, interim measures, commitments.[54]

As a last resort measures, if the infringement persists and causes serious harm to users and entails criminal offences involving threat to persons' life or safety, the Commission can request the temporary suspension of the service, following a specific procedure: 1) the Commission requests interested parties to submit written observations within a period that shall not be less than 14 working days, describing the measures it intends to request and identifying the intended addressee or addressees; 2) the Commission requests the DSC of the Member State of establishment to seek from the competent judicial authority of its Member State an order to temporarily restrict access to the service concerned by the infringement; 3) the Digital Service Coordinator seeks the order from the judge; 4) the order must be issued by a judge in the Member State of establishment.[55]

On 26 March 2024, the Commission has published guidelines under the DSA for the mitigation of systemic risks online for elections. The European Commission has published guidelines on recommended measures to Very Large Online Platforms and

[53] Fines up to 1% of the worldwide annual turnover can be imposed. Periodic penalties up to 5% of the average daily worldwide turnover can be imposed for each day of delay in replying to RFI by decision or allowing inspection. See: European Commission. The enforcement framework under the Digital Services Act. Available at: https://digital-strategy.ec.europa.eu/en/policies/dsa-enforcement (10. 10. 2024).

[54] See: European Commission. The cooperation framework under the Digital Services Act. Available at: https://digital-strategy.ec.europa.eu/en/policies/dsa-cooperation (10. 10. 2024).

[55] European Commission. The cooperation framework under the Digital Services Act. Available at: https://digital-strategy.ec.europa.eu/en/policies/dsa-cooperation (10. 10. 2024).

Search Engines to mitigate systemic risks online that may impact the integrity of elections, with specific guidance for the upcoming European Parliament elections in June.[56]

The European Commission has launched the DSA Transparency Database,[57] which tracks when online platforms remove content, and also requires VLOPs to maintain their own databases with detailed information on all their online advertisements. These repositories can be a tremendous asset for researchers, and can also help regulators identify harms and propose creative strategies to combat them.[58]

To monitor the addressees' compliance with the new rules and possibly enforce them, the DSA introduces two new oversight institutions: Digital Services Coordinators at the national level, and the Board for Digital Services at the EU level. These new public agencies would have specific supervisory rights with regard to the DSA—something the committee reports by the EU Parliament have been strongly advocating for.[59] Dig-

---

[56] These guidelines recommend mitigation measures and best practices to be undertaken by Very Large Online Platforms and Search Engines before, during, and after electoral events, such as to:

a) Reinforce their internal processes, including by setting up internal teams with adequate resources, using available analysis and information on local context-specific risks and on the use of their services by users to search and obtain information before, during and after elections, to improve their mitigation measures;
b) Implement elections-specific risk mitigation measures tailored to each individual electoral period and local context;
c) Adopt specific mitigation measures linked to generative AI: Very Large Online Platforms and Search Engines whose services could be used to create and/or disseminate generative AI content should assess and mitigate specific risks linked to AI, for example by clearly labelling content generated by AI (such as deepfakes), adapting their terms and conditions accordingly and enforcing them adequately;
d) Cooperate with EU level and national authorities, independent experts, and civil society organisations to foster an efficient exchange of information before, during and after the election and facilitate the use of adequate mitigation measures, including in the areas of Foreign Information Manipulation and Interference (FIMI), disinformation and cybersecurity;
e) Assess the effectiveness of the measures through post-election reviews.

Available at: EU Digital Services Act. The Digital Services Act (DSA) Regulation (EU) 2022/2065. Available at: https://www.eu-digital-services-act.com/ (10. 10. 2024).

[57] The Digital Services Act (DSA), obliges providers of hosting services to inform their users of the content moderation decisions they take and explain the reasons behind those decisions in so-called statements of reasons. To enhance transparency and facilitate scrutiny over content moderation decisions, providers of online platforms need to submit these statements of reasons to the DSA Transparency Database. The database allows to track the content moderation decisions taken by providers of online platforms in almost real-time. It also offers various tools for accessing, analysing, and downloading the information that platforms need to make available when they take content moderation decisions, contributing to the monitoring of the dissemination of illegal and harmful content online. See more at: European Commission. i. Welcome to the DSA Transparency Database! Available at: https://transparency.dsa.ec.europa.eu/ (10. 10. 2024).

[58] See: Freedom House, 2022.

[59] Under Art. 38 (2) DSA, each Member State shall designate a Digital Services Coordinator (hereinafter DSC) responsible for "all matters relating to application and enforcement" of the DSA. For supervision, investigation, and enforcement, the DSC shall have special rights awarded by the DSA and common to all Member States. Moreover, they will have the authority to impose fines, to impose measures against a service's management, and, as ultima ratio, to decide over the interruption of a service if the DSC identifies repeated infringements (Art. 41 DSA). To allow for a harmonized approach within the EU, the DSCs shall cooperate with each other and with other competent authorities. The DSA lays the cornerstone for this

ital Services Coordinators help the Commission to monitor and enforce obligations in the Digital Services Act (DSA). The Commission and the national Digital Service Coordinators (DSCs) are responsible for supervising, enforcing and monitoring the DSA.[60]

4. THE DIGITAL MARKET ACT (DMA)

Following the initial proposal of the European Commission in December 2020, the Regulation was adopted by the European Parliament and the Council on 14 September 2022. It was published in the Official Journal on 12 October 2022.[61] The DMA entered into force on 1 November 2022 and became applicable on 2 May 2023. Within two months of that date, companies providing core platform services will have to notify the Commission if they meet the quantitative thresholds and provide all relevant information. The Commission will then have 45 working days to adopt a decision designating a specific gatekeeper. The designated gatekeepers will have a maximum of six months after the Commission decision to ensure compliance with the obligations and prohibitions laid down in the DMA.[62]

The DMA builds on the existing P2B Regulation[63] and is aligned with other EU instruments, including the EU Charter of Fundamental Rights, the European Convention of Human Rights, the General Data Protection Regulation,[64] EU competition rules and the EU's consumer law acquis. The purpose of the DMA is to ensure the proper functioning of the market through effective competition in digital markets, and to solve

new authority (Art. 39 DSA) but leaves any further development of the task at the Members States' discretion. States that already adopted a similar law could, for instance, merge the already existing competent authority at the national level with the DSC. See: Flew, T. & Martin, F. R. 2022. *Digital Platform Regulation: Global Perspectives on Internet Governance*. Cham: Springer Nature Switzerland AG, pp. 73–74.

[60] Each Member State has to designate a Digital Services Coordinator (DSC), who is responsible for all matters relating to the application and enforcement of the DSA in that country. On 24 April, the European Commission decided to open infringement procedures by sending letters of formal notice to six Member States where significant delays in the designation and or empowerment of their Digital Services Coordinators had to be expected. At that time, Estonia, Poland, and Slovakia still had to designate their Digital Services Coordinators. In addition, despite designating their Digital Services Coordinators, Cyprus, Czechia and Portugal still have to empower them with the necessary powers and competences to carry out their tasks, including the imposition of sanctions in cases of non-compliance. When deciding on the next steps, the Commission will take into account the communication by Member States of the designation and empowerment of their Digital Services Coordinators. European Commission. Digital Services Coordinators. Available at: https://digital-strategy.ec.europa.eu/en/policies/dsa-dscs (10. 10. 2024).

[61] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act), OJ L 265, 12/10/2022.

[62] See: European Commission. About the Digital Markets Act. Available at: https://digital-markets-act.ec.europa.eu/about-dma_en (10. 10. 2024).

[63] Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services.

[64] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

the critical issues of the market to facilitate innovation and consumer protection by combating unfair and anti-competitive behaviour. It aims to allow platforms to unlock their full potential by facing the most critical issues at the EU level, so "as to allow end users and business users alike to reap the full benefits of the platform economy and the digital economy at large, in a contestable and fair environment."[65]

The DMA applies to companies that own large online platforms—which the law designates and refers to as gatekeepers—play a dominant role in the digital ecosystem, providing core platform services—also specified by the law—that provide essential access to end users. These gatekeepers are characterized by their strong economic position, significant influence over and impact on the market and on competitors, and active presence in multiple EU countries or the entire EU/EEA region. To be subject to the DMA, a company must hold a strong market position and connect a large user base to numerous businesses.[66]

The purpose of DMA is to contribute to the proper functioning of the internal market by laying down harmonised rules ensuring for all businesses, contestable and fair markets in the digital sector across the Union where gatekeepers are present, to the benefit of business users and end users. DMA shall apply to core platform services provided or offered by gatekeepers to business users established in the Union or end users established or located in the Union, irrespective of the place of establishment or residence of the gatekeepers and irrespective of the law otherwise applicable to the provision of service.[67]

5. DIFFERENCES IN REGULATORY MEASURES AND OBLIGATIONS BETWEEN DIGITAL SERVICES ACT (DSA) AND THE DIGITAL MARKET ACT (DMA)

The DMA is in particular aimed at harmonising existing rules in member states, in order to better prevent the formation of bottlenecks and the imposition of entry barriers to the digital single market. The DSA establishes a series of fundamental rules and principles regarding, essentially, the way intermediaries participate in the publication and distribution of online content. It especially focuses on content hosting and sharing platforms, such as Facebook, TikTok, Twitter, and YouTube.[68]

Differences between the Digital Markets Act (DMA) and the Digital Services Act (DSA) are apparent in the separate regulatory measures and obligations they impose on digital platforms. The DMA sets out a list of obligations for designated gatekeepers, including requirements to: a) eliminate unfair or anti-competitive practices; b) provide

[65] Chiarell, 2023, p. 38.

[66] The six designated gatekeeper companies to date that fall under the DMA's requirements include: a) Apple; b) Amazon; c) Alphabet (parent company of Google and Android; d) Meta (parent company of Facebook, Instagram and WhatsApp); e) ByteDance (parent company of TikTok); f) Microsoft. Under the DMA, gatekeepers will need to follow a set of rules that prevent them from engaging in unfair practices on their platforms, promoting a fairer and more competitive digital environment. See: Usercentrics, 2023.

[67] Article 1 of Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act).

[68] Barata, J. *et al*. 2021. *Unravelling the Digital Services Act package - RIS Special*. Strasbourg: European Audiovisual Observatory, p. 5.

access to data gathered or generated on their platforms; c) ensure compatibility; d) prevent favouring their own or specific partners' functionality or services. These provisions are aimed at promoting a fair and competitive digital landscape within the European Union. On the other hand, the Digital Services Act (DSA) aims to create a safer and more transparent online environment for users. The DSA introduces new obligations for online platforms, including: a) content moderation; b) mechanisms for handling user complaints; c) transparency of algorithms; d) cooperation with authorities; e) measures to prevent spreading illegal content.

While both Acts address different aspects of the digital market, there are some areas of overlap. For example, both regulations recognize the importance of transparency in online platforms' practices. The DMA requires designated gatekeepers to provide transparency reports on their algorithms and ranking criteria, while the DSA requires reports on content moderation practices from the VLOPs.[69]

6. CONCLUSION

As of February 2024, the European Union's (EU) Digital Services Act (DSA) is fully implemented across the bloc. The DSA is a landmark law for platform responsibility, and could transform how we understand and address the harms that online platforms exacerbate, including disinformation and harassment. Provisions within the DSA promise to aid civil society during a crucial period, as a record number of countries hold elections, generative artificial intelligence (AI) threatens to further distort the information landscape, and tech companies downsize their content moderation, trust and safety, and human rights teams. The act's potential lies in its transparency measures, which require more detailed reporting from tech companies and allow external researchers to access online platforms' data.[70] In conclusion, both the DSA and DMA are significant regulations introduced in the EU to regulate the digital market and address the challenges posed by digital platforms. While the DMA focuses on market competition and levelling the playing field, the DSA emphasizes user protection and transparency. Despite their differences, both Acts recognize the importance of transparency in online platforms' practices and aim to create a fair and competitive digital market. As businesses and consumers adapt to these regulations, the business landscape online will likely undergo significant changes.[71] The DSA is imperfect. The law could lead to the excessive removal of people's content as companies try to avoid fines, and governments within the EU could leverage the act to remove content protected by international human rights standards. Civil society and academic experts have also warned that emergency powers could be abused to block platforms. Additionally, the regulatory burden could make it difficult for small businesses with fewer financial and personnel resources to comply. However, despite these risks, the DSA presents a welcome model for internet regulation. As the

[69] See: Usercentrics, 2023.

[70] See: Freedom House, 2022.

[71] See: Usercentrics, 2023.

European Commission implements the act, platforms should ensure they are adopting best practices globally, not just in the EU. Because of the outsized impact that EU regulation has globally, the act's transparency measures can help civil society, policymakers, and tech companies across the world chart a path toward a more rights-centred and democratic online experience.[72]

LIST OF REFERENCES

Literature

Barata, J. *et al.* 2021. *Unravelling the Digital Services Act package - RIS Special*. Strasbourg: European Audiovisual Observatory.

Buiten, M. C. 2021. The Digital Services Act from Intermediary Liability to Platform Regulation. Journal of Intellectual Property. *Information Technology and E-Commerce Law*, 12(5), pp. 361-380. https://doi.org/10.2139/ssrn.3876328

Buri, I. & Van Hoboken, J. 2021. *The Digital Services Act (DSA) proposal: a critical overview*. Amsterdam: Faculty of Law University of Amsterdam.

Cauffman, C. & Goanta, C. 2021. A New Order: The Digital Services Act and Consumer Protection. *European Journal of Risk Regulation*, 12, pp. 758–774. https://doi.org/10.1017/err.2021.8

Chiarell, M. L. 2023. Digital Markets Act (DMA) and Digital Services Act (DSA): New Rules for the EU Digital Environment. *Athens Journal of Law*, 9(1), p. 33-58. https://doi.org/10.30958/ajl.9-1-2

Flew, T. & Martin, F. R. 2022. *Digital Platform Regulation: Global Perspectives on Internet Governance*. Cham: Springer Nature Switzerland AG. https://doi.org/10.1007/978-3-030-95220-4

Frosio, G. & Geiger, C. 2023. Taking fundamental rights seriously in the Digital Services Act's platform liability regime. *European Law Journal*, 29(1-2), pp. 36-67. https://doi.org/10.1111/eulj.12475

Leiser, M. 2023. Analysing the European Union's Digital Services Act Provisions for the Curtailment of Fake News: Disinformation, & Online Manipulation. pp. 1-13. Available at: https://osf.io/preprints/socarxiv/rkhx4 (10. 10. 2024). https://doi.org/10.31235/osf.io/rkhx4

Mostert, F. 2020. 'Digital due process': a need for online justice. *Journal of Intellectual Property Law & Practice*, 15(5), pp. 378–389. https://doi.org/10.1093/jiplp/jpaa024

Peukert, A. *et al.* 2022. European Copyright Society – Comment on Copyright and the Digital Services Act Proposal. *IIC - International Review of Intellectual Property and Competition Law*, 53, pp. 358-376. https://doi.org/10.1007/s40319-022-01154-1

Ponce Del Castillo, A. 2020. The Digital Services Act package: Reflections on the EU Commission's policy options. *ETUI Policy Brief*, 12, pp. 1-6. https://doi.org/10.2139/ssrn.3699389

[72] The EU Digital Services Act: A Win for Transparency, *op. cit.* (10/07/2024)

Turillazzi, A. *et al*. 2023. The digital services act: an analysis of its ethical, legal, and social implications. *Law, Innovation and Technology*, 15(1), pp. 83-106. https://doi.org /10.1080/17579961.2023.2184136

Legal Sources and Case Law

Case 507/17 Google LLC v Commission nationale de l'informatique et des libertés (CNIL), ECLI:EU:C:2019:772.

Case Glawischnig-Piesczek, ECLI:EU:C:2019:82.

Charter of Fundamental Rights of the European Union, 2012 OJ (C 326) 391.

Consolidated version of the Treaty on European Union, O. J. C 326, 26.10.2012.

Council of the European Union, Proposal for a Digital Services Act and amending Directive 2000/31/ EC – General approach, 18.11.2021, Council Document 13203/21.

COM (2020) 825: Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC.

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A Digital Single Market Strategy for Europe, Brussels, 6.5.2015, COM(2015) 192 final.

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), OJ L 178.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services.

Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/ EC (Digital Services Act), OJ L 265.

Report on the proposal for a regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC, 20.12.2021 - (COM(2020)0825 – C9-0418/2020 – 2020/0361(COD)).

Treaty on the European Union (TEU).

Internet Sources:

Alorica. EU Digital Services Act. Ensuring Online Safety and Fairness. Available at: https://www.alorica.com/insights/resource/eu-digital-services-act-ensuring-online-safety-and-fairness (10. 10. 2024).

Crowell. 2022. The Digital Services Act: EU Regulation of Intermediary Service Providers Imminent. Available at: https://www.crowell.com/en/insights/client-alerts/

the-digital-services-act-eu-regulation-of-intermediary-service-providers-imminent (10. 10. 2024).
Cuatrecasas. Digital Services Act: New regime for intermediary services. Available at: https://www.cuatrecasas.com/en/portugal/intellectual-property/art/digital-services-act-new-regime-for-intermediary-services (10. 10. 2024).
European Commission. Best interests of the child (BIC). Available at: https://home-affairs.ec.europa.eu/networks/european-migration-network-emn/emn-asylum-and-migration-glossary/glossary/best-interests-child-bic_en (10. 10. 2024).
European Commission. Digital Services Coordinators. Available at: https://digital-strategy.ec.europa.eu/en/policies/dsa-dscs (10. 10. 2024).
European Commission. About the Digital Markets Act. Available at: https://digital-markets-act.ec.europa.eu/about-dma_en (10. 10. 2024).
European Commission. The cooperation framework under the Digital Services Act. Available at: https://digital-strategy.ec.europa.eu/en/policies/dsa-cooperation (10. 10. 2024).
European Commission. The enforcement framework under the Digital Services Act. Available at: https://digital-strategy.ec.europa.eu/en/policies/dsa-enforcement (10. 10. 2024).
European Commission. f. The Digital Services Act Package. Available at: https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package (10. 10. 2024).
European Commission. Digital Services Act (DSA) overview. Available at: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en (10. 10. 2024).
European Commission. The 2022 Code of Practice on Disinformation. Available at: https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation (10. 10. 2024).
European Commission. i. Welcome to the DSA Transparency Database! Available at: https://transparency.dsa.ec.europa.eu/ (10. 10. 2024).
European Parliament. 2024. European Democracy Action Plan In "A New Push for European Democracy". Available at: https://www.europarl.europa.eu/legislative-train/theme-a-new-push-for-european-democracy/file-european-democracy-action-plan (10. 10. 2024).
EU Digital Services Act. The Digital Services Act (DSA) Regulation (EU) 2022/2065. Available at: https://www.eu-digital-services-act.com/ (10. 10. 2024).
Freedom House. 2022. The EU Digital Services Act: A Win for Transparency, New tech regulations are poised to help civil society foster a more democratic online experience. Available at: https://freedomhouse.org/article/eu-digital-services-act-win-transparency (10. 10. 2024).
GDPR Hub. CJEU - C-507/17 - Google (Territorial scope of de-referencing). Available at: https://gdprhub.eu/index.php?title=CJEU_-_C-507/17_-_Google_(Territorial_scope_of_de-referencing) (10. 10. 2024).
Herbert Smith Freehills. 2022. The Digital Services Act: Europe's new framework for online regulation to come into force next month. Available at: https://www.herbertsmithfreehills.com/notes/tmt/2022-10/the-digital-services-act-europes-new-framework-for-online-regulation-to-come-into-force-next-month (10. 10. 2024).

Marshall-Heyman, T. 2024. Digital Services Act: Age Verification and Protecting Children Online. Available at: https://www.criipto.com/blog/digital-services-act (10. 10. 2024).
Secure Privacy. 2024. Digital Services Act (DSA) of the European Union Explained. Available at: https://secureprivacy.ai/blog/eu-digital-services-act-explained (10. 10. 2024).
UCD Centre for Digital Policy. The Digital Services Act Package: A Primer. Available at: https://digitalpolicy.ie/the-digital-services-act-package-a-primer/ (10. 10. 2024).
Usercentrics. 2023. Key differences between the Digital Markets Act (DMA) and the Digital Services Act (DSA). Available at: https://usercentrics.com/knowledge-hub/differences-between-digital-markets-act-and-digital-services-act/ (10. 10. 2024).

UDC: 336.74:004 DOI: 10.56461/iup_rlrc.2024.5.ch5

Botond BRESZKOVICS*
Faculty of Law, University of Pécs, Hungary

NFTs UNDER THE FRAMEWORK OF MiCA**

In the European Union (EU), there are two distinct periods regarding the regulation of crypto assets, related services and crypto assets service providers. The distinction is based on the existence or lack of specific regulation of crypto assets. From a different perspective, a distinction can also be made between the regulatory environment before and after the implementation of the Markets in Crypto Assets regulation (MiCA/MiCAR). The former period can be characterized as the EU regulatory wild west of crypto assets, where the crypto sector was regulated, but only partially, by amending existing legislation. The second era of crypto-relevant EU regulation is the development of a specific regulatory framework striving for consistent legal cover of the whole crypto sector. In this paper, without aiming to be exhaustive, the MiCA's specific regulatory framework applying to the crypto asset market is described. The aim of this paper is to provide a summary overview of the state or lack of provisions in the MiCA regarding non-fungible tokens.

Keywords: EU, MiCA, DLT, crypto, NFT.

1. INTRODUCTION

It is not unfamiliar in the world of law that an examination begins with a clear definition of the relevant terms, and this case is no different. The present paper is fundamentally determined by one highly relevant term, namely the non-fungible token (NFT). Hence, in the following, I present a short review of the different academic approaches aimed to define NFT, following my own definition. Next, I will present the state of the NFT market between 2021 and 2023, based on the findings of market research companies. Finally, I will outline the evolving legal situation of non-fungible tokens in the European Union (EU), especially taking into account relevant legal provisions of the Markets in Crypto-Assets Regulation (MiCA/MiCAR).

* PhD student, ORCID: 0009-0005-9399-9005, e-mail: *breszkovics.botond@pte.ajk.hu*

** This paper was supported by „A Kulturális és Innovációs Minisztérium ÚNKP-23-3-II kódszámú új Nemzeti Kiválóság Programjának a Nemzeti Kutatási, Fejlesztési és Innovációs Alapból finanszírozott szakmai támogatásával készült”

2. THE DEFINITION OF NFT

The clear definition of non-fungible tokens greatly aids in their regulation. Nevertheless, the definition of NFTs has not yet been defined by the legislature. Fortunately, the academic literature has developed a wide range of conceptual approaches, which are presented below (Király, 2020, p. 45):

- The non-fungible token is a crypto asset on the blockchain that has unique data content that allows it to be identified, thereby distinguishing it from other crypto assets (Peres *et al*., 2023, p. 5).
- The NFT is a digitally created token that is a digital replica of a (virtual) asset without infringing intellectual property rights (Kraizberg, 2023).
- It is a digital asset that displays an object that exists in the material world, such as artwork, music, or a video game (Edelman, 2022, p. 35).
- An NFT is a unique collectable digital asset that exists on the blockchain, which identifies the ownership of a physical or virtual asset. According to this approach there are no two identical NFTs and the value of NFTs can be influenced by both demand or uniqueness and also by individual factors such as public interest in having NFTs (Hokianto, 2023, p. 9).
- It is a unique digital identifier that is stored safely on a public blockchain ensuring that tokens are not interchangeable and cannot be sub-divided (Laurence & Kim, 2021, p. 55). Note here that this approach excludes so-called fractional non-fungible tokens from its definition.
- The NFT is a means of authenticating the ownership and tracking the transaction of an individual physical or virtual object (Mazur, 2021, p. 20).
- NFTs are blockchain-based, non-fungible digital representations (tokens) of real or virtual content that, using structured metadata, enable the sale of these tokens and, rarely the content behind them, for alternative (cryptocurrency-based) compensation, without the need for third parties as intermediaries (Mezei, 2022, p. 9).

The technological definition of NFT is no less relevant, as the structure of a non-fungible token is framed by different technical standards. In terms of technical standards, 2018 is a notable year as the so-called ERC-721 technical standard was released in the Ethereum system, allowing the creation of NFTs (see erc721.org). Until today, the ERC-721 technical standard represents the typical NFT structure, but only on the Ethereum network. Beyond this, the ERC-1155 technical standard (see enjin.io) is also relevant which allows the bundled transfer of several fungible tokens and non-fungible tokens in a single transaction (Harmath, 2022).

Beyond the main definitions of NFTs, it is also useful to briefly discuss the classification of NFTs, which can be based on different factors. Most often the distinction is based on the existence or lack of utility associated with the non-fungible token. In this approach, a distinction can be made between simple or traditional NFTs and the utility NFT category (uNFT). Whereas a traditional NFT does not have any associated utility, the uNFT always has some linked utility (Bujtár, 2018, p. 150).

A further classification possibility is based on the applicability of the NFT. In this classification, NFT categories can be distinguished between art, gaming, collectables, domain names, membership, music, profile picture (PFP) and photography. An NFT may fall into one of the above categories, whether or not it has any advantage.

The previously presented academic and technical definitions show that, although there is no universally accepted definition of NFT, the relevant key elements can be clearly identified. The key characteristics defining NFT are the digital nature of the token as well as the uniqueness of the identifying data of the token ensuring that there is no possibility of fungibility. In addition, it is essential that the token provides a certificate of authority and is also based on any blockchain technology. In my view, the non-fungibility of a certain token should be examined on a case-by-case basis and should be classified on the basis of its actual scope of application. The reason for the *ad hoc* assessment is that the typical NFT technical standard used (like ERC-721) does not exclude initial NFT offerings (INOs), which process may cause the loss of uniqueness of the NFT. The reason is that a large volume of NFT offerings will basically cause the technically non-fungible tokens to act like fungible tokens.

In my own approach, based on the above, a non-fungible token (NFT) is a unique set of data that is fully or partially recorded on the blockchain. The NFT, as a virtual asset, can represent either physical or digital objects and other items.

The definition is supported by a comment which helps to make a distinction between the different NFTs. Depending on the localisation of the NFT data, a distinction can be made between on-chain and off-chain NFTs. In the case of on-chain NFTs, all data, such as metadata and the image, video or any other media file that visually represents the NFT, are located on the blockchain. By contrast, in the case of off-chain NFT, all or part of the data does not exist on the blockchain but is stored on an external storage. This external storage can be for example a centralized web server or a decentralized server such as IPFS (Inter Planetary File System) (see Cointelegraph, 2024). Off-chain NFTs basically use hyperlinks within the metadata referring to a file that visually represents the NFT and which is stored on external storage (Harmath & Breszkovics, 2022). Whether the NFT is on-chain or off-chain, the ability of the NFT as a virtual asset to authenticate rights or obligations, such as authenticating ownership on the blockchain, is the subject of another *ad hoc* test (Gebreab *et al*. 2022, p. 10).

3. THE NFT MARKET'S STATE

The trading volume of non-fungible tokens hit US$25.1 billion in 2021, although it fell slightly back to US$24.7 billion in 2022 (Hayward, 2023). The shades of the NFT market in 2021 and 2023 are represented by statistical reports by market research companies NonFungible.com and NFT18.com.

The comprehensive NFT market report, published by NonFungible in 2021 (NonFunglible, 2021), takes into account both primary and secondary market operations and analyses them together. According to the report, the market capitalisation of non-fungible tokens exceeded US$16 billion in 2021. Trading on the NFT market involved 1

million sellers and more than 2 million buyers. The number of active wallets with at least one transaction was estimated at 2.5 million. The average number of transactions per wallet was 1.8. The average NFT sales price was 807 US USD. The average number of days an NFT item was on hold in a wallet was 48 days.

According to the annual report by the NFT18, the market capitalisation of non-fungible tokens in 2023 was US$4.7 billion (NFT18, 2023). The annual trading on the NFT market had a minimum number of 100,000 sellers and buyers and a maximum number of 350,000 sellers and 450,000 buyers. The number of active wallets with at least one transaction was estimated at 2.03 million. The average NFT sales price was 665 USD. The volume of trading volume in USD in different NFT categories was dominated by collectable NFTs at 78%, followed by the art sector (12%), then metaverse worlds (5%), utility projects (4%) and finally the gaming sector (3%).

In addition to outlining the statistical data on the NFT market, here are two examples of high-value NFT transactions in 2021. Firstly, the first tweet was made by Jack Dorsey, co-founder and ex-CEO of Twitter, which was sold for USD 2.9 million (Locke, 2021). On the other hand, the NFT artwork "Everydays", Everydays: the First 5000 Days, sold by Christie's auction house for 69 million USD (Frank, 2021).

I consider that the reports on the two years of high and low numbers cited above provide a good reference point for the volatile nature of the NFT market, as well as an understanding of the awakening legislative interest.

4. THE CONCEPTUAL DEVELOPMENT OF SPECIFIC REGULATION OF CRYPTO-ASSETS IN THE EU

The aim of legal regulatory cover for the crypto-economic system in the European Union dates back to 2018 when the EU legislature examined the potential of FinTech solutions in the legal environment. Financial technology (FinTech) is an umbrella term that covers innovative digital technologies in financial services which have the capability to revolutionise financial services, financial markets and the functioning of financial institutions by developing new business models, applications, processes and products (Rácz, 2018, p. 340).

The wide definition of FinTech solutions also includes blockchain technology, which is the technology behind crypto-assets. Therefore, the Commission in its 2018 FinTech Action Plan (European Commission, 2018) called for a legal examination of the compatibility of the existing EU regulatory framework for ICOs and crypto-assets. The purpose of the assessment was to determine the need or inaction for regulatory intervention at the EU level. The outcome of the assessment was boosted by reports published in 2019 by both the European Securities and Markets Authority (ESMA) and the European Banking Authority (EBA). These reports explained the legal nature of crypto-assets under the existing EU financial legislation at the time.

4.1. Report from the European Securities and Markets Authority

The aforementioned ESMA report noted that crypto assets do not have a single legal definition in the EU capital market while referring to the definition of virtual currencies in the fifth Anti Money Laundering Directive (AMLD5). Due to the lack of a definition, ESMA indicated that it would examine the definition of transferable securities under the MiFID II regimes and the definition of electronic money under the Second Electronic Money Directive (EMD2). According to ESMA, particular crypto assets may fall under the MiFID II definition of a financial instrument (Bujtár, 2023, p. 30), but the classification of particular crypto assets as financial instruments will depend on the competent authority of the Member State and the implementation of EU legislation. Where a crypto asset is considered to be a financial instrument, the relevant EU legislation, in particular the Prospectus Directive, the Transparency Directive, MiFID II, MiFIR, CRD IV, MAR, SFD, CSDR, UCITS V, AIFMD, the Investor Compensation Schemes Directive (ICD), as well as the applicable rules of the AML/CFT, should be applied accordingly.

4.2. Report from the European Banking Authority

The EBA report states that there is no consistent view across the EU that recognises cryptocurrencies as legal tender (Szilovics, 2022a, p. 251) (i.e. fiat money). However, due to the wide range of crypto-assets that exist, certain crypto-assets with specific characteristics may qualify as electronic money under EMD2 or as scriptural money under Payments Services Directive 2 (PSD2), which also covers electronic money under EMD2. In this context, the EBA underlines that the classification of a crypto-asset should be done in a case-by-case manner taking into account that a crypto-asset may have different characteristics during its life cycle and thus the principle of substance over form should be followed. If the *ad hoc* test results in the classification of a certain crypto-asset as electronic money or money, then the relevant EU legislation should be applied, particularly the provisions on the prevention and combating of money laundering and terrorist financing.

Regarding the two reports, it is worth mentioning that both the ESMA and EBA reports made references to each other, they complemented each other, and their collective interpretation provided a comprehensive but also compact overview of the EU legislation at that time, which did not have specific provisions on crypto-assets. The reports are essentially based on the relevant EU legislation in force at that time, outlining the possible applications of the regulation, with a particular focus on capital market regulation and investor protection, while maintaining a transparent and sound market operation. At the same time, it became clear to the EU regulator that, although the *ad hoc* test may result in the application of legislation to certain crypto-assets, this only covers a narrow segment of crypto-assets. A significant part of the crypto market remains in the grey area of regulation. This recognition showed the need for specific regulation and provided inspiration for the MiCA.

5. THE SCOPE OF MiCA

In order to avoid regulatory overlaps and duplication of provisions, the MiCA leaves untouched and excludes from its scope those crypto-assets that qualify as financial instruments as defined in Directive 2014/65/EU and are subject to existing EU law. However, this does not apply to all crypto-assets as will be discussed below.

5.1. Broad and Narrow Definitions of Crypto-Assets in MiCA's Terminology

In MiCA's terminology crypto-assets is defined broadly as a digital representation of value or rights which may be transferred and stored electronically, using distributed ledger technology or similar technology. In a narrower sense, the regulation covers three types of crypto-assets by setting different requirements for each type depending on the level of risk they present. The classification is based on whether the crypto-asset is anchored to other assets or otherwise seeks to stabilise its value.

5.2. Specific Named Crypto-Assets

The first, named type of regulatory framework is the asset-referenced token — a type of crypto-asset that is not an electronic money token and that purports to maintain a stable value (Bujtár, 2022, p. 19) by referencing another value or right or a combination thereof, including one or more official currencies. The second is the so-called electronic money token or e-money token which is a type of crypto-asset that purports to maintain a stable value by referencing the value of one of the official currencies. The third is the utility token which is a type of crypto-asset that is only intended to provide access to a good or a service supplied by its issuer. Clearly, lawmakers intended to cover a wide range of crypto-assets when defining the different types of crypto-assets, thus making the legal provisions resilient to additional crypto-assets that may appear in the future.

6. THE SPECIAL STATUS OF NFTs IN THE MiCA'S REGULATORY FRAMEWORK

In MiCA's regulatory regime, the status of NFTs is specific. In general, the MiCA is not applicable to non-fungible tokens. This is expressly stated in its scope provisions and in certain points in the preamble. The preamble states, *inter alia*, that the MiCA does not apply to crypto-assets that are unique and not fungible with other crypto-assets, including digital art and collectables, and NFTs representing services or physical assets such as product guarantees or real estate. The reason for the exemption of non-fungible tokens from the MiCA is the limited financial use (Gáspár, 2022, p. 40) of NFTs and the related limited risk to the token holder and the financial system. Although the MiCA recognizes that NFTs might be traded on the marketplace and be accumulated speculatively. Nevertheless, it also states that NFTs have low liquidity, and relative value of one such crypto-asset in relation to another, each being unique, cannot be ascertained by means of comparison to an existing market or equivalent asset. Regarding the valuation

of NFTs, the MiCA does not specify a standard method to be followed in the market. The MiCA, however, provides an example of an indicator for determining the value of an NFT — the unique characteristics of certain token and their utility to the holder.

As a note here, the MiCA framework might not *expressis verbis* contain, but based on a logical interpretation of the legal text, it recognizes the category of uNFT (Breszkovics, 2022, p. 69). This can be explained by the fact that the MiCA identifies utility as a value-determining factor for NFTs, making a distinction between NFTs with and without utility. The scope of the regulation also excludes uNFTs.

However, in two instances, the MiCA departs from the main rule on the scope of the regulatory framework and provides for the application of its special rules to non-fungible tokens. It says that regulation should apply to crypto-assets that appear to be unique and non-fungible, but whose *de facto* features or whose features are linked to their *de facto* uses, would make them either fungible or not unique. In reality, this covers both fractionated and financial instrument NFT categories.

6. 1. Fractionalized Non-Fungible Tokens

The first type includes fractional parts of a unique and non-fungible crypto-asset or, in other words, fractionalized NFTs. These crypto assets should not be considered unique and non-fungible. In the approach of MiCA, the issuance of crypto-assets as NFTs in a large series or collection should be considered an indicator of their fungibility (Szívós, 2023, p. 80).

In the case of fractional NFTs in MiCA's framework, it is not sufficient for a crypto-asset to have a unique identifier in order to be considered unique and non-fungible. The assets or rights represented should also be unique and non-fungible in order for the crypto-asset to be considered unique and non-fungible. The examination and classification of fractionated NFTs is a task of the competent authorities, which need to follow a substance-over-form approach in the examination process. It is the features of the examined crypto-asset, rather than the issuer's designation that will determine its classification.

As a side note here, the MiCA application of fractional NFTs is interesting because it is not a new crypto-asset being issued, but a fractionation of an already existing "traditional" NFT. In the context of fractional NFT, there will be quasi-individual common ownership of a crypto-asset, where the ownership shares will be determined by the fraction of NFT held by the user.

6. 2. The Financial Instrument NFTs

The second category includes NFTs which are considered as financial instruments. This means that the uniqueness of a NFT is diminished and the financial use of the token is expanded, while the risk to the token holder and the financial system is increased. The financial instrument nature of a certain NFT is subject to *ad hoc* examination, but in the first line, it is the responsibility of the offerors or persons seeking admission to trading to correctly classify the crypto-asset. The classification may be challenged by competent authorities both before the date of publication of the offer and at any time thereafter. It

is relevant that in the *ad hoc* examination, the MiCA promotes discussions between the EBA, ESMA and European Insurance and Occupational Pensions Authority (EIOPA) to promote a common approach to the classification of crypto-assets (Szilovics, 2022a, p. 253). It is a safeguard provision that, where the classification of a crypto-asset appears to be inconsistent with the MiCA or other relevant Union legislative acts on financial services, the European Supervisory Authorities (ESAs) should make use of their powers under Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010 to ensure a consistent and coherent approach to such classification.

7. CLOSING THOUGHTS

In the introduction to this paper, the pre- and post-MiCA regulatory periods are not complementary but interdependent periods. In the regulatory framework, the definition of crypto-assets is flexible and future-proof, making it easy to adapt the rules to upcoming crypto-assets. MiCA recognises the specific nature of NFTs and as a general rule excludes them from the scope of the regulation. However, the MiCA does provide for the application of certain provisions to fractional and financial instrument NFTs. Among other relevant EU legislation affecting the crypto sector, the so-called DORA and the DLT Pilot Regulation do not contain express provisions on NFTs and neither does the EU Travel Rule regulation. However, they do have an impact on the NFT sector due to their indirect regulation of the crypto sector.

In conclusion, my view is that the MiCA and the other crypto-relevant EU legislation mentioned above are *de iure* capable of ensuring a properly regulated and transparent crypto sector where lay users and investors are well-informed and can operate safely. However, the *de facto* effect and effectiveness of crypto regulation will only be truly measured in a few years' time.

LIST OF REFERENCES

Literature

Breszkovics, B. 2022. NFTk-k jogi aspektusai. *Debrecen, Pro Futuro*, 12(2), pp. 69-70. https://doi.org/10.26521/profuturo/2022/2/12402

Bujtár, Z. 2021. *Az értékpapírosítás*. Pécs: Pécsi Tudományegyetem, Állam- és Jogtudományi Kar.

Bujtár, Z. 2022. A decentralizált pénzügyek (DeFi) árnyékbanki jellege. *JURA*, 28(4), pp. 18-20.

Bujtár, Z. 2023. Bankválság 2023-ban – megismétlődhet a 2007-2009-es nagy pénzügyi válság? In: Bujtár, Z. *et al.* (eds.), *A válságkezelés, gazdasági és jogi eszközei : Konferenciakötet – válogatott tanulmányok*. Pécs: Pécsi Tudományegyetem Állam- és Jogtudományi Kar, pp. 29-31.

Edelman, R. 2022: *The Truth About Crypto: A Practical, Easy to Understand Guide to Bitcoin, Blockchain, NFTs and Other Digital Assets*. New York: Simon & Schuster.

Kraizberg, E. 2023. Non-fungible tokens: a bubble or the end of an era of intellectual property rights. *Financial Innovation*, 9(32). https://doi.org/10.1186/s40854-022-00428-4

Gáspár, Z. 2022. Az el salvadori Bitcoin-törvény gazdasági és jogi aspektusai. In: Bujtár, Z. *et al.* (eds.), *Fenntartható növekedés (ESG) jogi és gazdasági aspektusai.* Pécs: Pécsi Tudományegyetem Állam- és Jogtudományi Kar, pp. 39-51.

Hokianto, H. F. 2023. Non-Fungible Tokens: A Literature Review. *SaNa: Journal of Blockchain, NFTs and Metaverse Technology*, 1(1), pp. 1-9. https://doi.org/10.58905/sana.v1i1.32

Király, P. B. 2020. A kriptovaluták pénzügyi fogyasztóvédelmi aspektusai. *Iustum Aequum Salutare*, 4, pp. 45-58.

Mezei, P. 2022. NFT-k a szerzői jog világában. *Iparjogvédelmi és Szerzői Jogi Szemle*, 127(3), pp. 7-23.

Rácz, D. 2018. Szabályozási kérdések a pénzügyi innováció területén. In: Fazekas, M. (ed.) *Jogi Tanulmányok. Jogtudományi Előadások az Eötvös Loránd Tudományegyetem Állam- és Jogtudományi Kar Doktori Iskoláinak Konferenciáján*. Budapest: ELTE Állam- és Jogtudományi Kar Állam- és Jogtudományi Doktori Iskola, pp. 342-254.

Peres, R. *et al.* 2023. Blockchain meets marketing: Opportunities, threats, and avenues for future research. *International Journal of Research in Marketing*, 40(1), pp. 1-11. https://doi.org/10.1016/j.ijresmar.2022.08.001

Gebreab, S. A. *et al.* 2022. NFT-Based Traceability and Ownership Management of Medical Devices. *IEEE Access PP,* 99(1), pp. 126394-126411. https://doi.org/10.1109/ACCESS.2022.3226128

Szilovics, C. 2022a. A kriptovaluták pénzfunkciójáról és gazdasági, társadalmi jelentőségéről. In: Bujtár, Z. *et al.* (eds.) *Kriptoeszközök világa a jog és a gazdaság szemszögéből : konferenciakötet : válogatott tanulmányok*. Pécs: Pécsi Tudományegyetem Állam- és Jogtudományi Kar, pp. 250-252.

Szívós, A. 2023. The Taxation of Cryptocurrency. In: Frankel, D. A. (eds.) *A Current Anthology of Law.* Athens: Athens Institute for Education and Research, pp. 79-83.

Laurence, T., & Kim, S. 2021. *NFTs for Dummies.* New Jersey: John Wiley & Sons Inc.

Legal sources

European Commission. 2018. FinTech Action Plan: For a more competitive and innovative European financial sector. COM(2018) 109 final. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018DC0109 (18. 5. 2024).

Directive 2011/61/EU of the European Parliament and of the Council of 8 June 2011 on Alternative Investment Fund Managers and amending Directives 2003/41/EC and 2009/65/EC and Regulations (EC) No 1060/2009 and (EU) No 1095/2010 Text with EEA relevance. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32011L0061 (18. 5. 2024).

Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing

Directives 2006/48/EC and 2006/49/EC Text with EEA relevance. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32013L0036 (18. 5. 2024).
Directive 2014/91/EU of the European Parliament and of the Council of 23 July 2014 amending Directive 2009/65/EC on the coordination of laws, regulations and administrative provisions relating to undertakings for collective investment in transferable securities (UCITS) as regards depositary functions, remuneration policies and sanctions Text with EEA relevance. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014L0091 (18. 5. 2024).
Directive 97/9/EC of the European Parliament and of the Council of 3 March 1997 on investor-compensation schemes. Available at: https://eur-lex.europa.eu/eli/dir/1997/9/oj (18. 5. 2024)
Proposal for a Regulation of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing. COM/2021/420 final. Available at: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A52021PC0420 (18. 5. 2024).
Regulation (EU) 2019/2088 of the European Parliament and of the Council of 27 November 2019 on sustainability-related disclosures in the financial services sector (Text with EEA relevance). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32019R2088 (18. 5. 2024).
DORA. Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (Text with EEA relevance). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2554 (18. 5. 2024).
Regulation (EU) 2022/858 of the European Parliament and of the Council of 30 May 2022 on a pilot regime for market infrastructures based on distributed ledger technology, and amending Regulations (EU) No 600/2014 and (EU) No 909/2014 and Directive 2014/65/EU (Text with EEA relevance). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R0858 (18. 5. 2024).
Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849 (Text with EEA relevance). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023R1113 (18. 5. 2024).
Regulation (EU) No 596/2014 of the European Parliament and of the Council of 16 April 2014 on market abuse (market abuse regulation) and repealing Directive 2003/6/EC of the European Parliament and of the Council and Commission Directives 2003/124/EC, 2003/125/EC and 2004/72/EC Text with EEA relevance. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014R0596 (18. 5. 2024).
Regulation (EU) No 600/2014 of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Regulation (EU) No 648/2012 Text with EEA relevance. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014R0600 (18. 5. 2024).

CSDR. Regulation (EU) No 909/2014 of the European Parliament and of the Council of 23 July 2014 on improving securities settlement in the European Union and on central securities depositories and amending Directives 98/26/EC and 2014/65/EU and Regulation (EU) No 236/2012 Text with EEA relevance. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014R0909 (18. 5. 2024).

Internet sources

Clifford chance. 2021. Non-fungible tokens: The global impact. Available at: https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2021/06/non-fungible-tokens-the-global-legal-impact.pdf (18. 5. 2024).

Cointelegraph. 2024. What is the InterPlanetary File System (IPFS), and how does it work? Available at: https://cointelegraph.com/learn/what-is-the-interplanetary-file-system-ipfs-how-does-it-work (18. 5. 2024).

NFT18. 2023. 2023 NFT annual report. Available at: https://nft18.com/reports/2023-nft-annual-report/ (18. 5. 2024).

enjin.io. ERC-1155. Available at: https://enjin.io/about/erc-1155 (18. 5. 2024).

erc721.org. ERC-721. Available at: https://erc721.org/ (18. 5. 2024).

European Banking Authority (EBA). 2019. Report with advice for the European Commission on crypto-assets. Available at: https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2545547/67493daa-85a8-4429-aa91-e9a5ed880684/EBA%20Report%20on%20crypto%20assets.pdf (18. 5. 2024).

European Council. 2022. Digital finance: agreement reached on European crypto-assets regulation (MiCA). Available at: https://www.consilium.europa.eu/en/press/press-releases/2022/06/30/digital-finance-agreement-reached-on-european-crypto-assets-regulation-mica/ (18. 5. 2024).

European Securities and Markets Authority (ESMA). 2019. Advice on Initial Coin Offerings and Crypto-Assets. ESMA50-157-1391. Available at: https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf (18. 5. 2024).

Frank, R. 2021. Beeple NFT becomes the most expensive ever sold at auction after fetching over $60 million. CNBC. Available at: https://www.cnbc.com/2021/03/11/most-expensive-nft-ever-sold-auctions-for-over-60-million.html (18. 5. 2024).

Harmath, D. & Breszkovics, B. Festmény a blokkláncon avagy, mi is az az NFT. https://kutatokejszakaja.pte.hu/programok/festmeny-a-blokklancon-avagy-mi-is-az-az-nft- (18. 5. 2024).

Harmath, D. Telegram chat messages. https://telegram.org/ (18. 5. 2024).

Hayward, A. 2023. NFT Sales in 2022 Nearly Matched the 2021 Boom, Despite Market Crash. Decrypt. Available at: https://decrypt.co/118438/2022-versus-2021-nft-sales (18. 5. 2024).

Learn. 2022. What are NFTs? Available at: https://opensea.io/learn/what-are-nfts (18. 5. 2024).

Non-fungible. 2021. Yearly NFT market report. Available at: https://nonfungible.com/reports/2021/en/yearly-nft-market-report (18. 5. 2024).

Locke, T. 2021. Jack Dorsey sells his first tweet ever as an NFT for over 2.9 million. CNBC. Available at: https://www.cnbc.com/2021/03/22/jack-dorsey-sells-his-first-tweet-ever-as-an-nft-for-over-2point9-million.html (18. 5. 2024).
Mazur, M. 2021. Non-Fungible Tokens (NFT). The Analysis of Risk and Return. IESEG School of Management. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3953535 (18. 5. 2024).

UDC: 323.266 DOI: 10.56461/iup_rlrc.2024.5.ch6

Fernanda F. FERNANDEZ JANKOV*
Law Faculty, University of São Paulo, Brazil
Fernandez & Jankov Legal Intelligence

TOWARDS A GLOBAL REGULATORY REGIME FOR TECH GIANTS

This paper offers tools for regulatory authorities to effectively address the spread of fake news by tech giants. Evaluating current frameworks, which often focus on symptom treatment like content removal and fact-checking, the study finds these methods insufficient for tackling the root causes of misinformation. Proposing a harm-based regulatory regime inspired by social medicine, political science, and legal theory, the paper emphasizes a holistic approach. Integrating insights from political science and revisiting the concept of regimes as global regulation, it provides a structured framework for regulatory authorities. This approach includes understanding socio-economic incentives, leveraging advanced technologies like AI, and promoting digital literacy. The study highlights the importance of principles, norms, rules, and decision-making processes to create a coherent regulatory environment adaptable to various socio-political contexts where interdisciplinary collaboration among governments, digital platforms, civil society, and international organizations is crucial. The proposed regime aims to foster a trustworthy information ecosystem, enhance societal trust, and mitigate the impact of fake news. By recognizing the complexity of fake news, this paper provides mechanisms for raising awareness among all actors involved and structuring their actions within such a legal framework. The ultimate aim is to establish a resilient and reliable digital public sphere, offering regulatory authorities a comprehensive strategy to combat digital misinformation effectively.

Keywords: tech giants regulatory regime, digital literacy, fake news, harm-based approach, trustworthy information ecosystem.

* PhD, post-doctorate programme, ORCID: 0009-0007-9737-4293, e-mail: *fernanda.jankov@usp.br*

1. INTRODUCTION

This paper offers tools for regulatory authorities to effectively address the spread of fake news by tech giants, providing insights on how to legally structure a regulatory regime using ideas from political science and legal theory.[1] In the digital age, the proliferation of fake news poses a significant challenge to the integrity of information disseminated online, particularly by tech giants. This paper examines the regulatory mechanisms aimed at holding these corporations accountable for the spread of misinformation, evaluating their effectiveness as deterrents. Current frameworks often focus on symptom treatment, such as content removal and fact-checking, rather than addressing the root causes and systemic issues that allow misinformation to thrive.

Drawing parallels between medical diagnosis and legal regulation, this study argues for a holistic and integrated approach to combating fake news. By incorporating insights from social medicine, political science, and legal theory, we propose a harm-based regulatory regime that addresses the multifaceted nature of the digital media landscape. This approach emphasizes the importance of understanding the socio-economic incentives and psychological factors that drive the production and dissemination of fake news, as well as the role of digital platforms in amplifying misleading content.

The paper advocates for the development of a comprehensive strategy that includes robust legal frameworks, educational initiatives, and technological solutions. Key to this strategy is the promotion of digital literacy programs to equip users with the skills needed to critically assess information. Additionally, leveraging advanced technologies such as artificial intelligence and machine learning can help detect and mitigate the spread of fake news.

By fostering a collaborative environment involving governments, private digital platforms, civil society, and international organizations, this paper aims to create a more resilient and trustworthy information ecosystem. The proposed regulatory regime emphasizes the importance of principles, norms, rules, and decision-making processes to create an environment for a coherent regime that is adaptable to various socio-political contexts. This interdisciplinary collaboration ensures that the regulatory measures are context-sensitive and effective.

Ultimately, the proposed regulatory regime seeks not only to hold tech giants accountable but also to restore societal trust in information and enhance the overall resilience of digital information ecosystems. By recognizing the complexity of fake news, this paper provides mechanisms for raising awareness among all actors involved and structuring their actions within such a legal framework. This study contributes to the ongoing discourse on effective legal strategies for combating digital misinformation, aiming to establish a resilient and reliable digital public sphere.

[1] Disclaimer: This paper does not aim to offer a complete Regulatory Regime for Tech Giants but rather to provide the foundational basis and legal structure from the perspective of legal thinking. It is intended to serve as a seed for debate and to enhance understanding of the complexity involved in addressing the regulation of Tech Giants. The ideas presented herein lay the groundwork for a broader research project that involves comparative law systems and interdisciplinary approaches. The purpose of this publication is to stimulate scholarly discussion and contribute to the ongoing discourse on this critical issue.

2. UNDERSTANDING FAKE NEWS AND ITS IMPACT

2.1. Defining Fake News

Fake news refers to misinformation or disinformation that is intentionally spread to deceive the public. According to Abiri & Buchheim (2022), fake news is not merely false information but a deliberate distortion intended to manipulate public perception. This understanding highlights the intentional aspect of fake news, distinguishing it from mere errors or inaccuracies in reporting. It is this deliberate intent to mislead that separates fake news from other forms of incorrect information.

Such manipulation is facilitated by the digital environment, which allows for rapid dissemination and amplification of misleading content. Moreover, as Abiri & Buchheim (2022) point out fake news exploits the digital epistemic divide, where different segments of the population have varying access to and trust in information sources. This divide is exacerbated by algorithmic filtering, which creates echo chambers and reinforces pre-existing beliefs. This scenario contributes to the challenge of distinguishing between credible and non-credible sources, further complicating the fight against fake news.

The aspect of what it serves is addressed in the definition offered by Humprecht (2018, p. 3) where fake news refers to "online publications of intentionally or knowingly false statements of facts that are produced to serve strategical purposes and are disseminated for social influence or profit." In this sense, the examination of the characteristics of fake news leads to the assertion that it is often produced and disseminated for strategic purposes, either ideological or commercial aiming to change recipients' perceptions of certain issues and, in the long run, influence their opinions or behaviour.

Humprecht (2018, p. 3) categorizes fake news into several types, including satire, parody, fabrication, manipulation, propaganda, and rumours or hoaxes. Satire and parody involve humour or exaggeration to critique or mock real events, which can sometimes be mistaken for factual news. Fabrication refers to completely false information created to deceive readers, while manipulation involves distorting or altering facts to mislead. Propaganda is biased or misleading information used to promote a political cause or point of view. Rumours and hoaxes are unverified pieces of information that spread rapidly, often causing public alarm or outrage. Based on Calil (2022) expands on these categories by discussing the role of public agents in social media regulation, arguably highlighting that fake news can also include misleading political statements and false narratives spread by political actors to manipulate public perception.

Approaching fake news from this perspective reveals that the issue extends beyond a simple dichotomy of true versus false information. Fake news is intricately linked to the concept of legitimacy, as it undermines the authority and credibility of "central" institutions, both political and scientific. This paper introduces the term "fake legitimacy" to describe the type of legitimacy that arises from such manipulation. Unlike genuine legitimacy, which is grounded in truth and authenticity,[2] 'fake legitimacy' stems from

[2] In the pre-digital era, information dissemination was primarily based on a broadcasting model, where information was distributed from a single source to a broad audience. This model was subject to higher levels of accountability as broadcasters were regulated by stringent legal and ethical standards, ensuring

misinformation and deception, creating a perception that does not align with reality. The creation of this "fake legitimacy"[3] prevents the establishment of a trustworthy information ecosystem and further erodes societal trust, which is essential for democratic governance.

2.2. Why Fake News Exists as a Disease and Its Symptoms

In examining fake news through the lens of a disease and its symptoms, this study aims to leverage interdisciplinary insights, particularly those proposed by Stephenson & Rinceanu (2023). Their work explores the historical and ongoing synergy between law and medicine, advocating for an integrated approach to internet regulation. Drawing on the ideas of legal realists like Oliver Wendell Holmes Jr. and Benjamin Cardozo, they argue that effective solutions to global internet regulation require the combined efforts of medical and legal professionals to address online social problems. This interdisciplinary approach is essential for understanding the epistemic changes brought about by digital media and for developing effective regulatory frameworks. The European Union's "notice-and-takedown" model and North America's "market self-regulation" model, for instance, represent different approaches to regulating online communications, highlighting the profound disagreements on free speech's role in democratic governance (Stephenson & Rinceanu, 2023).

By conceptualizing fake news as a disease, this paper emphasizes the need to diagnose and address the root causes of the digital epistemic divide rather than merely treating the symptoms of misinformation. This involves adopting sophisticated harm-based approaches that rebuild trust in epistemic institutions, integrate free speech theories, and leverage interdisciplinary insights from both law and medicine to create effective regulatory frameworks. By fostering transparency, accountability, and inclusive dialogue, these solutions aim to restore the common factual ground necessary for democratic legitimacy and social cooperation. This holistic approach not only addresses the immediate impacts of fake news but also seeks to understand and mitigate the underlying conditions that allow such misinformation to proliferate.

The drivers of fake news production and diffusion are multifaceted. At the individual level, according to Humprecht (2018, p. 3), psychological effects such as confirmation bias and motivated reasoning lead people to believe information that confirms their existing beliefs. This new environment is marked by a shift from an offline ‘broadcasting' to an online ‘participatory' communication model and, second, the rise of dominant, privately owned digital intermediaries, the so-called ‘Big Five’ (namely, Alphabet/formerly Google, Meta/formerly Facebook, Microsoft, Amazon, Apple).[4] Humprecht' s

---

the accuracy and reliability of the information provided. The shift to a participatory model in the digital age, where anyone can create and share content, has significantly reduced these accountability mechanisms, facilitating the spread of misinformation and the rise of 'fake legitimacy.'

[3] The term 'fake legitimacy' has been introduced in this paper as part of a broader research project. This project aims to further explore how the concept of legitimacy has evolved in the digital era, particularly in the context of misinformation and the influence of digital platforms.

[4] Max Planck Institute for the Study of Crime, Security and Law. 2024. *Rethinking Digital Media Regulation*. Available at: https://csl.mpg.de/en/projects/rethinking-digital-media-regulation?c=178896 (27. 6. 2024).

(2018, p. 3) research highlights that social media is often used for its entertainment value, which contributes to the uncritical dissemination of misleading information. Moreover, people tend to trust information from sources that align with their pre-existing beliefs, further fuelling the spread of fake news.

At the societal level, still follow the same study. Humprecht (2018, p. 10), factors such as media trust, political polarization, and the strength of public service broadcasting (PSB) significantly influence the prevalence and impact of fake news leading to the ascertainment that countries with strong PSB and higher levels of trust in government and professional news media tend to have lower levels of partisan disinformation. Conversely, countries with lower media trust and higher political polarization, such as the United States and the United Kingdom, experience higher levels of partisan fake news. This relationship underscores the role of institutional trust and the media environment in either mitigating or exacerbating the spread of fake news.

Another contributing factor is the media ecosystem as Abiri & Buchheim (2022, p. 45) add. A fragmented media landscape with varying journalistic standards enables the proliferation of fake news. Social media platforms, in particular, play a crucial role in spreading false information. These platforms often lack the rigorous editorial oversight found in traditional news organizations, allowing misinformation to circulate widely and quickly. The ease with which content can be shared and the algorithms that prioritize engaging (often sensational) content further exacerbates the issue (Caled & Silva, 2022).

Economic incentives also drive the spread of fake news. Fake news can be economically profitable, as sensational stories attract clicks and generate ad revenue. This financial motivation incentivizes the creation and dissemination of false content. Entities that produce fake news often prioritize virality over accuracy, exploiting the economic benefits of high engagement rates (Stephenson & Rinceanu, 2023, p. 79).

Political polarization, a fragmented media ecosystem, and economic incentives, collectively contribute to the resilience and spread of fake news. By understanding these underlying causes, it becomes evident why fake news exists as a persistent "disease" in the information landscape, creating an environment where misinformation can thrive, and challenging efforts to maintain an informed and cohesive society. This understanding is essential for this study as it aims at setting the core basis of a Regulatory Regime of Tech Giants which must address these specific issues if it is to be effective.

As for the symptoms of fake news, they manifest in various detrimental ways, extending far beyond the mere dissemination of false information as it erodes trust in traditional media and democratic institutions, contributes to societal polarization, and undermines the shared factual basis necessary for effective public discourse and policymaking, essential elements of legitimacy as relevant studies demonstrate. In this sense, the main issue with fake news lies not just in its inaccuracy but in its potential to fragment societies into separate epistemic communities, each with its own set of "facts". This fragmentation poses a significant threat to social cohesion and democratic governance, as it undermines the ability of societies to engage in informed and constructive dialogue (Abiri & Buchheim, 2022, p. 54).

Moreover, as Calil (2022, p. 176) outlines, fake news has a profound impact on public discourse and democratic processes. It can significantly influence public opinion

and electoral outcomes by presenting misleading information about candidates or policies. This misinformation can sway voter perceptions and decisions, potentially altering the course of democratic processes. By distorting the truth, fake news undermines the integrity of elections and the democratic ideals of informed decision-making and accountability.

Addressing these symptoms is the central concern of this research, as societal coherence demands the legitimacy of its governing institutions, both political and scientific. The scientific legitimacy is arguably even more crucial, as such knowledge should guide best political practices. When scientific facts are disputed or misrepresented, it becomes exceedingly difficult to formulate policies based on sound evidence, further eroding public trust and effective governance.

3. FAKE NEWS: REGULATORY FRAMEWORK SCHEMES

3.1. Germany / Europe

Internet regulation in Europe is predominantly guided by a "notice-and-takedown" approach, prominently represented by Germany's Network Enforcement Act (*Netzwerkdurchsetzungsgesetz* – NetzDG)[5] and a 'notice-and-action' approach found in the EU's Digital Services Act (DSA).[6]

Germany's NetzDG, effective from October 1, 2017, epitomizes the world's principal Internet regulatory model. It aims to enhance digital intermediaries' efforts to address problematic online content by mandating a regulatory framework with severe penalties for non-compliance. NetzDG has sparked controversy and concern over its impact on freedom of speech and fundamental rights both within Germany and internationally (Stephenson & Rinceanu). NetzDG employs a "notice-and-takedown" approach that requires extensive public and private cooperation. Digital media platforms must delete or block illegal content within specified timeframes, ranging from 24 hours to seven days.[7] Illegal content is defined by various infractions in Germany's Criminal Code, including offences such as insult and public order disturbances.[8] Platforms are obligated to inform complainants

---

[5] Act to Improve Enforcement of the Law in Social Networks *(Netzwerkdurchsetzungsgesetz* - NetzDG*), Federal Law Gazette* I at 3352, enacted 1 October 2017.

[6] European Union**,** Regulation (EU) 2022/2065 on a Single Market for Digital Services (Digital Services Act - DSA) and amending Directive 2000/31/EC, [2022] OJ L277/1, entered into force on 16 November 2022.

[7] § 3(2)(2): "Social networks must delete or block access to manifestly unlawful content within 24 hours of receiving a complaint." § 3(2)(3): "For all other unlawful content, the deadline for deletion or blocking access is seven days after receiving the complaint."

[8] Criminal Code *(Strafgesetzbuch* - StGB*)*, last amended by Article 1 of the Law of 28 March 2023, *Federal Law Gazette* I p. 368. § 185 StGB - Insult (*Beleidigung*); § 186 StGB - Defamation (*Üble Nachrede*); § 187 StGB - Malicious Gossip (*Verleumdung*); § 130 StGB - Incitement to Hatred (*Volksverhetzung*); § 201 StGB - Violation of the Privacy of the Spoken Word (*Verletzung der Vertraulichkeit des Wortes*); § 201a StGB - Violation of Privacy through Taking Unauthorized Photographs (*Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen*);§ 202a StGB - Data Espionage (*Ausspähen von Daten*); § 202b StGB - Phishing/Interception of Data (*Abfangen von Daten*); § 202c StGB - Preparation of Unauthorized Data Access (*Vorbereiten des Ausspähens und Abfangens von Daten*); § 241 StGB - Threat (*Bedrohung*), among others.

of their decisions and any rights of appeal[9] and report their content moderation activities publicly.[10] Additionally, platforms must report potentially criminal content, including IP addresses, to Germany's Federal Criminal Police Office (*Bundeskriminalamt*), notifying users no earlier than 4 (four) weeks after this transmission.[11] Non-compliance can result in fines of up to €50 (fifty) million for corporations and €5 (five) million for corporate officials.[12] The popularity of Germany's regulatory approach is evident, with over 25 countries and the EU adopting or proposing legislation influenced by NetzDG.[13]

The EU's Digital Services Act (DSA) based on a 'notice-and-action' model/approach is a significant testament to the influence of Germany's NetzDG. Enacted to shape Europe's digital future, the DSA aims to create a safe, predictable, and trustworthy online environment by countering harmful content such as hate speech, disinformation, and other objectionable content, while upholding fundamental rights.

Directly applicable to all 27 EU Member States, the DSA places primary responsibility on EU-based private digital intermediaries for handling illegal online content. Similar to NetzDG's "notice-and-takedown" model, the DSA introduces a "notice-and-action" mechanism, requiring digital platforms to provide an accessible procedure for users to report illegal content. The DSA defines "illegal content" broadly in Art. 3(h) as any information not compliant with Union law or the law of any Member State compliant with Union law.[14] This definition is broader than the German counterpart, which covers only violations of designated criminal provisions, as previously mentioned.

Complaints about illegal content can be submitted by individuals or entities, and platforms must respond in a timely, diligent, non-arbitrary, and objective manner, notifying complainants of decisions and legal remedies.[15] Notices from "trusted flaggers" receive priority and expedited processing; "trusted flagger" status is granted to entities with expertise in handling illegal content, such as Europol and the INHOPE Association.[16] Additionally, Art. 9 of the DSA requires platforms to comply with EU Member State orders to act against specific illegal content.

The DSA differs from NetzDG in several key ways. First, it does not prescribe specific timeframes for content removal, allowing platforms flexibility to make timely decisions and exempting them from liability if they act diligently.[17] Platforms must explain to users any restrictions imposed and their legal or contractual basis, with options for users to appeal through internal mechanisms, out-of-court settlements, or judicial redress.[18] Second, unlike

[9] § 3(2) of the NetzDG

[10] § 3(5) of the NetzDG

[11] § 3a NetzDG

[12] § 4 NetzDG

[13] *Search results: NETZGD.* Available at: https://justitia-int.org/?s=NetzDG (10. 10. 2024).

[14] Art. 3(h) DSA.

[15] Arts. 16, 17, 18 DSA.

[16] Art 22 DSA.

[17] Art 14 DSA.

[18] Art 20 DSA.

NetzDG's strict requirements, the DSA mandates that platforms notify authorities only when they suspect a criminal offence involving a threat to life or personal safety.[19] Third, the DSA does not require platforms to continuously monitor website traffic for illegal content.[20]

In conclusion, the intent behind the Digital Services Act (DSA) is indeed to create a cohesive regulatory framework across the European Union, addressing illegal content and establishing clear rules for digital platforms. This framework aims to replace or supersede fragmented national regulations, such as Germany's Netzwerkdurchsetzungsgesetz (NetzDG), thereby achieving consistency and uniformity within the EU's single market.[21]

It is crucial to observe, that the European Union's Digital Services Act (DSA) has attracted criticism for its potential to lead to over-censorship and for perceived gaps in its enforcement mechanisms. While the Act aims to tackle disinformation and illegal content, critics worry that granting the European Commission direct intervention powers during crises could prompt hasty or excessive content removal, affecting lawful expressions, such as satire and political critique. This concern is amplified by recent proposals that would allow the Commission to unilaterally declare a crisis and dictate platforms' responses, which could undermine the careful balance initially sought by lawmakers to protect free expression while combating disinformation.[22]

Furthermore, the DSA's transparency provisions, though beneficial for accountability, include exceptions that could allow platforms to withhold information deemed sensitive, potentially limiting the Act's effectiveness. Critics also highlight that while the DSA permits vetted researchers access to data for compliance assessments, trade secret protections might restrict meaningful analysis, weakening external oversight. Additionally, the DSA's "light-touch" approach to disinformation allows platforms significant discretion over "lawful but awful" content, leading to concerns about inconsistent moderation practices and the Act's overall ability to manage disinformation at scale effectively.[23]

3.2. United States of America

The United States employs a "market self-regulation" model, arguably symbolizing deep disagreement on the constitutional role of freedom of expression in democratic nations. The primary regulatory framework in Section 230 of the Communications

[19] Art. 21 DSA.

[20] Art. 7 DSA.

[21] European Parliament and Council Regulation (EU) 2022/2065 of 19 October 2022 on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC [2022] OJ L277/1, recitals 9, 10 and 14.

[22] Meyers, Z. 2022. *Will the Digital Services Act save Europe from disinformation?* Centre for European Reform. Available at: https://www.cer.eu/insights/will-digital-services-act-save-europe-disinformation (9. 10. 2024); Buri, I. & van Hoboken, I. 2021. *The DSA proposal: a critical overview*. Institute for Information Law, DSA Observatory. Available at: https://dsa-observatory.eu/wp-content/uploads/2021/11/Buri-Van-Hoboken-DSA-discussion-paper-Version-28_10_21.pdf (10. 10. 2024).

[23] Amnesty International. 2022. *What the Digital Services Act means for human rights and harmful Big Tech business models. Amnesty International EU Office*. Available at: https://www.amnesty.org/en/documents/pol30/5830/2022/en/ (10. 10. 2024); Buri, I. & van Hoboken, I. 2021. *The DSA proposal: a critical overview*. Institute for Information Law, DSA Observatory. Available at: https://dsa-observatory.eu/wp-content/uploads/2021/11/Buri-Van-Hoboken-DSA-discussion-paper-Version-28_10_21.pdf (10. 10. 2024).

Decency Act (CDA)[24], which protects digital platforms from civil liability for offensive speech acts.[25] Courts have interpreted this broadly to protect against claims based on third-party content, including negligence, deceptive trade practices, unfair competition, and more.[26] This broad safe harbour is considered essential for a functioning Internet. This provision has been broadly interpreted by courts to shield digital platforms from liability for content created by users. This includes protection from claims of negligence, deceptive trade practices, unfair competition, and more. The broad safe harbour provision is considered essential for maintaining a functional Internet, as it allows platforms to host user-generated content without fear of constant litigation.[27]

It is relevant to mention the current state of Litigation and Legislative Responses as numerous issues related to content moderation and free speech are currently being litigated before the US Supreme Court in cases such as Moody v. NetChoice, LLC.[28] Over 100 bills have been proposed in state legislatures to regulate social media platforms' content moderation policies. For instance, Florida's Senate Bill 7072[29] sought to regulate social media platforms by requiring transparency in censorship decisions and consistent application of standards. However, the Eleventh Circuit Court of Appeals declared it unconstitutional, raising critical questions about the nature of digital platforms' roles as "speech" or "editorial discretion" and whether they can be regulated as "common carriers"[30].

In summary, Section 230 provides significant protection for digital platforms, including from liability for hosting offensive speech, such as hate speech, aligning with First Amendment principles.[31] Although such content is protected by free speech laws, platforms address it by setting their content policies or updating their Terms of Use to balance user expression with community standards. The shift from a traditional "broadcasting" model to an interactive "participatory" model has positioned these platforms as new gatekeepers. This role raises tensions between their profit-driven business models and their responsibilities to uphold human rights, such as freedom of expression, privacy, and protection from harm

---

[24] United States, Communications Decency Act, 47 U.S.C. § 230 (1996).

[25] Section 230 The text of Section 230(c)(1) states: "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."

[26] Cases on the broad interpretation of Section 230: *Zeran* v. *America Online, Inc*., 129 F.3d 327 (4th Cir. 1997); *Fair Housing Council of San Fernando Valley* v. *Roommates.com,* LLC, 521 F.3d 1157 (9th Cir. 2008); *Jones* v. *Dirty World Entertainmen*t *Recordings* LLC, 755 F.3d 398 (6th Cir. 2014); *Doe* v. *MySpace, Inc*., 528 F.3d 413 (5th Cir. 2008); *Force* v. *Facebook, Inc*., 934 F.3d 53 (2d Cir. 2019).

[27] Importance of safe harbour for a functioning Internet see further: Vogus, C. 2021. *Answers to Five Key Questions from House Energy & Commerce Section 230 Hearing.* Center for Democracy and Technology. Available at: https://cdt.org/insights/answers-to-five-key-questions-from-house-energy-commerce-section-230-hearing/ (10. 10. 2024).

[28] *Moody v. NetChoice*, LLC, 603 U.S. (2024)

[29] Florida Senate Bill 7072, 2021; *Governor Ron DeSantis Signs Bill to Stop the Censorship of Floridians by Big Tech.* 2021. Available at: https://www.flgov.com/2021/05/24/governor-ron-desantis-signs-bill-to-stop-the-censorship-of-floridians-by-big-tech/ (10. 10. 2024).

[30] *NetChoice, LLC, et al.* v. *Attorney General, State of Florida, et al.*, No. 21-12355 (11th Cir. 2022).

[31] United States Constitution, Amendment I.

Digital platforms thus navigate a complex landscape where they must reconcile their commitment to free speech with pressures to moderate content. Their policies and practices influence public discourse, raising questions about transparency, accountability, and the balance between enabling open dialogue and restricting harmful content. This delicate position often places platforms at the centre of debates about the limits of Section 230 and the role of private entities in regulating speech in digital spaces.

3.3. Canada

Canada has adopted a distinctive 'hybrid' model of online governance, reflected in its proposed Bill C-63,[32] which pivots from traditional "notice-and-takedown" systems to a more nuanced "systems-based" regulatory approach. This approach emphasizes collaboration among various stakeholders and aims to address the complexities of modern digital communications.[33]

Therefore, Canada's new regulatory proposal, embodied in Bill C-63, marks a shift from conventional content removal strategies to a systems-based risk assessment model. This model mandates a "duty to act responsibly" for digital platforms, focusing on transparency and systemic decision-making processes upstream of conventional content review mechanisms.[34]

Bill C-63 emphasizes proactive risk management, requiring digital platforms to implement measures to mitigate harmful content before it escalates.[35] The Canadian government engaged in extensive public consultations to inform this regulatory framework. Input from citizens and experts highlighted concerns about potential overreach and privatized censorship, emphasizing the need for precise definitions of harmful content, caution against proactive monitoring, and transparency in enforcement actions.[36]

A significant aspect of the Canadian model is its attempt to balance regulatory actions with the protection of free expression. Expert consultations underscored the importance of not incentivizing general monitoring, which could lead to over-censorship and infringe on free speech rights.[37] Canada's approach involves a diverse array of stakeholders, including public and private entities, fostering a more holistic regulatory environment. This multi-stakeholder approach integrates socio-technical-legal elements into the regulatory framework, ensuring a broader perspective on digital governance.[38]

Drawing insights from fields such as medical diagnostics and social medicine, Canada's model incorporates systemic causation and contextual regulatory measures, enhancing the effectiveness and adaptability of online governance strategies. This

---

[32] Online Harms Act, Bill C-63, 1st Sess, 44th Parl, 2024.

[33] Rinceanu, J. & Stephenson, R. 2024. *Differential Diagnosis in Online Regulation.* Eucrim. Available at: https://eucrim.eu/articles/differential-diagnosis-in-online-regulation/ (10. 10. 2024).

[34] *Online Harms Act, Bill C-63*, 1st Sess, 44th Parl, 2024, s. 3.

[35] s. 5.

[36] s. 7.

[37] s. 11.

[38] s. 15.

interdisciplinary approach aims to create a resilient and adaptable framework capable of addressing the evolving challenges in the digital landscape.[39]

In conclusion, the Canadian regulatory model exemplified by Bill C-63, the Online Harms Act, underscores a balanced and adaptive approach to online safety. Through extensive public and expert consultations, the government integrated diverse perspectives to address systemic factors and emphasize transparency in regulatory practices.[40] By moving beyond conventional content removal, this systems-based framework imposes a "duty to act responsibly" on digital platforms, promoting proactive risk management. The approach mitigates risks such as overreach and privatized censorship, ensuring accountability while preserving free expression. This robust framework not only strengthens the regulatory landscape but also adapts to the evolving challenges of online harms in a way that aligns with democratic values and public expectations.[41]

4. A HOLISTIC AND INTEGRATED APPROACH TO THE REGULATORY REGIME OF TECH GIANTS

4.1. The Need for a Global Regime

The regulation of fake news, hate speech, and other harmful online content varies substantially across regions, resulting in a fragmented and often ineffective global landscape, as previously described. These regulatory approaches differ so drastically that achieving a unified global framework appears nearly impossible, compounded by the unique limitations and challenges each system faces.

Firstly, they often treat issues like fake news and hate speech as isolated problems, leading to fragmented and ineffective regulations. For instance, the EU Digital Services Act tends to address these issues separately, failing to consider the interconnected nature of the digital media landscape.

Secondly, the varying regulations adopted by different countries can lead to unintended consequences, such as censorship or the spread of propaganda, due to a lack of contextual adaptation. The differing approaches between Europe and the USA highlight this issue, resulting in inconsistencies in enforcement and effectiveness. The lack of a unified global approach complicates the enforcement of consistent anti-misinformation measures, creating a fragmented regulatory environment (Abiri & Buchheim, 2022).

Thirdly, these regulatory approaches are primarily reactive, dealing with fake news after it has already been disseminated. Despite extensive fact-checking efforts during the USA 2020 elections and the COVID-19 pandemic, misinformation continued to significantly influence public perception (Humprecht, 2018).

[39] s. 20.

[40] Government of Canada. 2021. *Have your say: The Government's proposed approach to address harmful content online*. Available at: https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content.html (10. 10. 2024).

[41] For further details on this framework and its impact on digital platforms, refer to: Salloum, J. *et al*. 2024. *Canada's new Online Harms Act (C-63): what you need to know.* Osler. Available at: https://www.osler.com/en/insights/updates/canada-s-new-online-harms-act-c-63-what-you-need-to-know/?pdf=1 (10. 10. 2024).

Fourthly, aggressive content moderation raises concerns about censorship and the suppression of free speech. Efforts to curb misinformation must be carefully balanced to avoid infringing on individual rights to freedom of expression. Overzealous content removal can stifle legitimate discourse and contribute to perceptions of bias and unfairness, further eroding public trust in digital platforms (Calil, 2022). Variations in human rights protections and constitutional structures pose significant challenges, particularly in the context of filtering and blocking online speech. Effective regulation requires a nuanced understanding of political and constitutional contexts (Humprecht, 2018).

Fifthly, the immense power of private digital platforms, which own and control much of the Internet's infrastructure, facilitates privatized government censorship. This, combined with economic incentives, threatens the quality and quantity of public discourse. The economic interests of these platforms often conflict with the public's need for reliable information, leading to a privatized form of censorship that undermines democratic processes (Calil, 2022).

Sixthly, addressing the root causes of misinformation requires regulatory frameworks that consider the underlying economic incentives and the role of algorithmic amplification by digital platforms (Abiri & Buchheim, 2022). These economic incentives drive the spread of fake news, making it profitable to create and disseminate sensational stories that attract clicks and generate ad revenue.

Finally, the analysis of existing regulatory frameworks reveals significant deficiencies in addressing the complexities of the digital media landscape. The pervasive issue of digital fake news poses a substantial threat to democracies, public health, and even the future of our planet. Despite efforts such as fact-checking and content removal during the USA 2020 elections and the COVID-19 pandemic, a significant portion of the population continues to believe in misinformation. This indicates that truth-based solutions like fact-checking do not fully address the problem. To effectively combat misinformation and protect democratic integrity, there is a critical need for a unified global regulatory regime. This regime should be based on comprehensive principles, norms, and rules that are adaptable to various socio-political contexts, ensuring consistent enforcement and effectiveness across different regions. It should integrate proactive strategies, technological solutions, and interdisciplinary approaches to create a balanced and effective regulatory framework. Only through such a holistic and integrated approach can we hope to address the root causes of misinformation and foster a healthier digital public sphere.

4.2. Regulatory Regime Basis and Structure

The regulation of fake news, hate speech, and other harmful online content can benefit from methodologies inspired by social medicine and comparative law. Drawing parallels between medical diagnosis (as it was previously suggested in Section 2.2) and legal regulation, we argue for a more holistic and integrated approach. This approach acknowledges the multifaceted nature of the digital media landscape and incorporates various stakeholders to create a comprehensive strategy (Flew, Martin & Suzor, 2019).

Historically, the perspective of Rudolf Virchow, a 19th-century physician, underscores the importance of considering social determinants in addressing health issues. Virchow advocated that political actions are necessary to address societal health problems, an approach that can be analogously applied to digital misinformation, where societal factors play a crucial role (Taylor & Rieger, 1985). Similarly, George Engel's biopsychosocial model from the 1960s integrates biological, psychological, and social factors in understanding health and illness. This model emphasizes the interconnected nature of these factors, relevant to the digital domain where technological, psychological, and social elements are deeply intertwined (Engel, 1977; Stephenson & Rinceanu, 2023, p. 75).

Comparative legal methodology, particularly functionalism, offers valuable insights into regulatory frameworks. This method aims to uncover broader socio-political connections underlying legal doctrines by gathering and interpreting information about various legal systems, evaluating similarities and differences between domestic legal regimes, and developing hypotheses to address shared regulatory challenges (Zweigert & Kötz, 1998). Such an approach ensures that regulatory measures are context-sensitive and adaptable to different socio-political landscapes.

Using this interdisciplinary methodological approach within a comparative legal framework, we propose a rational reconstruction of the regulatory regime for tech giants. When John Ruggie introduced the concept of international regimes into the international politics literature in 1975, he defined a regime as: "a set of mutual expectations, rules and regulations, plans, organizational energies and financial commitments, which have been accepted by a group of states" (Ruggie, 1975, p. 570).

Later, Krasner (1983, p. 2) elaborated on this definition, describing international regimes as: "sets of implicit or explicit principles, norms, rules and decision-making procedures around which actors' expectations converge in a given area of international relations" (Krasner, 1983, p. 2). Principles are beliefs about a fact, cause, or reaction. Norms are standards of behaviour defined in terms of rights and obligations. Rules are specific prescriptions and prospects for action. Decision-making processes establish actions that tend to prevail, practices for making and implementing collective choices.

"The principles of the regime generally define the objectives expected to be pursued by its members." (Krasner, 1983, p. 4). For example, the norms of the Paris Agreement (2015) do not require its members to immediately achieve all climate goals but incorporate prescriptions for members to practice transparency and accountability, aiming to lead them towards gradual and sustained climate action." For a regulatory regime addressing fake news and harmful content, principles would involve commitments to transparency, accountability, and the protection of human rights. These principles should harmonize the need for free expression with the imperative to prevent harm caused by misinformation.

Ronald Dworkin's theory (Dworkin, 1977) emphasizes the importance of principles over mere rules. The author argues that the community's political practices should express principles that go beyond simple rules. He distinguishes between three models of political association: the associative model, the rules model, and the principles model (Dworkin, 1977). The principles model is particularly relevant as it insists that members of a political community are genuinely linked by common principles, not just by rules

created through political agreements. This model satisfies the conditions of a pluralistic society by ensuring that citizens respect the principles of their particular community, even if these differ from those of other communities.

Norms, in the context of Dworkin's framework, serve as a bridge between principles and rules. They are standards of behaviour that carry the weight of principles but provide more specific guidance similar to rules. In the regulatory regime for tech giants, norms would include standards for content moderation, such as the duty to remove or flag misinformation and the obligation to ensure that such actions do not unjustly infringe on freedom of expression. These norms must be adaptable to various socio-political contexts, allowing for effective implementation across different legal landscapes (Humprecht, 2018, p. 10). Dworkin's distinction between principles, norms, and rules highlights that norms carry weight and importance, providing the flexibility needed to adapt to specific contexts while being grounded in overarching principles of justice and equity. Norms in this regulatory regime ensure that the actions of tech giants align with the broader principles of the regime, providing a balanced approach to regulation. Arguably allowing the international community to enshrine the set principles on legal agreements serving as a basis for the rules to be developed in domestic regulation schemes.

Rules are more specific than norms, detailing the rights and obligations of regime members. For tech giants, rules would specify procedures for content removal, the steps required to verify the authenticity of content, and the obligations to provide users with mechanisms to appeal content moderation decisions. Rules should also encompass requirements for transparency reports and data sharing with regulatory bodies to enhance accountability (Abiri & Buchheim, 2022, p. 110).

Dworkin argues that the application of rules requires discretion and judgment, especially in "hard cases" where rules may conflict or be insufficient (Dworkin, 1977). In such instances, judges and regulators must resort to principles to guide their decisions, ensuring that the outcomes align with the broader principles of justice and equity.

As for the decision-making processes in this regulatory regime should promote the implementation of principles, norms, and rules through collaborative and interdisciplinary approaches. This includes engaging stakeholders from governments, private digital platforms, civil society, and international organizations. Educational initiatives are essential, promoting digital literacy to help users critically assess information (Caled & Silva, 2022, p. 135). Leveraging advanced technologies such as artificial intelligence and machine learning can enhance the detection and mitigation of fake news, making content moderation more effective (Stephenson & Rinceanu, 2023, p. 79).

Effective regulation must also consider the unique political, cultural, and legal contexts of different regions. Disinformation strategies vary significantly across countries, influenced by national news agendas and political cultures, necessitating tailored regulatory approaches (Humprecht, 2018, p. 85).

As a result of the suggested interdisciplinarity approach it is feasible to incorporate proactive strategies that are necessary to prevent the spread of misinformation. This includes real-time monitoring and early intervention mechanisms to address fake news before it gains traction. Addressing the root causes of misinformation, such as economic

incentives and algorithmic amplification, is vital for a sustainable solution (Abiri & Buchheim, 2022, p. 95).

In summary, the ideas previously developed constitute the theoretical basis for a Global Regulatory Regime for Tech Giants. This framework aligns with the format set by Sabino Cassese, integrating core legal structures with soft law and interdisciplinary aspects. Utilizing tools from Comparative Law, this approach aims to create a balanced and effective regime that not only holds tech giants accountable but also fosters a trustworthy information ecosystem (Cassese, 2005, p. 47).

Implementing this integrated approach requires collaboration among various stakeholders, including governments, private digital platforms, civil society, and international organizations. Global regulatory systems, as articulated by Cassese, thrive on mutual connections and joint decision-making processes. This involves the active participation of states, sub-state entities, and international bodies to create a cohesive regulatory environment (Cassese, 2005, p. 45). Such an environment ensures consistent enforcement and effectiveness across different regions, addressing the root causes of misinformation and promoting a healthier digital public sphere.

By leveraging Cassese's insights (Cassese, 2005) into global regulation, the proposed framework offers a practical pathway to operationalize the interdisciplinary and harm-based approaches discussed. This comprehensive strategy not only addresses the immediate impacts of fake news but also seeks to understand and mitigate the underlying conditions that allow such misinformation to proliferate. Through fostering transparency, accountability, and inclusive dialogue, this regime aims to restore the common factual ground necessary for democratic legitimacy and social cooperation, ultimately enhancing societal trust and resilience in the digital age.

5. CONCLUSION

The pervasive issue of fake news poses a significant threat to the integrity of information disseminated online, particularly by tech giants. This paper has examined the regulatory mechanisms that hold these corporations accountable for the spread of misinformation and evaluated their effectiveness as deterrents. Our analysis reveals that current regulatory frameworks, which often focus on symptom treatment such as content removal and fact-checking, are insufficient for addressing the root causes of misinformation.

The harm-based approach proposed in this study advocates for a holistic and integrative regulatory regime that goes beyond merely reacting to false content. By drawing on methodologies from social medicine and comparative law, we emphasize the importance of understanding the socioeconomic incentives, psychological drivers, and technological dynamics that fuel the production and dissemination of fake news.

Key to this approach is the development of robust legal frameworks that mandate transparency and accountability from tech giants. This includes distinguishing the responsibilities of content creators and sharers, particularly in relation to public agents, to ensure that accountability is appropriately distributed. The integration of soft law and

guidelines can further promote ethical behaviour and best practices among digital platforms, fostering a culture of responsibility.

Drawing on Ronald Dworkin's distinction between principles, norms, and rules, this paper advocates for a regulatory regime that incorporates these elements to create a coherent and adaptable framework. Principles provide the foundational values, norms serve as guidelines for behaviour, and rules specify the rights and obligations of regime members. This structure ensures that the regulatory measures are grounded in justice and equity, adaptable to various socio-political contexts, and capable of addressing the underlying issues of misinformation.

The proposed harm-based regulatory regime aims to proactively combat the spread of fake news by fostering a more resilient and trustworthy digital information ecosystem. By focusing on the root causes and integrating legal, technological, and educational measures, this approach provides a balanced and effective solution to the pervasive issue of fake news.

In conclusion, the need for a holistic and integrative regulatory regime based on a harm-based approach is paramount in addressing the multifaceted nature of fake news. Such a regime not only enhances the resilience of digital information ecosystems but also ensures the restoration of societal trust and the protection of democratic integrity. Through comprehensive and proactive measures, this approach can significantly mitigate the impact of misinformation and foster a healthier digital public sphere.

By drawing on the concepts of global regulatory systems, differentiating responsibilities, promoting digital literacy, and leveraging technology, the proposed regime can effectively address the challenges of digital misinformation. Moreover, by focusing on reparation and the restoration of societal trust, the regime can foster a more trustworthy and reliable information ecosystem.

This comprehensive strategy ensures that regulatory measures are context-sensitive and adaptable to different socio-political landscapes, promoting ethical behaviour online and fostering a healthier digital public sphere. Through proactive and collaborative efforts, this approach can significantly mitigate the impact of misinformation and strengthen the resilience of digital information ecosystems.

ACKNOWLEDGEMENTS

I extend my deepest gratitude to Prof. Dr Fernando Menezes de Almeida and Dr Rodrigo Garcia Cadore, LL.M., for their invaluable guidance throughout the Comparative Constitutional Practices course at the University of São Paulo. Their expertise has been instrumental in shaping this paper. I also thank my colleagues for their insights, particularly during the session on Practices of Constitutional Emotionalization and Rationalization (24 November 2023), which focused on Fake News and Trust in Supreme and Constitutional Courts. The discussions with guest discussant Ana Luíza Calil, and the works of Edda Humprecht and Gulad Alibri/Johannes Buchheim, have greatly enriched my understanding.

LIST OF REFERENCES

Books and Articles

Abiri, G. & Buchheim, J. 2022. Beyond True and False: Fake News and the Digital Epistemic Divide. *Michigan Technology Law Review*, 29, pp. 59-109. https://doi.org/10.36645/mtlr.29.1.beyond

Amnesty International. 2022. *What the Digital Services Act means for human rights and harmful Big Tech business models. Amnesty International EU Office*. Available at: https://www.amnesty.org/en/documents/pol30/5830/2022/en/ (10. 10. 2024).

Buri, I. & van Hoboken, I. 2021. *The DSA proposal: a critical overview*. Institute for Information Law, DSA Observatory. Available at: https://dsa-observatory.eu/wp-content/uploads/2021/11/Buri-Van-Hoboken-DSA-discussion-paper-Version-28_10_21.pdf (10. 10. 2024).

Caled, D. & Silva, M. J. 2022. Digital media and misinformation: An outlook on multidisciplinary strategies against manipulation. *Journal of Computational Social Science*, 5, pp. 123–159. https://doi.org/10.1007/s42001-021-00118-8

Calil, A. L. 2022. Public Agents in Social Media Regulation: The Brazilian Case in a Comparative Perspective, *Journal of Law, Market & Innovation*, 1(2), pp. 162-182.

Cassese, S. 2005. Administrative Law Without the State? The Challenge of Global Regulation. *New York University Journal of International Law and Politics*, 37(4), pp. 663-684.

Dworkin, R. 1977. *Taking Rights Seriously*. London: Duckworth.

Engel, G. L. 1977. The Need for a New Medical Model: A Challenge for Biomedicine. *Science*, 196(4286), pp. 129-136. https://doi.org/10.1126/science.847460

Flew, T., Martin, F. & Suzor, N. 2019. Internet Regulation as Media Policy: Rethinking the Question of Digital Communication Platform Governance. *Journal of Digital Media & Policy*, 10(1), pp. 33-50. https://doi.org/10.1386/jdmp.10.1.33_1

Government of Canada. 2021. *Have your say: The Government's proposed approach to address harmful content online*. Available at: https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content.html (10. 10. 2024).

Governor Ron DeSantis Signs Bill to Stop the Censorship of Floridians by Big Tech. 2021. Available at: https://www.flgov.com/2021/05/24/governor-ron-desantis-signs-bill-to-stop-the-censorship-of-floridians-by-big-tech/ (10. 10. 2024)

Humprecht, E. 2018. Where Fake News Flourishes: A Comparison across Four Western Democracies. *Information, Communication & Society*, 22(13), pp. 1973-1988. https://doi.org/10.1080/1369118X.2018.1474241

Krasner, S. D. 1983. International Regimes. In: Krasner, S. D. (ed.), *International Regimes*. Ithaca, NY: Cornell University Press, pp. 1-21.

Meyers, Z. 2022. *Will the Digital Services Act save Europe from disinformation?* Centre for European Reform. Available at: https://www.cer.eu/insights/will-digital-services-act-save-europe-disinformation (9. 10. 2024).

Salloum, J. *et al.* 2024. *Canada's new Online Harms Act (C-63): what you need to know.* Osler. Available at: https://www.osler.com/en/insights/updates/canada-s-new-online-harms-act-c-63-what-you-need-to-know/?pdf=1 (10. 10. 2024).
Max Planck Institute for the Study of Crime, Security and Law. 2024. *Rethinking Digital Media Regulation*. Available at: https://csl.mpg.de/en/projects/rethinking-digital-media-regulation?c=178896 (27. 6. 2024).
Rinceanu, J. & Stephenson, R. 2024. *Differential Diagnosis in Online Regulation*. Eucrim. Available at: https://eucrim.eu/articles/differential-diagnosis-in-online-regulation/ (10. 10. 2024).
Ruggie, J. G. 1975. International Responses to Technology: Concepts and Trends. *International Organization*, 29(3), pp. 557-583. https://doi.org/10.1017/S0020818300031696
Stephenson, R. & Rinceanu, J. 2023. Digital Iatrogenesis: Towards an Integrative Model of Internet Regulation. *Eucrim*, 1, pp. 73-80. Available at: https://eucrim.eu/articles/digital-iatrogenesis/ (10. 10. 2024).
Taylor, R. & Rieger, A. 1985. Medicine as a social science: Rudolf Virchow on the typhus epidemic in Upper Silesia. *International Journal of Health Services*, 15(4), pp. 547-559. https://doi.org/10.2190/XX9V-ACD4-KUXD-C0E5
Vogus, C. 2021. *Answers to Five Key Questions from House Energy & Commerce Section 230 Hearing*. Center for Democracy and Technology. Available at: https://cdt.org/insights/answers-to-five-key-questions-from-house-energy-commerce-section-230-hearing/ (10. 10. 2024).
Zweigert, K. & Kötz, H. 1998. *Introduction to Comparative Law*. Oxford: Clarendon Press; New York: Oxford University Press.

Legal Sources and Case-Law

Act to Improve Enforcement of the Law in Social Networks *(Netzwerkdurchsetzungsgesetz* - NetzDG*), Federal Law Gazette* I at 3352, enacted 1 October 2017
Criminal Code *(Strafgesetzbuch* - StGB*)*, last amended by Article 1 of the Law of 28 March 2023, *Federal Law Gazette* I p. 368.
Doe v. *MySpace, Inc*., 528 F.3d 413 (5th Cir. 2008)
European Parliament and Council Regulation (EU) 2022/2065 of 19 October 2022 on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC [2022] OJ L277/1.
Fair Housing Council of San Fernando Valley v. *Roommates.com,* LLC, 521 F.3d 1157 (9th Cir. 2008).
Florida Senate Bill 7072, 2021.
Force v. *Facebook, Inc*., 934 F.3d 53 (2d Cir. 2019).
Jones v. *Dirty World Entertainmen*t *Recordings* LLC, 755 F.3d 398 (6th Cir. 2014).
Moody v. NetChoice, LLC, 603 U.S. (2024)
NetChoice, LLC, *et al.* v. *Attorney General, State of Florida, et al.*, No. 21-12355 (11th Cir. 2022).
Online Harms Act, Bill C-63, 1st Sess, 44th Parl, 2024.

United States, Communications Decency Act, 47 U.S.C. § 230 (1996).United States Constitution.
United Nations (2015) Paris Agreement.
Zeran v. *America Online, Inc*., 129 F.3d 327 (4th Cir. 1997)

UDC: 342.725(439) DOI: 10.56461/iup_rlrc.2024.5.ch7

Gábor FEKETE*
Faculty of Law, University of Pécs, Hungary

THE LAW OF LANGUAGE USE IN HUNGARIAN CIVIL PROCEEDINGS, THE APPLICABILITY OF TRANSLATION SOFTWARE

The new Hungarian Civil Procedure Act entered into force on 1 January 2018 and, among other things, re-regulated the rules on the use of language in civil proceedings. In addition to the national law, EU and international law provisions apply to exercising the right to use language.

The study presents the rules of Hungarian civil procedural law concerning the use of language, i.e., the range of languages that can be used orally and in writing, and the rules on the bearing of costs related to the use of language. It details how these rules reflect Hungary's international legal obligations under the European Charter for Regional or Minority Languages. It also explains which language use provisions must be considered when applying EU law. The Regulation on the service of documents gives the addressee the right to refuse to accept the document. The study explains the content of this right of refusal and the translation obligation of the party requesting service.

Interpretation and translation are closely related to language use. Technological developments have led to the widespread availability of translation and interpreting software. This paper will show to what extent their use in civil proceedings is appropriate in light of the above provisions.

Keywords: use of language, civil procedure, service of documents in EU, EU law.

1. THE RIGHT TO USE LANGUAGE IN HUNGARIAN CIVIL PROCEEDING

1.1. The Framework of Hungarian Procedural Law

According to the Hungarian Constitution, everyone has the right to have any charge against him or her, or any rights and obligations in a lawsuit, adjudicated by an independent and impartial tribunal established by law, in a fair and public trial within a reasonable

* PhD student, ORCID: 0000-0002-2211-1081, e-mail: *gaborfekete@outlook.com*

time.[1] The Constitution identifies three branches of judicial activity: criminal, civil and administrative. A new code governs the procedural rules of civil justice, Act CXXX of 2016 on the Code of Civil Procedure, which entered into force on 1 January 2018.

Hungary is an active member of the European Union and the international community. When drafting a new code, the legislator must consider the obligations arising from EU membership and international commitments.[2] The Constitution stipulates that Hungary shall ensure the consistency of international law and Hungarian law to fulfil its obligations under international law. [3]

Underlining the significant difference between the right to use language in criminal and civil matters is essential. Concerning civil litigation, there is no obligation under EU law or international law to ensure parties' unrestricted use of their mother tongue, and these limitations are mainly reflected in the rules on the costs of interpretation and translation. In comparison, in EU law, specific legal instruments on judicial cooperation in civil matters and certain international treaties lay down specific rules on the use of language in civil disputes, described in detail below, following a description of the Hungarian national rules.

1.2. New Rules of Use of Language in Code of Civil Procedure

The Hungarian Civil Procedural Code contains a simple and unambiguous main rule regarding the use of language stipulating that the language of court proceedings is Hungarian.[4] It regulates the rules for using written and oral language in separate paragraphs, including references to obligations under EU and international law. As regards the use of the written language, it stipulates that, unless otherwise provided by law, a binding legal act of the European Union or an international convention, pleadings addressed to the court must be submitted in Hungarian, and the court shall send its pleadings and its decision in Hungarian.[5] Regarding the use of oral language, it states that in court proceedings, everyone has the right to use their mother tongue or, in the context of an international convention, their mother tongue or regional or national language. In court proceedings, members of all nationalities living in Hungary and recognised by the National Minority Act are entitled to use their national language under international conventions on the use of regional or minority languages.[6]

The new Code was designed to increase litigation efficiency, revise procedural principles to promote efficiency, enshrine good judicial practice in law, and strengthen the role of electronic law.[7] These conceptual objectives are reflected in the new Code at several points concerning the right to use languages.

---

1 Constitution of the Republic of Hungary of 2011 (rev. 2016), Art. XXVIII.

2 Art. E(2) of the Constitution.

3 Art. Q(2) of the Constitution.

4 Code of Civil Procedure of the Republic of Hungary, Art. 113 (1).

5 Code of Civil Procedure, Art. 113 (2).

6 Code of Civil Procedure, Art. 113 (3).

7 Concept of the new Code of Civil Procedure – 2015. Available at: https://2015-2019.kormany.hu/download/6/42/40000/20150224%20PP%20koncepci%C3%B3.pdf#!DocumentBrowse (15. 7. 2024).

The previous Code of Civil Procedure, based on the requirements of equality before the law and national equality, regulated the use of language at a fundamental level and stipulated, among other things, that no one may suffer disadvantages because of not knowing Hungarian.[8] In practice, the Regulation of these principles and the emphasis on the principle that no one should be disadvantaged has led to courts providing interpretation and translation in civil proceedings, to a greater extent than justified, with advance payments from the state or at state expense. In the previous legislation, the combined interpretation of the rule that exercising linguistic rights and the interpreter's fees were part of the litigation costs needed to be revised. The seriousness of the problem is illustrated by the fact that intending to harmonise the law, the Civil Chamber of the Supreme Court of Justice has also issued an opinion on the bearing of costs concerning the use of language.[9]

The new Code regulates the rules on the use of language in the chapter of general provisions under the heading of other general rules, thus clarifying that the legislator does not consider the use of language as a principle, but a technical issue.

The new regulatory approach will also contribute to litigation efficiency by terminating the uncertainty concerning the costs of language use. Litigants will clearly understand the legal costs they must advance and bear concerning language use. Furthermore, no additional costs will be incurred by the ex-post recovery of unnecessary advances of litigation costs by the state concerning language use.[10] The Civil Code requires the plaintiff to advance the costs of language use, and if they fail to do so despite being ordered to do so by the court, the proceedings shall be suspended. [11]

Based on the above, two types of exceptions to the general rule on language use can be envisaged: one being a binding legal act of the European Union and the other an obligation based on an international convention. These types of exceptions are described below.

2. THE EUROPEAN CHARTER FOR REGIONAL AND MINORITY LANGUAGES

2.1. Commitments Under the Charter

The European Charter for Regional or Minority Languages (hereafter "the Charter"), concluded within the framework of the Council of Europe, aims to safeguard Europe's cultural richness and traditions by protecting its historic regional or minority languages without prejudice to the official languages and to create ever closer unity between the States Parties.[12] The purpose of the Charter is to guarantee the right to the private and public use of a regional or minority language, as enshrined in several international conventions.[13]

---

[8] Art. 6(1) of Act III of 1952 on the Code of Civil Procedure.

[9] Opinion No. 3/2006 (XI. 27.) PK on the advance payment and bearing of the costs of interpreters and translation in connection with the use of the mother tongue, regional or minority language.

[10] Code of Civil Procedure, Art. 79 (2), (3).

[11] Code of Civil Procedure, Art. 121 (1) (e).

[12] European Charter for Regional or Minority Languages of 5 November 1992 (Charter).

[13] Under the principles set out in the International Covenant on Civil and Political Rights of the United Nations and the Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms.

The provisions of the Charter are applicable in Hungary from 1 March 1998.

The Charter lays down specific rules on the administration of justice in criminal, civil and administrative matters. For each type of case, the Charter sets out several language preference "packages" from which States Parties can choose how to ensure the right to use languages.[14]

Concerning civil proceedings under the Charter, States Parties may undertake, jointly or severally, to (i) ensure that judicial authorities, at the request of a party, conduct proceedings in regional or minority languages and/or (ii) allow a litigant to appear in person before a court in his or her regional or minority language without incurring extra costs and/or (iii) allow the submission of documents and evidence in regional or minority languages, if necessary with the assistance of interpreters and translations.[15]

Concerning civil proceedings, Hungary has undertaken the obligations set out in Article 9(1)(b)(ii) and (iii) of the Charter in respect of Croatian, German, Romanian, Serbian, Slovak, Slovene, Romanian and Basque languages. The Charter's commitment in Article 9(1)(b)(ii) means that in civil proceedings in the above-listed regional or minority languages, a litigant who has to appear in person in court should be allowed to use his or her regional or minority language without incurring extra costs. The Charter has also undertaken an obligation in Article 9(1)(b)(iii) for Croatian, German, Romanian, Serbian, Slovak, Slovene, Romani and Basque, which means that, as an exception to the main rule of the Civil Procedure Code, these languages should be allowed to submit documents and evidence in regional or minority languages in civil proceedings, if necessary with the assistance of interpreters and translations. It is essential to underline that Hungary has not undertaken an obligation under Article 9(1)(b)(i) of the Charter to conduct the entire procedure (allowing for both written and oral statements) in a regional or minority language at the request of one of the parties.

It should be stressed that the nationalities recognised in Hungary are Bulgarian, Croatian, German, Greek, Armenian, Polish, Romanian, Ruthenian, Serbian, Slovak, Slovene, Slovenian, Ukrainian and Polish.

The languages listed in Hungary's commitment to the Charter and the languages of the recognised nationalities overlap significantly but are not identical. Legal uncertainty remained regarding the use of Bulgarian, Greek, Polish, Armenian, Ruthenian, and Ukrainian, which the Constitutional Court clarified in the following decision.

2.2. Language Use Rights of Recognised Nationalities Not Mentioned Under Hungarian Commitments

A judge in an administrative case appealed to the Hungarian Constitutional Court, claiming that the Hungarian commitment concerning the Charter and the procedural rules of use of language, as described above, were contrary to the Constitution. In the view of the initiating judge, the rules violate the right of national minorities to use languages and the prohibition of discrimination.

---

[14] Szalayné Sándor, E. 2016. A nyelvhasználat jogi szabályozhatósága. *Acta Humana*, 3, pp. 9-18.

[15] Charter, Art. 9(1)(b).

It should be noted that the rules of the Civil Procedural Code on the right to use languages apply not only in civil proceedings but also in other proceedings, including the administrative proceedings on which this case is based.

As a basis for the application, the applicant argued that, under the Constitution, all nationalities, including the Ukrainian and Ruthenian nationalities, should be entitled to the rights under the Civil Procedure Code in the same conditions. However, since the Government of the Republic of Hungary has not undertaken any obligation concerning the Ukrainian and Ruthenian languages in the area of civil justice, and therefore the Charter does not provide for an exception to the main rule of the procedural law concerning these languages and thus for the Ukrainian and Ruthenian nationalities, the rights of nationalities and the right to non-discrimination are infringed.

The Constitutional Court examined the petition in merits and found it unfounded.[16]

The Constitutional Court confirmed that Hungary had not assumed any international legal obligations concerning the Ukrainian and Ruthenian languages in civil justice. Therefore, the Charter does not protect the rights of the Ukrainian and Ruthenian nationalities in these languages and thus for the nationalities of Ukraine and Ruthenia under the Article 113 (2) of the Civil Procedural Code. The European Union does not have a binding act providing for such an exception, and neither does the European Council and its Additional Protocol nor the International Covenant on Civil and Political Rights.

Concerning the Charter, the Constitutional Court pointed out that the Charter had left it to the States Parties to decide which languages they would undertake to protect and determine the levels of protection provided by the Charter. It stressed that the Charter laid down rules not only on the provision of language use but also on the bearing of the related costs.

Concerning Hungarian national minority law, it stressed that, under the Constitution, national minorities living in Hungary had the right to use their mother tongue under the rules laid down in the sectoral procedural codes. The Constitutional Court has interpreted them in the light of nationality law, and found that the under the Article 113(3) of the Civil Procedure Act any party who is required to appear in person before the court and who is a member of a nationality recognised in the Act on the Rights of Nationalities and who lives in Hungary is entitled to the right to use his or her national language orally in civil proceedings, in administrative proceedings and non-litigation proceedings, exempt from the payment of the costs (interpreter's fees) incurred in this connection. Under Article 113(2) of the Civil Procedure Act, a member of a recognised nationality living in Hungary has the right to submit to the court documents and evidence in his or her national language, if necessary, with the assistance of interpreters and translations. However, concerning the use of written languages, Hungary has not made any commitment in the Charter to provide written communication free of charge to persons belonging to the minorities listed in the Charter. However, the rules on, for example, cost discounts for members of national minorities are also applicable in this case.

[16] Hungarian Constitutional Court's Decision No. 2/2021 (I. 7.).

Based on the above, the Constitutional Court has concluded that the procedural laws permit the use of language by members of national minorities as stipulated by the National Minority Act, both orally and in writing. However, it also noted a difference in the costs of language use between the languages of the recognised national minorities and the languages covered by the undertaking given concerning the Charter.

Concerning the prohibition of discrimination, the Constitutional Court pointed out that, according to its settled practice, it cannot be considered discrimination if the legislation lays down different provisions for a group of persons with different characteristics because unconstitutional discrimination is only possible within a comparable group of persons belonging to the same category. The disputed provisions of the Civil Procedural Code grant additional rights to members of national minorities, for example, compared to those granted to natural persons whose mother tongue is Hungarian or who do not belong to a national minority.

The Constitutional Court pointed out in its reasoning that, under the Civil Procedural Code, all nationalities have the right to use their mother tongue in civil proceedings. If a party who is a member of a nationality recognised by the law and who is required to appear in person before the court wishes to use his or her national language in person, he or she may do so without incurring any extra costs, that is to say, the cost of providing an interpreter remains borne by the state. They are also entitled to use the language of their nationality in writing, as they can submit documents and evidence in their national language in civil proceedings, but not free of charge. The Constitutional Court has pointed out that this right does not apply to regional or minority languages in the absence of an undertaking with respect to the Charter. Moreover, the Charter also does not require the acceding States to attach legal aid to all forms of language use. It has found no breach of Constitutional rules and stressed that the responsibility of the legislator to set the scope of the state's obligation to bear the costs of some aspects of the litigation also in view of the budgetary constraints.

3. THE RULES ON THE USE OF LANGUAGE IN THE REGULATION OF THE SERVICE OF DOCUMENTS

Binding acts of EU law also influence the rules on the use of language in Hungarian civil proceedings. Among these, the Regulation on the service of documents[17] deserves special mention as a legal instrument binding and directly applicable in the Member States regarding service between the Member States in civil and commercial matters. [18] The Regulation provides for several methods of service. Service may be effected by the use of transmitting or receiving agencies, by consular or diplomatic channels, by a diplomatic representative or consular officer directly in the Member State addressed, by

[17] Regulation (EU) 2020/1784 of the European Parliament and of the Council of 25 November 2020 on the service in the Member States of judicial and extrajudicial documents in civil or commercial matters (service of documents), OJ L 405, 2.12.2020. (Regulation).

[18] Judgment of the Court (First Chamber) of 19 December 2012 in Case C-325/11 Alder [ECLI:EU:C:2012:824].

direct postal services, by electronic means or by direct service.[19] There shall be no subordination between the different methods of service.[20]

The Regulation lays down rules on the use of language at two levels. First, the right of the addressee to refuse to accept the document applies to all service methods.[21] On the other hand, it lays down rules on the language in which the bodies involved in the service of documents and the central bodies communicate. An essential element of the right to use languages is the question of the rules on costs, the rules of the Regulation on costs being set out in a separate subsection.

3.1. Right to Refuse to Accept a Document

According to the case law of the Court of Justice, the possibility of refusing to accept a document derives from the need to safeguard the recipient's right to defence, as provided for in the second paragraph of Article 47 of the Charter and Article 6 of the European Convention for the Protection of Human Rights and Fundamental Freedoms, signed in Rome on 4 November 1950.[22] The purpose of the Regulation on the service of documents is to modernise and expedite the transmission of judicial documents between Member States. However, these objectives cannot be achieved if national provisions in any way weaken the rights of the defence of the addressees. Failure to properly inform the addressee of his right to refuse to accept the document is a substantial but remediable procedural violation.[23]

Failure to inform the addressee properly will result in service being deemed improper and the time limit for exercising the right to refuse not being triggered.[24] In the absence of proper service, the court seized of the dispute may not give a decision which has the force of res judicata, including a decision on the substance of the matter and a decision determining the procedural sanction applicable to the other party affected by service, nor may it attach any legal force or enforceability to it. A decision based on improper service may be subsequently effectively challenged, a refusal of recognition may be sought in a cross-border context, and enforceability may be challenged in a purely national context by an application for revocation of the enforcement order under Hungarian law.

The new Regulation on the service of documents improves the procedure for the addressee's right to refuse to accept a document if it has not been drawn up or translated into the appropriate language.[25]

---

[19] For rules on the various methods of service, see section 12 of the Regulation.

[20] Judgment of the Court (Third Chamber) of 9 February 2006 Case C-473/04 Plumex [ECLI:EU:C:2006:96].

[21] Art. 12(6) of the Regulation.

[22] Promulgated by Act XXXI of 1993.

[23] Judgment of the Court (First Chamber) of 16 September 2015 in Case C-519/13 Alpha Bank Cyprus [ECLI:EU:C:2015:603].

[24] Judgment of the Court (Fourth Chamber) of 7 July 2022 in Case C-7/21 LKW Walter [ECLI:EU:C:2022:527].

[25] Ammon, U. 2006. Language conflicts in the European Union. *International Journal of Applied Linguistics*, 16(3), pp. 319-338.

The conditions for the lawfulness of a declaration of refusal to accept a document have not changed since the first Regulation. The addressee still has the right to refuse if the language of the document to be served is not the language which the addressee understands, or an official language of the Member State addressed or, if that Member State has several official languages, the official language or one of the official languages of the place where service is to be effected.[26]

Under the above rule, the addressee shall not have the right to refuse to accept service of a document in an official language of the Member State addressed, irrespective of whether they understand that official language. The conclusion to be drawn from that rule, in particular in the light of the fact that it has remained unchanged since the first Regulation on the service of documents, is that in respect of a person residing in a Member State, European Union law requires that person to be able to administer documents in the language of that Member State.

The new Regulation on the service of documents has doubled the time limit for the addressee to make a statement of refusal to accept a document to two weeks from the service date.[27] The statement of refusal may be sent in writing on the form prescribed by the Regulation or by other written declaration to the receiving agency or, in the case of other service methods, to the "sending" agency.[28] The Regulation makes it clear that the "sending" institution decides the validity of the exercise of the right of refusal and that a duly repeated service may remedy any irregularity in the service.[29]

In addition to the above, the Court of Justice case law provides guidance on the lawfulness of refusal of service and the adequacy of linguistic knowledge. The court in the Member State of transmission must ensure that the addressee has been informed of their right to refuse service under the Regulation. In doing so, whether the addressee has been duly informed, whether the defect has subsequently been remedied in the absence of such information or in the event of irregular service and whether such person was not prevented from exercising their right to refuse service. In light of all the circumstances of the case, it is necessary to assess the addressee's language knowledge since legal language is different from everyday and business language. [30] Therefore, for example, the use of a language stipulated in the course of a business activity does not constitute sufficient knowledge of the language required for court proceedings.[31]

The question of which documents should be translated to be served appropriately cannot be avoided. Here again, the case-law of the Court of Justice provides guidance, according to which the addressee of a document instituting proceedings may not refuse to accept it if it puts the addressee in a position to enforce their rights in the Member State of origin in the context of judicial proceedings, provided that the document

[26] Art.12(1) and (6) of the Regulation.

[27] Art. 12(3), (6) of the Regulation.

[28] Art. 12(4), (6) of the Regulation.

[29] Art. 12(5), (6) of Regulation (EC) No 1246/2004.

[30] Order of the Court (Tenth Chamber) of 28 April 2016 in Case C-384/14 Alta Realitat [ECLI:EU:C:2016:316].

[31] Judgment of the Court (Third Chamber) of 8 May 2008 in Case C-14/07 Weiss [ECLI:EU:C:2008:264].

contains an annexe of supporting documents, which are not drawn up in the language of the Member State addressed or in a language of the Member State of transmission which the addressee understands, but are purely evidential documents and are not indispensable to an understanding of the subject-matter and the pleas in law and main arguments of the applicant. The national court shall determine whether the content of the document instituting the proceedings is sufficient to enable the defendant to assert their rights or whether the sender is required to remedy the lack of a translation of an indispensable annexe.[32] Thus, for example, EU law precludes a national legal provision which obliges all businesses to provide all the information on invoices relating to cross-border transactions exclusively in the official language of that federal entity, as otherwise they will be considered null and void.[33]

3.2. Language of Communication Between Bodies Concerned for the Regulation

In the practical application of the methods of service governed by the Regulation, communication between these bodies via transmitting and receiving agencies and, for all methods of service, communication with the central body may involve the need for translation. It is established practice that the language of the communication will always be the language of the requested body, i.e., the burden of translation falls on the requesting party, both for the request and for the reply.

The Regulation requires Member States to communicate to the Commission, for publication, the languages accepted for completing the forms.[34] The Commission will make this information publicly available on the European Judicial Portal in the European Judicial Atlas in Civil Matters, in the country information section of the Regulation application on the service of documents.[35] Typically, Member States accept requests in languages other than their official languages; for example, Hungary receives requests in English, German and French in addition to Hungarian.

It is essential to underline that the range of languages accepted by the Member States for the forms of the Regulation on the service of documents is entirely independent of the addressee's right to refuse to accept the document.

3.3. Rules Relating to the Charging of Costs

The Regulation contains a short and clear provision on the bearing of translation costs. According to this provision, the applicant is to bear translation costs incurred prior to the transmission of the document.[36] Regarding the detailed rules, applying national procedural rules becomes necessary.

---

[32] Judgment of the Court (Third Chamber) of 8 May 2008. in Case C-14/07 Weiss [ECLI:EU:C:2008:264].

[33] Judgment of the Court (Grand Chamber) of 21 June 2016 in Case C-15/15 New Valmar [ECLI:EU:C:2016:464].

[34] Art. 3(4)(d) of the Regulation.

[35] European Justice – Hungary, serving documents. Available at: https://e-justice.europa.eu/38580/HU/serving_documents_recast (15. 7. 2024).

[36] Art. 9(2) of the Regulation.

The above shows that the applicant's right to effective legal protection is limited by the need to ensure that the defendant's rights of defence are adequately protected.[37] The Hungarian Code of Civil Procedure assigns to the court the task of contributing, in the manner and by the means provided for by law, to the fulfilment of the parties' procedural obligations in order to ensure the concentration of proceedings. The purpose of the court's intervention activity is to facilitate the exercise of the parties' right to be heard; its means are questioning, calling for statements, and providing information.

Where cross-border service is necessary, the court's duty to intervene requires it to inform the parties, in particular the party requesting service, of the methods of service provided for by the Regulation on the service of documents and the relevant rules on the right of the addressee to refuse to accept service. In particular, the requesting party should be informed of the possible need for the documents to be translated and the languages that may be used.

Regarding the costs of translation, the Hungarian procedural rule[38] is aligned with the Regulation on the service of documents, according to which the applicant is to advance the costs of service of a court document abroad not relating to the taking of evidence under a binding European Union act or an international convention.[39] The costs of service of the document abroad relating to the taking of evidence are to be determined by the rules on the interest of the taking of evidence.[40] Failure to advance the costs shall entail, in the first case, the consequences of a stay of proceedings and, in the second case, the consequences of failing to give evidence in the absence of other evidence. [41]

The Regulation refers to the law of the requesting state regarding the form of translation accepted. According to this law, a translation may be accepted in addition to a certified translation or a translation considered suitable for use in proceedings under the law of the transmitting Member State.[42] Hungarian law does not provide for a certified translation. As a general rule, a simple translation may be used in civil proceedings unless otherwise provided by law, EU legislation or international conventions or unless the parties dispute the authenticity of the translation.[43]

The exact linguistic requirement described concerning the Regulation on the Service of Documents is provided for in, among other regulations the Brussels Ia Regulation,[44] the Brussels IIb Regulation,[45] and the Regulation on the European Small Claims

[37] Art. 6 of Act CXXX of 2016 on the Code of Civil Procedure on the intervention of the court.

[38] Code of Civil Procedure, Art. 79 (4).

[39] Art. 265 (1) of the Code of Civil Procedure.

[40] Code of Civil Procedure, Art. 121 (1) (e).

[41] Code of Civil Procedure, Art. 265 (1).

[42] Recital 25 of the Regulation.

[43] Code of Civil Procedure, Art. 62.

[44] Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters Article, OJ L 351, 20.12.2012.

[45] Council Regulation (EU) No 2019/1111 of 25 June 2019 on jurisdiction, recognition and enforcement of judgments and decisions in matrimonial matters and the matters of parental responsibility and the expulsion of children Article 55, OJ L 178, 2.7.2019.

Procedure.[46] In light of the above, the above statement concerning the Regulation on the service of documents appears to be generalisable in the sense that, as regards judicial cooperation in civil matters, the legal persons concerned may be expected to be able to practise in the official language of their state of residence.

4. THE FUTURE OF LANGUAGE USE – THE USE OF TRANSLATION AND INTERPRETATION PROGRAMMES

The Office of the United Nations High Commissioner for Human Rights, in its report "Steps to overcome obstacles and challenges to equal political participation," states that political and social participation rights play a crucial role in promoting the rule of law, human rights and the elimination of discrimination, among other things. It recommends the introduction of measures to overcome language barriers. Such measures could include the use of language technology.[47] Language technologies are tools capable of processing communication between people and of communicating directly with people, in particular, written translation programs, oral interpretation programs, and language learning aids.[48]

Concerning the use of language, both Hungarian law and the Charter and the Regulation on the service of documents cited in the study contain provisions on the authenticity of translation but do not provide for the method of producing a simple translation, which does not exclude machine translation.

However, recent legislative developments have addressed the possibility of machine translation. EU legislators are considering, in connection of the E-codex system, to allow machine translation at the EU level.[49]

Legal language differs considerably from everyday language because of its complexity and the use of legal terms.[50] This difference requires specific translation and interpretation skills, and the use of applications developed for ordinary language in a legal context is far from straightforward. For this reason, although simple translations can be produced using translation software in the absence of a prohibition, as described above, they are not currently of sufficient quality in a legal context and, in any case, require appropriate proofreading.[51] An example of this is the operation of the Court of Justice of the European Union, which translates its judgments into all languages, and the

---

[46] Regulation (EC) No 861/2007 of the European Parliament and of the Council establishing a European Small Claims Procedure Article 6, OJ L 199, 31.7.2007.

[47] Factors that impede equal political participation and steps to overcome those challenges in points 13, 55, 73, 95. General Assembly of the UN. 2014. Factors that impede equal political participation and steps to overcome those challenges - Report of the Office of the United Nations High Commissioner for Human Rights. Available at: https://documents.un.org/doc/undoc/gen/g14/069/52/pdf/g1406952.pdf (15. 7. 2024)

[48] Láncos, P. L. 2022. A nyelvtechnológia szerepe a kisebbségi nyelvek és a nyelvi kisebbségek társadalmi, politikai és gazdasági részvételének elősegítésében. *In Medias Res*, 5, pp. 67-77.

[49] eu-LISA. Eu- LISA's approach to multilingualism. Available at: https://www.eulisa.europa.eu/AboutUs/MandateAndActivities/Multilingualism (15. 7. 2024).

[50] Cao, D. 2013. Legal Translation. In: Chapelle, C. A. (ed.), *The Encyclopedia of Applied Linguistics.*

[51] Rules of Procedure of the Court of Justice of the European Union, Art. 41.

judgments are authentic in all languages. Legal translators and linguists continue to use the software, developed for the EU legal language, only as a tool for internal use.[52] Also, for internal use only, the European Commission provides eTranslation, a cutting-edge neural machine translation service ever produced. The Commission is stressing that it produces raw machine translations. It may be used to get the gist of a text or as the starting point for a human-quality translation, but if the user needs a perfectly accurate, high-quality translation, a skilled professional translator still needs to revise the text.[53]

LIST OF REFERENCES

Ammon, U. 2006. Language conflicts in the European Union. *International Journal of Applied Linguistics*, 16(3), pp. 319-338. https://doi.org/10.1111/j.1473-4192.2006.00121.x.

Cao, D. 2013. Legal Translation. *The Encyclopedia of Applied Linguistics.* https://doi.org/10.1002/9781405198431.wbeal0679

Láncos, P. L. 2022. A nyelvtechnológia szerepe a kisebbségi nyelvek és a nyelvi kisebbségek társadalmi, politikai és gazdasági részvételének elősegítésében. *In Medias Res*, 5, pp. 67-77.

Szalayné Sándor, E. 2016. A nyelvhasználat jogi szabályozhatósága, *Acta Humana*, 3, pp. 9-18.

Szabó, P. 2022. Nyelvi sokféleség és terminológiai kihívásokaz Európai Unió Bíróságán. *Európai Jog*, 1, pp. 1-13.

Legal Sources and Case Law

Act III of 1952 on the Code of Civil Procedure.

Code of Civil Procedure of the Republic of Hungary.

Constitution of the Republic of Hungary of 2011 (rev. 2016).

Convention for the Protection of Human Rights and Fundamental Freedoms.

Council Regulation (EU) No 2019/1111 of 25 June 2019 on jurisdiction, recognition and enforcement of judgments and decisions in matrimonial matters and the matters of parental responsibility and the expulsion of children Article 55, OJ L 178, 2. 7. 2019.

Covenant on Civil and Political Rights.

European Charter for Regional or Minority Languages of 5 November 1992.

European Commission. eTranslation - The European Commission's Machine Translation system. Available at: https://commission.europa.eu/resources-partners/etranslation_en (15. 7. 2024).

General Assembly of the UN. 2014. Factors that impede equal political participation and steps to overcome those challenges - Report of the Office of the United Nations High Commissioner for Human Rights. Available at: https://documents.un.org/doc/undoc/gen/g14/069/52/pdf/g1406952.pdf (15. 7. 2024)

[52] Szabó, P. 2022. Nyelvi sokféleség és terminológiai kihívásokaz Európai Unió Bíróságán. *Európai Jog*, 1, pp. 1-13

[53] European Commission. eTranslation - The European Commission's Machine Translation system. Available at: https://commission.europa.eu/resources-partners/etranslation_en (15. 7. 2024).

Hungarian Constitutional Court's Decision No. 2/2021 (I. 7.).
Judgment of the Court (First Chamber) of 19 December 2012 in Case C-325/11 Alder [ECLI:EU:C:2012:824].
Judgment of the Court (First Chamber) of 16 September 2015 in Case C-519/13 Alpha Bank Cyprus [ECLI:EU:C:2015:603].
Judgment of the Court (Fourth Chamber) of 7 July 2022 in Case C-7/21 LKW Walter [ECLI:EU:C:2022:527].
Judgment of the Court (Grand Chamber) of 21 June 2016 in Case C-15/15 New Valmar [ECLI:EU:C:2016:464].
Judgment of the Court (Third Chamber) of 9 February 2006 Case C-473/04 Plumex [ECLI:EU:C:2006:96].
Judgment of the Court (Third Chamber) of 8 May 2008 in Case C-14/07 Weiss [ECLI:EU:C:2008:264].
Opinion No. 3/2006 (XI. 27.) PK on the advance payment and bearing of the costs of interpreters and translation in connection with the use of the mother tongue, regional or minority language.
Order of the Court (Tenth Chamber) of 28 April 2016 in Case C-384/14 Alta Realitat [ECLI:EU:C:2016:316].
Regulation (EC) No 1246/2004.
Regulation (EC) No 861/2007 of the European Parliament and of the Council establishing a European Small Claims Procedure Article 6, OJ L 199, 31.7.2007.
Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters Article, OJ L 351, 20.12.2012.
Regulation (EU) 2020/1784 of the European Parliament and of the Council of 25 November 2020 on the service in the Member States of judicial and extrajudicial documents in civil or commercial matters (service of documents), OJ L 405, 2.12.2020.
Rules of Procedure of the Court of Justice of the European Union.

UDC: 004.8:343(4-672EU) DOI: 10.56461/iup_rlrc.2024.5.ch8

*Marina M. MATIĆ BOŠKOVIĆ**
Institute of Criminological and Sociological Research, Belgrade, Serbia

IMPLICATIONS OF EU AI REGULATION FOR CRIMINAL JUSTICE**

Artificial intelligence (AI) is becoming part of the judiciary worldwide. The use of artificial intelligence is different from country to country. While AI has the potential to enhance efficiency, accuracy, and decision-making, it also raises significant ethical and legal concerns, particularly regarding the right to a fair trial. Compared to other judicial procedures, the criminal procedure has specifics and is the most vulnerable to the use of artificial intelligence due to power imbalance. Specifically, criminal procedure directly influences citizens' fundamental rights, including deprivation of liberty. Therefore, challenges identified in the use of artificial intelligence such as bias and discrimination have increased impact in criminal procedures. Beyond criminal procedure, artificial intelligence is used by investigative authorities before the criminal trial or even to prevent criminal acts, however, the same challenges and risks exist as for the criminal procedure. The artificial intelligence tools are developed by humans and inequalities that exist in the real criminal justice system will be reproduced in the AI tools.

The European Union (EU) and Council of Europe (CoE) are making efforts to develop a legal framework for the use of artificial intelligence in the judiciary. The article focuses on acts adopted by EU institutions on AI use in judiciary: European Parliament Resolution 2020/2016 (INI) Artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters, Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence and amending certain Union legislative acts (COM/2021/206 final) and CoE European Ethical Charter on the use of Artificial Intelligence in the judicial system and their environment.

* PhD, Senior Research Fellow, ORCID: 0000-0003-1359-0276,
e-mail: *m.m.boskovic@roldevelopmentlab.com*

** The current paper is part of a research endeavour funded by the Ministry of Science, Technological Development and Innovation of the Republic of Serbia, conducted by the Institute of Criminological and Sociological Research, 2024, number 451-03-66/2024-03/200039.

In the article author assessed the implications of using artificial intelligence in the criminal justice system, particularly focusing on whether such use jeopardizes the right to a fair trial. The analysis is structured around key concerns and explores potential advancements and the influence of the proposed EU Regulation on AI.

Keywords: artificial intelligence, technology, fundamental rights, bias, criminal procedure.

1. INTRODUCTION

There are different definitions of artificial intelligence, but for this article, the most relevant is one provided in the European Parliament's legislative resolution on the Proposal for a Regulation on Artificial Intelligence (AI Act).[1] The European Parliament defines AI systems as: "*a machine-based system designed to operate with varying levels of autonomy, that may exhibit adaptiveness after deployment and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments*".[2]

In the theory, there are different categorizations of the AI technologies in the justice system. Sourdin makes a distinction between supportive, replacement and disruptive technologies (Sourdin, 2018, p. 1117). According to Sourdin, supportive technologies assist in enhancing online information services related to justice processes. They may involve platforms or systems that provide access to legal information, court schedules, case updates, and other relevant data. Replacement technologies, replace physical court proceedings with online alternatives, such as video conferencing tools for conducting hearings, trials, and other legal proceedings remotely. Disruptive technologies fundamentally change traditional legal processes and procedures and inform judges' decisions by applying prediction models or in some countries online dispute resolutions for low-value civil claims.[3] Reiling's categories include organization of information (i.e. the system used to organize and analyse vast amounts of data to recognize patterns and extract relevant information), provision of advice (i.e. chatbots, virtual assistants), and prediction of outcomes (predictive models) (Reiling, 2020, p. 8).

AI's capability to rapidly process and analyse large volumes of data presents significant opportunities for enhancing evidence-based decision-making (Baker & Robinson, 2021, p. 39). The advent of big data has revolutionised various sectors, including criminal justice. However, these advancements also raise unprecedented ethical and regulatory questions that need to be addressed to ensure the responsible and fair use of AI technologies.

---

1 European Parliament legislative resolution of 13 March on the Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, COM/2021/206 – C9-0146/2021 – 2021/0106(COD).

2 Article 3 of the Proposal for a Regulation on AI Act.

3 Small Claims Online – A Users Guide – Northern Ireland 2011. Available at: https://www.justice-ni.gov.uk/sites/default/files/publications/justice/small-claims-online-user-guide-v2.pdf (2. 10. 2024).

Due to the various uses of AI in the justice systems, the author structures the discussion according to the different phases of the criminal procedure, from investigation to sentencing and post-conviction phase. This approach allows for a clear understanding of how AI impacts each stage, from investigation to sentencing and beyond and identifies challenges in its application. Furthermore, the author evaluates how the new EU Regulation addresses the challenges associated with using AI in the criminal justice system, specifically ethical considerations such as privacy, bias, accountability, transparency, and the overall impact on fundamental rights.

2. USE OF ARTIFICIAL INTELLIGENCE IN CRIMINAL JUSTICE

In the context of criminal justice, AI can be applied in various ways to support the system (Quattrocolo, 2020, p. 3). The criminal justice system, particularly in the United States, has extensively integrated algorithmic and digital solutions across various phases of criminal proceedings. This integration impacts multiple aspects of the process, from investigation to sentencing and the execution of penalties and has the potential to enhance efficiency, accuracy, and fairness across various stages of criminal proceedings.

The European Union's structure and functioning, including the area of criminal law, have been significantly reformed after the Treaty of Lisbon, which entered into force on December 1, 2009. This Treaty marked a new era for EU criminal law by enhancing cooperation, harmonization, and integration across member states while upholding fundamental rights and the rule of law (Matić Bošković, 2021, p. 126).[4] The European criminal justice system is underpinned by a comprehensive framework of guarantees designed to ensure fairness, transparency, and protection of fundamental rights throughout criminal proceedings (Matić Bošković, 2022, p. 32). As computational modelling and artificial intelligence (AI) become more integrated into this system, it is important to identify the aspects of criminal justice that may be most closely affected (Quattrocolo, 2020, p. 23).

AI tools can enhance the efficiency and accuracy of collecting and analysing data during criminal investigations. Techniques such as facial recognition, data mining, and predictive analytics can expedite investigations and uncover patterns that might be missed by human investigators (Matić Bošković, 2020, p. 139). Tools such as predictive policing algorithms analyse data to forecast potential criminal activity and allocate police resources more effectively. For example, in crime detection, AI can analyse datasets to detect patterns indicative of fraudulent activities, helping to prevent and investigate financial crimes more effectively. As an example, there are machine learning algorithms used to detect anomalies in financial transactions, especially in the detection of money laundering, such as G.I.A.N.O.S. developed in Italy by the Italian Banking

[4] Article 83 TFEU (Treaty on the Functioning of the European Union) introduced the concept of 'Eurocrimes', enabling the EU to establish minimum rules concerning the definition of criminal offences and sanctions in areas of particularly serious crime with a cross-border dimension, such as terrorism, human trafficking, drug trafficking, and cybercrime. Article 82 TFEU facilitated judicial cooperation in criminal matters, allowing the EU to adopt measures for mutual recognition of judgments and judicial decisions, as well as cross-border cooperation.

Association (Costanzi, 2019, p. 8). The use of PredPol (Heaven, 2020), which predicts crime hotspots based on historical data, helps in strategic planning and crime prevention. The extensive use of data in criminal justice raises concerns about bias, privacy and data protection. Safeguarding individuals' personal information is essential to prevent misuse and protect civil liberties.

Related to judicial decision-making AI can assist judges by analysing past case law and identifying relevant precedents, streamlining the decision-making process and improving the consistency of judicial decisions. AI can assist judges by analysing past case law and identifying relevant precedents, streamlining the decision-making process and improving the consistency of judicial decisions. Specifically, legal research tools that utilize AI to quickly find relevant case law and legal principles. Risk assessment is one of the AI functionalities relevant to judicial decision-making (Bouchagiar, 2024, p. 76). Algorithms assist judges in making informed decisions regarding bail, sentencing, and parole by evaluating the risk of reoffending. These risk assessments are based on various data points, including criminal history, demographic information, and behaviour patterns. The Correctional Offender Management Profiling for Alternative Sanctions (COMPAS) algorithm, which is used to assess the risk of recidivism and inform sentencing decisions, exemplifies the application of AI in judicial processes (Brennan, Dieterich & Ehret, 2009, p. 21). The criticisms of COMPAS highlight significant concerns about racial bias and fairness in the use of AI in criminal justice. Although AI can help standardize sentencing by providing data-driven recommendations based on the specifics of the case and the defendant's background, algorithms can perpetuate existing biases in the data they analyse, leading to discriminatory outcomes (McDaniel & Pease, 2021, p. 46). Ensuring fairness and transparency in these systems is crucial to maintaining justice.

Concerning post-conviction monitoring, AI technologies can be used to monitor individuals on probation or parole, ensuring compliance with the terms of their release. Electronic monitoring systems can provide real-time data to authorities, such as GPS ankle monitors and automated reporting systems, which help ensure that offenders adhere to the terms of their release or probation (Matić Bošković & Kostić, 2019, p. 223).

AI systems can process information faster than humans, leading to quicker resolution of cases and investigations, while advanced algorithms can reduce human error, ensuring more precise outcomes in various criminal justice processes. By automating routine tasks, AI allows human resources to focus on more complex aspects of criminal justice. However, AI also brings up important ethical considerations such as data protection in the collection and processing of vast amounts of data, infringement of individual privacy rights by technologies like facial recognition, algorithmic bias in unfair risk assessments, and accountability for AI systems (Matić Bošković & Nenadić, 2021, p. 281). It is essential to ensure that these technologies are used in a manner that upholds the comprehensive framework of European guarantees, particularly those related to fair trial rights, privacy, non-discrimination, and transparency.[5]

[5] Article 6 of the European Convention on Human Rights (ECHR) guarantees the right to a fair trial, which includes the right to be heard, the right to an impartial tribunal, and the right to legal representation. The use of AI must align with these principles to ensure that defendants' rights are not compromised.

3. EFFORTS TO REGULATE THE USE OF ARTIFICIAL INTELLIGENCE IN EUROPE

Efforts to regulate the use of AI in Europe have been underway to address various concerns regarding ethics, accountability, transparency, and the protection of fundamental rights. The European Commission's Strategy on Artificial Intelligence for Europe adopted in April 2018 emphasizes the significance of AI for Europe's advancement and outlines steps to stimulate investments, promote data availability, and ensure inclusive digital transformation.[6] Following the Communication, the European Commission adopted the Coordinated Plan on Artificial Intelligence in December 2018, which outlines objectives such as fostering common efforts among Member States, promoting public-private practices, building the European data space, and enhancing understanding of AI security aspects.[7] The Commission's Communication on Towards a Common European Data Space emphasized the socio-economic benefits of data-driven innovation, including technologies like AI and the Internet of Things (IoT).[8] The 2019-2023 e-Justice Action Plan recognizes AI as a major development in ICT and emphasizes the need to further explore its implications in the field of justice.[9]

Some of the key initiatives and efforts to regulate the use of AI in the judiciary include the 2018 Council of Europe Commission for the Efficiency of Justice (CEPEJ) Ethical Charter on the use of AI in judicial Systems and their Environment,[10] Ethical Guidelines for Trustworthy AI prepared by the European Commission's High-Level Expert Group on IA in April 2019,[11] The European Parliament Resolution from October 2021, and the European Commission's Proposal for a Regulation on AI from April 2021.

The CEPEJ Ethical Charter on the Use of AI in Judicial Systems underlines the importance of responsible AI use, particularly in ensuring compliance with fundamental rights and data protection regulations. The proliferation of ethical principles surrounding the

---

Article 14 of the ECHR prohibits discrimination, thus AI systems must be designed and implemented in a manner that avoids biases and ensures equal treatment for all individuals, regardless of race, gender, or other protected characteristics. AI systems used in criminal justice must comply with the General Data Protection Regulation (GDPR), ensuring that personal data is processed lawfully, fairly, and transparently. This includes safeguarding against unauthorized access and misuse of data.

6 Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, *Artificial Intelligence for Europe,* 25 April 2018, COM (2018) 237 final.

7 Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, *Coordinated Plan on Artificial Intelligence,* 7 December 2018, COM (2018) 795 final.

8 Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, *Towards a common European data space,* 25 April 2018, COM (2018) 232 final.

9 2019-2023 Action Plan European e-Justice, OJ 2019/C 96/05.

10 CEPEJ, European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their Environment, adopted at the 31st plenary meeting of the CEPEJ, Strasbourg, 3-4 December 2018.

11 High-Level Expert Group on AI (AI HLEG), *Ethical Guidelines for Trustworthy AI,* 8 April 2019.

use of AI[12] Emphasizes the importance of addressing its implications in the administration of justice. The CEPEJ has developed five ethical principles specifically for AI use in the administration of justice, each aiming to uphold fundamental rights; non-discrimination; quality and security; transparency, impartiality and fairness; and under user control.

The fundamental rights principle emphasizes that the design and implementation of AI must be compatible with fundamental rights, as outlined in the European Convention on Human Rights and the Convention on the Protection of Personal Data.[13] It stresses the need to prioritize human rights considerations in the development and deployment of AI systems within the legal context. The Charter advocates for ensuring that users are informed actors and maintain control over the choices made by AI systems. This principle aims to empower individuals interacting with AI technologies, ensuring transparency and accountability in decision-making processes. Transparency, impartiality, and fairness principles should ensure that data processing methods are accessible and understandable. It also emphasizes the need for external audits to be authorized, promoting accountability and fairness in the use of AI within the judicial systems. Efforts should be made to avoid discrimination between individuals and groups, as evidenced by the risk illustrated by the COMPAS tools, where biased data or algorithms may preserve unjust distinctions. Users of AI algorithms must disclose the choice made, data used, and assumptions employed to ensure effective legal protection and judicial review. Users must understand and control AI algorithms' outcomes. AI should not dictate decisions, and users must be able to deviate from algorithmic outcomes easily, as demonstrated by the Loomis case,[14] where concerns were raised about the lack of transparency and control over the COMPAS tool's operation. Therefore, it is essential to implement rigorous oversight and accountability mechanisms to mitigate the risks.

The Ethical Charter acknowledges the diverse application of AI in the judicial context and encourages certain uses while advocating for a cautious approach and further research on other areas. The Charter supports certain uses of AI in the judiciary, including case-law enhancement by analysing and categorizing case-laws, access to law through AI chatbots, and the creation of strategic tools to analyse legal data. The Charter advises caution in certain AI applications, such as Online Dispute Resolution and recommends informing applicants whether their dispute resolution process is fully automated or involves human mediators, allowing them to make informed choices about their participation. Some uses of AI, such as judge profiling and anticipating court decisions, require further scientific research before widespread adoption. The Charter recognizes the sensitivity of individual profiling in the criminal justice context and anticipation of court decisions. It emphasizes the importance of ethical considerations and safeguards when using AI for profiling purposes, highlighting the potential impact on individual rights and due process.[15]

[12] UNESCO, (2021) Recommendation on the Ethics of Artificial Intelligence; OECD, (2019) Scoping the OECD AI Principles: Deliberations of the Expert Group on Artificial Intelligence at the OECD (AIGO).

[13] Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Dana, EST No. 108, as amended by the CETS amending protocol No. 223.

[14] *Loomis v. Wisconsin*, 881 N.W.2d 749 (Wis. 2016) 137 S. Ct. 2290 (2017).

[15] The Committee of Ministers of the Council of Europe adopted Recommendations Rec (2020)1 on the human rights impacts of algorithmic systems, along with Guidelines (Appendix to Recommendation

The Consultative Council of the Convention for the Protection of Individuals with regards to Automatic Processing, has recently issued new Guidelines on Artificial Intelligence and Data Protection to address the challenges posed by AI technologies to data protection and privacy rights.[16] The Guidelines emphasize the importance of ensuring that AI systems comply with data protection principles such as purpose limitation, data minimization, transparency, and accountability.

The European Commission established the High-Level Expert Group on AI (AI HLEG) in June 2018 to support the implementation of the Strategy AI for Europe. In its first year, the AI HLEG issued the Ethics Guidelines for Trustworthy AI, which outlines ethical principles and values essential for ensuring the trustworthiness of AI systems. The document emphasized that trustworthy AI can be achieved by adhering to seven key requirements: human agency and oversight; technical robustness and safety; privacy and data governance; transparency; diversity, non-discrimination and fairness; environmental and societal well-being; and accountability.[17]

The European Parliament also recognized the need to address AI issues and published the resolution on October 6, 2021.[18] The Resolution address various aspects of artificial intelligence in criminal law and its use by police and judicial authorities. While acknowledging the potential benefits of AI applications in law enforcement, members of the European Parliament (MEP) express concerns about the risks of bias, discrimination, and privacy violations associated with their use. MEPs advocate for strong measures to ensure data security, privacy and protection against unauthorized access to personal data. In addition, the Resolution insists on caution against blind reliance on AI, emphasizing the importance of human intervention in decision-making processes, especially in legal or judicial matters. MEPs call for a ban on the use of AI to propose judicial decisions, highlighting the limitations of predictive policing and the need for human judgment. The Resolution calls for a permanent prohibition on AI mass scale scoring of individuals, particularly by law enforcement authorities, citing concerns about autonomy,

Rec(2020)1 to enable member states to fulfil their obligations in this regard. The key recommendations and principles outline in these documents are revision of legislative framework to ensure compliance with applicable laws and regulations; setting up legislative, regulatory and supervisory mechanisms; engagement of members states in dialogue with all relevant stakeholders; to build expertise and promote digital literacy to enable better understanding of algorithmic systems. The Guidelines provide detailed guidance on data management, analysis, and modeling, transparency, accountability, effective remedies, precautionary measures, research, innovation, and public awareness, aiming to support member states in fulfilling their obligation and promoting the responsible and ethical use of algorithmic systems in alignment with human rights principles.

[16] Guidelines has been adopted on January 25, 2019. Available at: https://rm.coe.int/guidelines-on-artificial-intelligence-and-data-protection/168091f9d8 (1. 10. 2024).

[17] These requirements for trustworthy AI are further elaborated in the Communication of the Commission Building Trust in Human-Centric Artificial Intelligence, 8 April 2019, COM (2019) 168 final. This communication emphasised the importance of building trust in Ai systems prioritising human values, rights, and well-being, and promoting ethical and responsible AI development and deployment across Europe.

[18] European Parliament Resolution 2020/2016 (INI) Artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters.

non-discrimination, and fundamental rights. Additionally, MEPs express apprehension regarding the law enforcement and intelligence services' use of private facial recognition databases.

The European Commission's Regulation on AI Act is a significant legislative proposal aimed at regulating the development, deployment, and use of AI systems within the European Union. The AI Act seeks to establish a harmonised regulatory framework for AI systems across the EU, with the overarching goal of promoting trustworthy and ethical AI while ensuring the protection of fundamental rights, safety and security. The Regulation categorises AI systems into different risk levels based on their potential to cause harm (unacceptable risk, high risk and limited risk). AI systems classified as high risk must comply with specific requirements, such as ensuring the quality and integrity of training data and documentation; providing transparency about the capabilities, limitations, and purposes of the AI system; ensuring the accuracy, robustness and reliability of the AI system; implementing mechanisms for human oversight and intervention; and maintaining documentation and records to demonstrate compliance with regulatory requirements.

The European Commission has identified in the Annex of the proposal for a Regulation on AI Act certain AI systems used in the administration of justice as high risk due to their potential to cause considerable harm to fundamental rights, such as the right to a fair trial and effective remedy, as result of issues like opaqueness and unfair bias. These high-risk AI applications include systems that assist judicial staff in researching, interpreting facts and the law, and applying the law to specific cases. However, systems not directly linked to adjudication, such as those involving anonymization of judgements or document handling, are not considered high-risk.

In response to these concerns, the European Union is prioritizing the regulation of AI systems for courts throughout their design, development, and use stages. The aim is to create trustworthy applications that can be safely employed by court users without jeopardizing their rights. This involves establishing binding standards and regulations to ensure transparency, fairness, and accountability in the development and deployment of AI systems within the judicial system. However, there are examples from other non-EU countries where the lack of adherence to binding standards has compromised litigants' rights, despite significant investment in the research and development of AI solutions. As it is mentioned COMPAS has faced challenges related to bias. The algorithm excluded race to prevent bias but left the poverty rate, which also led to bias (Angwin *et al*.,, 2022, p. 270). The COMPAS example highlights the need for constant monitoring of AI solutions and its result, to enable immediate action if there are challenges in application.

4. CONCLUSION

The integration of AI into the criminal justice system has the potential to significantly enhance the efficiency, quality and predictability of various phases of the criminal procedure. However, it also raises several concerns, particularly regarding fundamental rights such as the right to a fair trial, personal data protection, and issues of discrimination and biases.

The opaque nature of many AI algorithms can undermine the transparency required for a fair trial, so defendants may not understand how an AI system reached its conclusions, limiting their ability to challenge potentially biased or inaccurate results. The extensive use of personal data in AI systems can pose significant privacy risks, especially if data is not adequately protected. AI systems that aggregate and analyse data from multiple sources may inadvertently expose sensitive personal information.

The draft Regulation on AI adopted by the European Parliament represents a significant step towards establishing a comprehensive legal framework for AI in the EU. By classifying AI systems, particularly those used in critical areas like criminal justice, as high-risk and subjecting them to stringent requirements, the Regulation aims to ensure that AI technologies are developed and used in ways that are safe, fair, and trustworthy. The emphasis on transparency, accountability, and human oversight reflects the EU's commitment to protecting fundamental rights while fostering innovation and competitiveness in the AI sector.

Specifically, the draft Regulation emphasizes the importance of fairness and non-discrimination in AI applications, particularly in criminal justice. AI systems must be designed and used in ways that prevent bias and discrimination. Regular audits and assessments are required to ensure that AI systems comply with these principles. According to the draft Regulation AI systems in criminal justice must be subject to human oversight to ensure that decisions made by or with the assistance of AI are fair and just, while accountability mechanisms must be established to address any errors or misuse of AI systems in criminal justice. The draft Regulation mandates that AI systems in criminal justice be transparent and explainable. This means that decisions made by AI must be understandable to the affected individuals and the public. Clear documentation and communication are required to ensure that users and stakeholders are aware of how AI systems operate and the basis for their decisions.

The draft AI Regulation by the European Union is anticipated to play a crucial role in ensuring the safe and ethical use of AI in the criminal justice system. The draft Regulation is designed to address several key concerns and provide a comprehensive framework for the responsible deployment of AI technologies.

LIST OF REFERENCES

Angwin, J., Larson, J., Mattu, S. & Kirchner, L. 2022. Machine Bias. In: Martin, K. (ed.) *Ethics of Data and Analytics : Concepts and Cases.* Auerbach Publications, pp. 264-275. https://doi.org/10.1201/9781003278290-37

Baker, D. & Robinson, P. H. 2021. *Artificial Intelligence and the Law – Cybercrime and Criminal Liability*. London: Routledge, Taylor and Francis Group. https://doi.org/10.4324/9780429344015

Brennan, T., Dieterich, W. & Ehret, B. 2009 Evaluating the predictive validity of the COMPAS Risk and Needs Assessment System. *Criminal Justice and Behavior*, 36(1), pp. 21-40. https://doi.org/10.1177/0093854808326545

Bouchagiar, G. 2024. Is Europe prepared for Risk Assessment Technologies in criminal justice? Lessons from the US experience. *New Journal of European Criminal Law*, 15(1), pp. 72-98. https://doi.org/10.1177/20322844241228676

Costanzi, C. 2019. Big data e garantismo digitale. Le nuove frontiere della giustizia penale nel XXI secolo, Giustizia penale e nuove tecnologie. *La Legislazione Penale*, (12), pp. 1-16. Available at: https://www.lalegislazionepenale.eu/wp-content/uploads/2019/12/Costanzi_GP-nuove-tecnologie-LP_Rev.pdf (1. 10. 2024). https://doi.org/10.3280/MG2018-001002

Heaven, W. D. 2020. Predictive policing algorithms are racist. They need to be dismantled. *MIT Technology Review.* Available at: https://www.technologyreview.com/2020/07/17/1005396/predictive-policing-algorithms-racist-dismantled-machine-learning-bias-criminal-justice/ (1. 10. 2024).

Matić Bošković, M. 2022. *Krivično procesno pravo EU*. Beograd: Institut za kriminološka i sociološka istraživanja.

Matić Bošković, M. 2021. Impact of Modern Technologies on Free Movement of Evidence in European Union. *Journal of Criminology and Criminal Law*, 59(3), pp. 123-140. https://doi.org/10.47152/rkkp.59.3.6

Matić Bošković, M. & Nenadić, S. 2021. Impact of COVID-19 Pandemic on Criminal Justice Systems Across Europe. In: Duić, D. & Petrašević, T. (eds.), *EU 2021 – The Future of the EU in and After the Pandemic*. Osijek: Faculty of Law, University of Osijek, pp. 263-290. https://doi.org/10.25234/eclic/18307

Matić Bošković, M. 2020. Implications of New Technologies on Criminal Justice System. *Journal of Eastern-European Criminal Law*, 2, pp. 137-147.

Matić Bošković, M. & Kostić, J. 2019. Kućni zatvor: iskustva u primeni. In: Bejatović, S. (ed.), *Izmene u krivičnom zakonodavstvu i statusu nosilaca pravosudnih funkcija i adekvatnost državne reakcije na kriminalitet (međunarodni pravni standardi i stanje u Srbiji). LIX redovno godišnje savetovanje udruženja. Srpsko udruženje za krivično-pravnu teoriju i praksu*. Beograd: Intermex, pp. 216-229.

McDaniel, J. L. M. & Pease, K. G. 2021. *Predictive Policing and Artificial Intelligence*. New York: Routledge, Taylor and Francis Group. https://doi.org/10.4324/9780429265365

Reiling, A. D. 2020. Courts and Artificial Intelligence. *International Journal for Court Administration*, 11(2), pp. 1-10. https://doi.org/10.36745/ijca.343

Sourdin, T. 2018. Judge v Robot? Artificial Intelligence and Judicial Decision-Making. *University of New South Wales Law Journal (UNSWLJ),* 41(4), pp. 1114-1133. https://doi.org/10.53637/ZGUX2213

Quattrocolo, S. 2020. *Artificial Intelligence, Computational Modelling and Criminal Proceedings – A Framework for A European Legal Discussion*. Berlin: Springer. https://doi.org/10.1007/978-3-030-52470-8

UDC: 314.15:351.86 DOI: 10.56461/iup_rlrc.2024.5.ch9

*Vladimir MIKIĆ**
Institute of Comparative Law, Belgrade, Serbia

WEAPONIZED MIGRATION AS A TOOL OF CLANDESTINE AGGRESSION IN CONTEMPORARY INTERNATIONAL LAW**

Although the crime of aggression is expressly defined by the Rome Statute of the International Criminal Court through seven criminalized types of activities, it seems that a special form of aggression has begun to appear as a new instrument of influence in international relations. Namely, several states have been exercising a particular tool of aggression: causing a swift influx of migrants or refugees into neighboring countries, in order for the latter to be politically or economically destabilized.

Even if "indirect" aggression, such as spy-flights over foreign territory, is a well-known, though illegal, practice in international relations, aggression by the means of using migrants contains a special new component—unarmed human beings (and with foreign nationality) being forced to cross national borders, unwillingly taking risks of being inhumanely treated or physically endangered by the other side as well. Also named "refugee aggression," this type of illicit activity of a state or its agents can cause severe political and security effects by a mere threat that it will be carried out.

Keywords: migration,aggression, hybrid warfare, international law.

1. INTRODUCTION

One of the most iconic characters in the history of cinematography is Antonio "Tony" Montana, more or less impressively portrayed by the young American actor Al Pacino.

Tony is a refugee originally from Cuba, with a criminal background, but also awkwardly distinguished by an honest and brave character. Claiming that he had long been forced to work for free within the confines of an inhumane and authoritarian regime,

* PhD, Research Associate, ORCID: 0009-0001-8706-4175, e-mail: v.mikic@iup.rs

** This paper is a result of the research conducted at the Institute of Comparative Law financed by the Ministry of Science, Technological Development and Innovation of the Republic of Serbia under the Contract on realisation and financing of scientific research of SRO in 2024 registered under no. 451-03-66/2024-03/200049.

Tony, as it turns out, brought with him into the asylum state, the United States of America (USA), some dangerous habits inherited from his previous life. The host country hardly profited from his presence at its soil, and at the end of the movie (probably not a spoiler alert), it turns out that Mr. Montana didn't live his short life the way he planned. A potential implicit conclusion is that only the Cuban regime benefited from the whole story.

The opening scenes of "Scarface" (directed by Brian de Palma in 1983) are dedicated to the 1980 *Mariel Boatlift*, a mass migration movement during which the Cuban dictator Fidel Castro coerced Jimmy Carter administration of the USA "into foreign policy concessions after sending more than 100,000 Cuban migrants, including criminals and the mentally disabled, to Florida" (Steger, 2017, p. 1). One of them, at least in fiction, was Tony. Not many people knew in 1980 (or at the time of the distribution of the movie) that *weaponized migration* would in fact turn out to be a new, special form of aggression, notably distant from classical types of breaches of international law. More movies on the subject will be directed (or not), but the weaponizing of migrants *in real life* is here to stay (although the Microsoft Word still puts the notion through the spell-checking mechanism, even in 2024).

Instrumentalization of migration crisis is not particularly new method which international actors use, but it catches new sorts of attention. Yet, the accelerated pace of its use (or *threat* of its use) manifests that many authoritarian regimes will not fail to discover its damaging potential. In the aftermath of the Belarus refugee crisis,[1] *even* such a developed and influential international actor as the European Union (EU) was, in 2021, "unprepared for such a vicious game where displaced people were used as pawns in a coercive geopolitical strategy" (Miholjčić, 2022, p. 7).[2] Greenhill, who has coined the phrase of "weaponized migration" (Başer, 2022, p. 169; Schoemaker, 2019, p. 364), sees this hybrid weapon, aimed at producing, sustaining, or deepening political instability, as nothing less than a "new crime of refugee aggression" (Greenhill, 2022, p. 157). State-sponsored influxes of refugees create an additional threat to international security, particularly on the borders of the EU,[3] which is already going through the process marked by serious institutional problems and political upheavals, owing a lot to demagoguery and xenophobia (practically because of the practical non-existence of state borders in the EU). Apart from traditional military incursions or other conventional types of influencing foreign states, weaponized migration violates the international law

[1] "In the fall of 2021, the leaders of several European countries announced that they were being confronted by an entirely new security threat: weaponized migration" (Greenhill, 2022, p. 155).

[2] The EU, however, reacted soon. "A highly worrying phenomenon observed is the increasing role of State actors in artificially creating and facilitating irregular migration," as is stated in the European Commission adopted in December 2021 the "Proposal for a Regulation of the European Parliament and of the Council addressing situations of the instrumentalization in the field of migration and asylum" (the 2021 Proposal). Belarus "showed how little Western governments (…) understand the tactic and the ways it plays on the inherently contradictory and hypocritical politics surrounding migration in many advanced democracies" (Greenhill, 2022, p. 157)

[3] "More and more governments may seek to turn migrants and asylum seekers "into bullets," as the political scientist Mark Leonard warned— especially to target the EU, a coveted destination that is surrounded by impoverished, repressive and unstable states" (Greenhill, 2022, p. 156).

in new, hardly conceivable but dangerously risky ways. Migration exploitation has risen to become a "very important modern foreign policy instrument" in the international relations (Miholjčić, 2022, p. 3).

At the beginning of the paper types of abuses of refugees and migrants by the state and non-state actors are presented, mapping a true trend present throughout the globe. Next, objectives of weaponized migration are exposed, regardless of whether political, military, or economic motives are in place. Before concluding remarks are summarized, the fourth part of the paper summarily deals with normative framework on the weaponized migration.

2. TYPES AND EXAMPLES OF WEAPONIZING THE REFUGEES AND THE MIGRANTS

Purposely displacing people over borders for political aims can be defined in various ways. It "refers to those instances in which a perpetrating actor attempts to exert power by strategically creating or exploiting migration outflows, threatening to overwhelm the capacity of the target state to accommodate the inflow and to destabilize the target state" (Sie Dhian Ho & Wijnkoop, 2022, p. 1), or to "the creation, exacerbation, or instrumentalization of people" (Petty, 2022, p. 134). Weaponized migration, from one point of view, occurs when a challenging state or non-state actor exploits human migration—whether voluntary or forced—in order to achieve political, military, and/or economic objectives" (Steger, 2017, p. 6). In accordance with one rather extensive categorization, there exist no less than seven types of weaponization of migrants: "the coercive, dispossessive, extortive, economic, fifth-column, militarized, and political/propaganda variants" (Başer, 2022, p. 170).

From only the recent historical point of view, there have been more than a bunch of examples of engineered migration and refugee crises. An authoritative author identified more than 80 cases of resorting to the tactic since the adoption of the Convention Relating to the Status of Refugees (the 1951 Convention) (Greenhill, 2022, p. 157). Probably the earliest noted cases included Pakistan creating conditions for "refugee aggression" against India in 1978, from what was then East Pakistan (nowadays the country's name is Bangladesh), while the Libyan leader Muammar al-Qaddafi in his time threatened the EU to "turn Europe black" and "Muslim" if Libya does not receive financial assistance (Greenhill, 2022, p. 159; similarly: Başer, 2022, p. 170). In the 1980s, Thailand hosted a quarter million Cambodian refugees, using them as a human buffer zone to protect itself in the ongoing conflict with Cambodia (Başer, 2022, p. 177), and, in the 1990s, the Albanian government threatened to do the similar thing against the interests of Italy (Greenhill, 2022, p. 158). President of Haiti Jean-Bertrand Aristide persuaded the US in 1994 "to reinstall him in office in part by threatening to mobilize large numbers of Haitians to "take to the sea" and head for the [US]" (Greenhill, 2022, p. 158). Back in 2007, "Iran exported 80,000 Afghans in protest to Afghan President Hamad Karzai allowing an official NATO presence in Afghanistan" (Başer, 2022, p. 175), and has since continued to threaten its Afghan refugee population with expulsion (Steger, 2017, p. 8).

More recent examples of employing this type of unconventional means of influencing international relations include activities in which the authorities of Belarus, Russia, and Turkey were engaged.

In 2021, Belarus artificially generated a migrants' crisis in the border areas with Latvia, Lithuania, and Poland (Miholjčić, 2022, p. 3). Belarus announced that it will allow migrants to enter more easily its territory than earlier, liberalizing its visa regime, organizing the migrants' entry, and financing their accommodation and transport to its western borders (Sie Dhian Ho & Wijnkoop, 2022, p. 20). In response, the three endangered EU countries declared a state of emergency and deployed army forces on their borders with Belarus (Miholjčić, 2022, p. 7), while Poland and Finland introduced new emergency legislation as a response to possible further similar threats (Sie Dhian Ho & Wijnkoop, 2022, p. 32).

Russia was also accused of forcibly sending migrants into its neighbouring European countries, maybe as a part of a deliberate strategy (Schoemaker, 2019, p. 361). It has also been suggested that Russia intentionally targeted civilians in Ukraine since February 2022 to influence the political situation in the EU (Petty, 2022, p. 113), in order to provoke "hybrid instrumentalized migration" (Sie Dhian Ho & Wijnkoop, 2022, p. 21). This was also the main point of the accusation made in 2016 by General Philip Breedlove, head of NATO forces in Europe, who accused Russia of working actively to exacerbate the refugee flows in an attempt to destabilize and destroy the EU (Schoemaker, 2019, p. 361).

Finally, the world witnessed the 2020 migration crisis on the Greek-Turkish border, when during a single month there were more than 50,000 registered attempts to enter the territory of Greece illegally. According to one study, most of the migrants did not come from Syria, but from Afghanistan, Pakistan, Somalia and sub-Saharan countries, and they "have lived in Turkey for years, as their knowledge of Turkish language shows" (Kotoulas & Pusztai, 2020, pp. 6-7), which implied a classic example of an engineered migration.

3. OBJECTIVES OF REFUGEE AGGRESSION

Intentions of state actors resorting to weaponized migration are not always identical. They may range from financially-motivated activities to raising levels of terrorist threats, provoking political instability and threatening liberal and democratic order of target states, obtaining national military objectives, or framing the most efficient ambient for enabling authoritarian regimes to stay in power.

Financial (economic) extortion appears to be the first motive for abusing the vulnerable position of displaced people by means of weaponized migration. Mechanisms for extracting political or economic concessions can be noted in several examples. In its negotiations with the EU in 2016, Turkey succeeded in its financial demands by "utilizing the fear of a new refugee influx" into the EU (Miholjčić, 2022, p. 4; similar conclusions are drawn by: Kotoulas & Pusztai, 2020, p. 11). Turkey threatened to lease the migrants from the Middle East "unless Brussels provided certain concessions", which resulted in Turkey receiving promises of ample financial assistance, a revival of talks on the accession of the country to the EU, as well as visa-free travel for citizens of that

country (Greenhill, 2022, p. 159). The agreement concluded with the EU was "a direct result of the dramatic mass migration event of 2015" which meant that, "according to the deal Turkey continues to receive generous EU funding," assuming "the obligation of stopping the mass influx in Europe" (Kotoulas & Pusztai, 2020, p. 10). Indeed, the Turkish government was "able to use Syrian refugees as a bargaining chip in extracting billions in payments and political concessions from the EU" (Petty, 2022, p. 122). Extracting aid from wealthy targets had also presumably been the main course of action by other actors. Thus, "the Moroccan government`s financial and political pressure on Spain to solve illegal border crossings" (Miholjčić, 2022, p. 3), whilst the Belarusian President of the Republic publicly proclaimed in 2002 and 2004 that, "if the Europeans don't pay, we will not protect Europe from these flows" (Greenhill, 2010, p. 118).

Potential terrorist infiltration is another objective of coercive actors in the field of weaponizing migrants. This goes on by the means of "terrorism by violent extremist organizations creeping into migration and refugee flows and conducting terrorist attacks in the country of asylum under the guise of refugee status" (Başer, 2022, p. 170), and by "efforts (…) to infiltrate refugee flows and to facilitate terrorist operations in states offering asylum" (Steger, 2017, p. 1). Furthermore, terrorist attacks in Europe "have implanted a daunting idea that potential terrorists might penetrate the EU territory using the migration influx" (Miholjčić, 2022, p. 4).

Strategic engineered migration can also be motivated by the idea of threatening democratic model of government of target states, while, in addition, it may serve to merely weaken these states politically. Such is the case with "the attempts (…) threatening to overwhelm the capacity of the target state to accommodate the inflow and to destabilize the target state" (Sie Dhian Ho & Wijnkoop, 2022, p. 5), particularly because surveys demonstrate that migration have obtained the status of "a highly politically salient issue in potential target countries" (Sie Dhian Ho & Wijnkoop, 2022, p. 13). In addition, "influencing public opinion and destabilizing society are not side effects but rather central objectives of the perpetrating actor, in cases of instrumentalized migration crises" (Sie Dhian Ho & Wijnkoop, 2022, p. 18). Weaponizing migration can also raise interstate and international (regional) distrust, and thus endanger the genuine national security interests of neighbouring countries. It can "create instability in border areas" (Kotoulas & Pusztai, 2020, p. 13), as, for example, Belarus sought to "discomfit, humiliate, and sow division within the EU" by its actions in the 2021 crisis (Greenhill, 2022, p. 155).

Forced migration is also aimed at provoking anti-immigration sentiments. Thus, "challengers [can seek] to influence the behaviour of potentially vulnerable targets disinclined to accede to their demands under normal circumstances—powerful advanced liberal democracies" (Greenhill, 2010, p. 123). By strategically creating these migration outflows, the perpetrators aim to weaken and destabilize the target country, create unrest and popular dissatisfaction, and erode the power base of the target government (Sie Dhian Ho & Wijnkoop, 2022, p. 9). The immigration has for long been seized upon as a particularly attractive issue by far-right political options throughout the world. It can be claimed that, in a particularly cunning way, weaponized migration might "trigger more restrictive immigration policies within the [EU] and thus call in question the

fundamentals of liberal democratic ideology and tolerance entrenched in the core of the EU`s existence" (Miholjčić, 2022, p. 2; similar: Greenhill, 2022, p. 158). Thus, refugee aggression deliberately endangers the very core of the political visions of a targeted society, creating and strengthening xenophobic sentiments at the same time.[4] This happens because "accepting large numbers of refugees *en masse* is often a politically charged and domestically divisive issue" (Petty, 2022, p. 114-115), while "the most heated debate concerning migrant control is over the constitutionality of repressive measures" (Turanjanin, 2023, p. 411). Mass migrations can serve as a tool of foreign policy, constituting an important component of *migration diplomacy* (Kotoulas & Pusztai, 2020, p. 14; Sie Dhian Ho & Wijnkoop, 2022, p. 2), notably because intensifying diplomatic discord with foreign (neighbouring) countries is in the interest of populist authoritarian governments.

Secondary military objectives can also be achieved by introducing weaponized migration into the arena of foreign relations (Steger, 2017, p. 5). Quasi-aggressive actors can thus "check the operational readiness and abilities" of a potential adversary, which "functions as a simulation of war" (Kotoulas & Pusztai, 2020, p. 13). As for a historical example, "in the early 1980s, the Pakistani leader Muhammad Zia-ul-Haq agreed to continue to host three million Afghan refugees then residing in Pakistan (…) in exchange for a variety of concessions from Washington, including the cessation of U.S. opposition to Pakistan's nuclear weapons program" (Greenhill, 2022, p. 158). The Turkish government have recently used the similar method, *inter alia*, to gain "tacit approval for its military interventions in northern Syria" (Miholjčić, 2022, p. 3).

Refugee aggression can be aimed at maintaining repressive regimes in power, serving at the same time as an unconventional tool of political retaliation. Such was the case with the Moroccan government very recently, which enticed "thousands of people [smuggled into Spain following] the news that a Spanish hospital had accommodated the Polisario Front's leader, Brahim Ghali, for COVID-19 treatment." An enormous influx of refugees was "a result of an increasing diplomatic tension between Madrid and Rabat over the question concerning Western Sahara status," and Moroccan officials were irritated by the Spanish decision to hospitalize the leader of a rebel group fighting for the independence of Western Sahara from Morocco and responded with opening fences to the Spanish enclave" (Miholjčić, 2022, p. 5). Similarly, by staging the refugee crisis of 2021, "the Belarus regime wanted to punish the EU for previously imposed sanctions and concurrently discourage them from further sanctioning" (Miholjčić, 2022, p. 8).

4. LEGAL FRAMEWORK ON THE WEAPONIZED MIGRATION

International regulation of immigration weaponization is not quite missing, although the subject remains an "ungoverned domain" from the international law perspective (Petty, 2022, p. 128). The 1951 Convention, and its 1967 Protocol Relating to the Status of Refugees both define a state's obligations and responsibilities towards protecting refugees

[4] "The Belarusian engineered crisis included around several thousand people, which is an insignificant fraction of overall EU asylum statistics, however, the distress effect that migration influx has on communities within the bloc presents a bigger issue than the figures themselves" (Miholjčić, 2022, p. 9).

on their territory. The right to liberty and security of person is also guaranteed by Art. 6 of the Charter of Fundamental Rights of the EU, while Art. 15 of the European Convention for the Protection of Human Rights and Fundamental Freedoms states that "in time of war or other public emergency threatening the life of the nation any High Contracting Party may take measures derogating from its obligations under this Convention to the extent strictly required by the exigencies of the situation, provided that such measures are not inconsistent with its other obligations under international law." However, the core principle underlying the 1951 Convention (Art. 33) and its Protocol is the *non-refoulement principle* (Başer, 2022, p. 173; Turanjanin, 2023, p. 413). Namely, Art. 33 ensures that no Contracting State shall expel or return (*refouler*) a refugee to any territory where his (her) life or freedom would be threatened in a discriminatory fashion.

Weaponized migration represents a novel domain of the law of the war. As such, it cannot easily be treated under the law of armed conflict, partly because "principles of the laws of war that were set down in an era that could not possibly have considered the ways in which states now compete against each other" (Petty, 2022, p. 116). It may be assessed as an indirect aggression, out of the scope of the right of a state to resort to armed force, guaranteed by Art. 2 Para. 4 of the Charter of the United Nations. Traditionally, as a notorious form of proscribed behavior, aggression refers, in broad terms, "to an illegal, unjustified, improper or immoral attack or intervention by one state, or its agents, upon another" (Evans & Newnham, 1998, p. 10).

However, as a tool of warfare, weaponized migration "is far closer to bombs and bullets than to electronic jamming or dropping leaflets" (Petty, 2022, p. 134). For example, massive influx of migrants from Turkey into Greece in March 2020 represented nothing less than "outright violation and state aggression against Greece and the EU" (Kotoulas & Pusztai, 2020, p. 11). Comparably, Ylva Johansson, EU Commissioner for Home Affairs strongly suggested in 2021 that the Belarusian refugee strategy represented a novel way of "using human beings in an act of aggression" (Greenhill, 2022, p 156). Within the same context, the President of the European Commission Ursula von der Leyen "described the situation as 'not a migration crisis', but as a 'hybrid attack'" (Petty, 2022, p. 114).

One of the sources for making a legally appropriate estimation on whether weaponized migration is in fact aggression is the Rome Statute of the International Criminal Court of 1998 (the Rome Statute). Its Art. 8bis Para. 2 Sect. "g" explicitly states that one of the types of aggression is represented by "sending by or on behalf of a State of armed bands, groups, irregulars or mercenaries, which carry out acts of armed force against another State of such gravity as to amount to the acts listed above, or its substantial involvement therein." The same list of activities—including the *ad verbum* wording of the Sect. "g"—is outlined by the Art. 3 of the United Nations General Assembly Resolution No. 3314 (XXIX), adopted in 1974. Thus, no direct link is formally established between *aggression* and *refugee aggression*.

It may be useful to remind that, in the boundaries of international criminal law, *criminal intent* (*mens rea*) is necessary for establishing criminal responsibility (Art. 30 of the Rome Statute). Thus, in order to establish a solid case of "weaponized migration," intentional refugee flows should not be a side effect, but a clear, specific intent

additional to the general intent of harming non-combatants through indiscriminate targeting (Schoemaker, 2019, p. 371). In the current state of the international legal framework, weaponized migration cannot be clearly identified with aggression in the sense of international public law, or international criminal law (humanitarian law).

Certain authors have proposed suggestions to improve the current sorrowful normative state of affairs. On one side of the line of arguments, a mechanism (although politically less attractive and therefore not much probable), is to be developed to create policies aiming at "accommodating and integrating the migrants," which could create "a window of opportunity for the EU to continue developing more effective asylum and integration systems rather than an occasion to waste resources on border fortifying and detention systems" (Miholjčić, 2022, pp. 8-9). Similarly, particular states should construct "sustainable migration partnerships with third countries (...) to find the collective will to conceptualize, build and defend fortresses with *gates*" (Sie Dhian Ho & Wijnkoop, 2022, p. 3). Another liberal-minded research claims that "an effective response of potential target states requires (…) a collective identity, involving: (1) raising public awareness; (2) collective will and narrative power; (3) countering disinformation; and (4) mobilizing international allies (Sie Dhian Ho & Wijnkoop, 2022, p. 38). In addition, it is necessary "to invest in information campaigns and other preventative community measures" which can "raise awareness among potential migrants that they should be suspicious of promises of perpetrators that they can help them enter the target country and inform them that institutions to deal with instrumentalization of migration are in place and effective" (Sie Dhian Ho & Wijnkoop, 2022, p. 26). On the other hand, there is a conservative call for a wake-up in the direction of firmly resisting refugee aggression. Hence, the *deterrence* line of thought suggests that "if competitors know that [weaponized migration] will be held out as a violation of the law of war and that as a type of "armed attack", it may legitimately provoke retaliation, they may be less likely to engage in this sort of conduct in the first place" (Sie Dhian Ho & Wijnkoop, 2022, p. 116).

5. CONCLUDING REMARKS

As long as "there are more people in the world who want to leave their countries than there are other countries willing to accept them" (Petty, 2022, p. 123), exporting migrants will be a powerful type of quasi-aggression. Put quite bluntly by the cited General Breedlove, weaponized migration remains an action basically concentrated on actions aimed "to get people on the road and make them someone else's problem" (Schoemaker, 2019, p. 362).

However, combating irregular migration as a warfare instrument needs to be based on perfecting international legal regimes in the direction of creating a more efficient definition of aggression (violation of any given country's sovereignty). Due to the fact that it represents a new type of covert violation of the political and economic integrity of a sovereign country, aggression conducted by the weaponization of migrants or refugees cannot be easily identified. The omission of refugee aggression in the Rome Statute is historically relatively understandable, but this legal gap must be filled. The basic concern remains that the mentioned type of aggression appears to be gaining momentum, which may bring excessive dangers to international security.

In the field of refugee aggression, a porous legal context—or, to put it in a more direct way, a true *vacuum*—merely attracts new dangers. In particular, engineered migration can be perilous for the very survival of smaller countries, in which "migrant flows of significant size could be perceived as a threat to cultural or the social fabric of the country, regardless of any potential economic benefit or humanitarian imperative" (Petty, 2022, p. 126). Such is the case with Lebanon, which has approximately six million inhabitants but hosts over a million of Syrian refugees (Schoemaker, 2019, p. 365), and this example could easily be applied anew in any smaller country in Europe, or elsewhere. There will hardly be any space for extended patience if the weaponized migration becomes directly confronted with a more electrified international atmosphere. In this field, as in any other, time is of the essence.

LIST OF REFERENCES

Başer, S. 2022. The Most Insidious Weapon of the Changing World: Migration. *Bilge Strateji*, 13(24), pp. 167-185. https://doi.org/10.35705/bs.1198447

European Commission. 2021. Proposal for a Regulation of the European Parliament and of the Council addressing situations of the instrumentalization in the field of migration and asylum. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2021%3A890%3AFIN&qid=1639757068345 (10. 10. 2024).

Evans, G. & Newnham, J. 1998. *The Penguin Dictionary of International Relations*. London: Penguin Books.

Greenhill, K. M. 2022. When Migrants Become Weapons: The Long History and Worrying

Future of a Coercive Tactic, *Foreign Affairs*, 101(2), pp. 155-165.

Greenhill, K. M. 2010. Weapons of Mass Migration: Forced Displacement as an Instrument of Coercion. Strategic Insights, 9(1), pp. 116-159. https://doi.org/10.7591/9780801458668

Kotoulas, I. E. & Pusztai, W. 2020. *Migration as a Weapon: Turkey's Hybrid Warfare Against the European Union, Foreign Affairs Institute - Report No. 1*. Athens: Foreign Affairs Institute.

Miholjčić, N. 2022. Migration as an Instrument of Modern Political Warfare: Cases of Turkey, Morocco and Belarus. *Jean Monnet Network on EU Law Enforcement - Working Paper Series,* 12/22, pp. 1-12.

Rome Statute of the International Criminal Court. 1998. Available at: https://www.icc-cpi.int/sites/default/files/2024-05/Rome-Statute-eng.pdf (10. 10. 2024).

Schoemaker, H. 2019. Allegations of Russian Weaponized Migration Against the EU: With the Blackest Intention? *Military Spectator*, 7/8, pp. 361-373.

Steger, N. D. 2017. *The Weaponization of Migration: Examining Migration as a 21st Century Tool of Political Warfare*. Thesis. Monterey: Naval Postgraduate School.

Petty, A. R. 2022. Migrants as a Weapons System. *Journal of National Security Law and Policy*,13, pp. 113-139.

Sie Dhian Ho, M. & Wijnkoop, M. 2022. *The instrumentalization of migration: A geopolitical perspective and toolbox*. Hague: Clingendael – Netherlands Institute of International Relations.

Turanjanin, V. 2023. Migrants and Safety in Serbia During and after Corona Virus Pandemic. *EU and Comparative Law Issues and Challenges Series (ECLIC)*, 6, pp. 410-429. https://doi.org/10.25234/eclic/22437

United Nations General Assembly. 1951. The Convention Relating to the Status of Refugees. Available at: https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-relating-status-refugees (10. 10. 2024).

United Nations General Assembly. 1974. Resolution No. 3314 (XXIX). Available at: https://legal.un.org/avl/ha/da/da.html (10. 10. 2024.)

UDC: 343.14(450) DOI: 10.56461/iup_rlrc.2024.5.ch10

Marco CECCHI*
Faculty of Law, eCampus University & University of Florence, Italy

REINFORCED REASONING ON A-TYPICAL EVIDENCE. AN ANALYSIS BASED ON THE ITALIAN EXPERIENCE

The atypical evidence (i.e. the evidence not regulated by law) is a kind of evidence that assumes relevance in the Italian system, when – but not only – the process concerns technological innovations or instruments (e.g. videotaping, tracking by GPS, secret agent equipped for sound, trojan virus, AI tools etc.).

A way to manage this peculiar evidence into the judgement is reinforced reasoning. In every juridical situation where this method is feasible, the judge has to adopt a decision technique structured by necessary steps, made up of arguments concerning salient aspects of the case/evidence under his examination and which must be appreciated in order to decide legitimately. These logic-argumentative passages increase the epistemological quality and the transparency of the assessment: and, overall, the value of the pronouncement.

In particular, in front of atypical evidence, the decision maker has to cross three different steps – elaborated by jurisprudence and doctrine – to achieve the right conclusion: and this is precisely what we're going to analyse in the paper.
Keywords: evidence, reinforced reasoning, judgement, tehnological innovations, legitimacy.

1. A-TYPICAL EVIDENCE WITHIN THE ITALIAN CRIMINAL LAW SYSTEM

In Italy, the Criminal Procedure Code – CPC outlines two types of evidence: typical evidence and a-typical evidence. The difference is that the first one is completely regulated by law, while the second one is not legally defined in all its aspects but only in its essential features of legitimacy (*viz.* the legislator delimits solely the *an*, leaving open the *quomodo*).

Jurists have discussed for a long – and, regarding the correct encasing of new technological evidentiary, all today they still argue case by case (*i.e.* new technology by new technology) – about the exact definition of these two categories. Belonging to either category has significant consequences in terms of admissibility and exclusion/usability of evidence in the proceedings.

* PhD, Researcher, ORCID: 0000-0002-7335-2029, e-mail: *marco.cecchi@uniecampus.it*

To be clear, let me give an example. We can talk about identification or recognition. Arts. 213-217 CPC determine how this kind of evidence must be assumed, and – that is the point of our interest, at least at this moment – these articles refer to identification or recognition performed by a human being[1]. So, if it is a person to identify another person (art. 213 CPC), an object (art. 215 CPC) or something else (*e.g.* a voice, a sound or any other element perceptible through sensorial discernment – art. 216 CPC), that's typical evidence. Instead, if the recognition is executed for instance by an animal, assume a dog, we are facing a-typical evidence: because, in this case, the manner of performing the act/activity is not predetermined by law, but it is determined – according to the particularities of the facts, item by item – by the judge after having heard the parties.

The result, in both cases, is the same: a positive or a negative outcome of identification. What changes is the identifier and subsequently the way as evidence runs. It is clear that the mood to recognize someone or something cannot be identical if the performance is man-made rather than dog-made.

So, here lies the demarcation line: a divergence in the legal pre-definition of *modalities of evidence's exercise/assumption*. And, seeing that modalities of evidence's exercise/assumption are arranged to allow judge and parties to evaluate as best as possible the *credibility of the source* and the *reliability of the proof*, we can furthermore observe that evidence legally predefined is normally considered in itself suitable and trustable to

[1] Specifically, "When it is necessary to identify a person, the court shall ask the person who will perform the identification to describe the person and indicate all the details he is able to recall. The court shall also ask him whether he has been previously called to perform the identification, whether before or after the criminal act under prosecution he has seen, either directly or in a photo or otherwise, the person to be identified, whether the latter has been indicated or described to him, and whether any other circumstances may affect the reliability of the identification procedure. […] The person performing the identification shall be asked to leave the room and the court shall call in the room at least two persons that look as similar as possible, also in the clothing, to the person subject to identification. The court shall invite the latter to choose his position among the other participants, making sure that his appearance is as close as possible to what he looked like when he was seen by the person called to perform the identification. When the latter is brought back into the room, the court shall ask him whether or not he can identify any of the persons in the lineup and, in case of an affirmative answer, the court shall ask him to point out the identified person and specify whether he is completely certain of the identification. If there are well-founded reasons to believe that the person called to perform the identification may be intimidated or influenced by the presence of the person subject to the identification, the court shall order that the procedure be performed in a way so that the latter is not able to see the former. The record shall specify the methods employed in the identification procedure, under penalty of nullity. The court may order that the identification be recorded by photo, video or any other devices or procedures. […] When it is necessary to identify the *corpus delicti* or other material related to the offence, the court shall proceed following the provisions [just explained], provided they are applicable. Having obtained, if possible, at least two objects similar to the one to be identified, the court shall ask the person called to perform the identification whether or not he can recognise any of them. In case of an affirmative answer, the court shall ask him to specify which object he has recognised and whether he is completely certain of the identification. […] When ordering the identification of voices, sounds or any other element that may be the object of sensorial perception, the court shall follow the provisions [exposed *supra*], provided they are applicable. […] If more than one person is called to identify the same person or the same object, the court shall proceed by separate actions, taking due care to prevent any communication between the person who has performed the identification and those who still have to perform it. If the same person is required to identify more than one person or object, the court shall order that, in each action, the person or object to be identified be placed among different persons and objects" (Gialuz, Lupária & Scarpa, 2017, pp. 231-233).

establish the facts; conversely, the suitability and trustability of atypical evidence must be ensured by judge and parties with a careful configuration of its manifestation's way.

Well, without pausing on the distinction between the formation of evidence during cross-examination (the golden rule of the adversarial system)[2] and acquisition of evidence already formed (weak contradictory on the proof)[3], now we care to emphasize those that are the fundamental characteristics of atypical evidence.

CPC, Book III, Title I – General Provisions sets up requirements of "Evidence not regulated by law" (art. 189)[4]:

1) aptness to determine/ascertain the facts[5] – it must be concretely able to provide probatory elements that are significant/relevant for judgement and appreciable in their reliability;
2) not compromised of moral freedom[6] – it must remain free the individual capacity of self-determination according to the situation are not allowed practices like hypnosis, lie detector, narcoanalysis *et similia*;
3) duty (for the judge) of hearing the parties on the methods of gathering evidence, preliminary to decide on the admission of this kind of proof[7] – a tailor-made suit is made for atypical evidence, and this operation is not carried out alone by a judge but takes place with the parties' contribution.

These are the conditions of the right to evidence.[8] Wherever there is a need to introduce into the trial probative elements that are not provided for by law, we especially refer

---

[2] When the formation of evidence occurs in cross-examination, we have "means of evidence". CPC, Book III, Title II provides seven typical means of evidence: testimony, examination of the parties, confrontations, formal identifications, judicial simulations, expert evidence, and documentary evidence.

[3] To acquire evidence unformed in cross-examination we have "means of obtaining evidence". CPC, Book III, Title III provides four typical means of obtaining evidence: inspections, searches, seizures, and interception of conversations or communications.

[4] The rule reads as follows: "If evidence not regulated by law is requested, the court may introduce it if it is deemed suitable to determine the facts and does not compromise the moral freedom of the person. After hearing the parties on the methods for gathering evidence, the court shall order the admission of evidence". The *Report of CPC's project* affirms that Art. 189 is a "middle road" between the principle of atypicality and principle of legality (*sub-species* precision or clarity principle) of evidence, because "[it] avoids excessive restrictions on the ascertainment of the truth, taking into account the continuous technological development that extends the frontiers of investigation, without endangering the guarantees of defence".

[5] Which facts? The facts are illustrated by art. 187 CPC – Facts in issue: "Facts concerning accusations, criminal liabilities and the determination of either the sentence or the security measure are facts in issue. Facts on which the application of procedural rules depends are also facts in issue. Facts concerning the civil liability resulting from an offence are also facts in issue if a civil party joins the criminal proceedings".

[6] Moral freedom is moreover protected by art. 188 CPC – Moral freedom of the person during evidence gathering: "Methods or techniques which may influence the freedom of self-determination or alter the capacity to recall and evaluate facts shall not be used, not even with the consent of the person concerned".

[7] The decision is contestable through the appeal of closing judgment (art. 586 § 1 CPC).

[8] Right to evidence – indispensable to support defensive and accusatory reconstructions within the process – is an expression of the protagonism guaranteed to lawyer/defence (art. 24 IC) and prosecutor/accuse (art. 112 IC), before a third and impartial judge (art. 111 IC), in our criminal procedural system.

to means, techniques and tools that technological progress makes available for criminal proceedings and that cannot be embedded in any regimented evidentiary typology… otherwise, we have a "label fraud": because this mechanism would be used for circumventing the existing rules by smuggling occurred omissions or irregularities concerning typical evidence as mere atypicality profiles of that evidence.[9]

However, and beyond this or other issues on the subject, there is a very important problem – that arose in the early 2000s – that all today occupies centre stage. The theme is the use of atypical evidence (specifically, atypical means of obtaining evidence – see nt. 3) via instruments attacking fundamental rights and freedoms.

In particular, an aspect extremely sensitive is the following: the assault, through these invasive devices, to rights safeguarded by Art. 13 (personal liberty), 14 (personal domicile) and 15 (inviolability of correspondence and communication) of the Italian Constitution – IC.

It is constitutionally established that these rights and freedoms are, first of all, inviolable and, in addition, protected with a double warranty: a reinforced statutory reserve and a jurisdictional reserve – that is to say, that any compression of them is allowed only in such cases and in such manner as provided by the law and by order of the judiciary stating legally reasons.[10] The undetermined nature of atypical evidence clashes against the guarantees just exposed – that is the main problem.

Jurisprudence (primarily) and doctrine (ensuing case law) have drawn a pattern to face the situation – see *infra*, § 3; and the scheme drafted perfectly intersects a method of evaluation and justification that organizes the judgement (*rectus* a part of the judgement) into several mandatory logic-argumentative steps: the duty, or burden, of reinforced reasoning.

2. A PARTICULAR DUTY OF EVALUATION AND JUSTIFICATION FOR THE JUDGE: THE THEORY OF REINFORCED REASONING

The so-called reinforced reasoning is a method of evaluation (judgement) and justification (explanation/grounds of the pronouncement), developed by jurisprudence (case law) and refined by doctrine (specialist literature), that breaks down the decision into several necessary logic-argumentative steps.

By 'reinforced reasoning' we mean "a formula which, on the one hand, imposes caution [a sort of warning] with regard to certain specific legal profiles related to the decision-making process and, on the other hand, demands that the decision be based on more solid grounds with regard to such questions (*recite* arguments), the verification

[9] If there is a legal framework for that evidence, it cannot be circumvented. Also, the Supreme Court of Cassation recognizes a principle of non-substitutability in this matter: "When the code establishes a prohibition of evidence or an express exclusion of usability, the recourse to other procedural instruments, both typical and atypical, aimed at surreptitiously circumventing such a bar is prohibited" (Cass., Sec. V, September 7, 2015, no. 36080, Sollecito e Knox; see more Cass., Un. Sec., May 28, 2003, no. 36747, Torcasio and Cass., Un. Sec., April 19, 2012, no. 28997, Pasqua).

[10] One guide principle here is proportionality. The act adopted must be proportional to circumstances, and conditions and indispensable to achieve the purpose stated by law; and the sacrifice of the constitutional right or freedom must be justified by the seriousness of the offence.

of which is considered essential for the legitimacy of the assessment issued. […] The peculiar characteristic of this method of evaluation (*i.e.* judgement) and justification (*i.e.* explanation of the decision's reasons) lies in the fact that the judge is required to go through a series of mandatory steps, made up of arguments concerning salient aspects of the case under examination and which must be appreciated (*i.e.* adapted in content to the specifics of the concrete case) in the light of parameters and criteria widely shared and/or consolidated, and intersubjectively verifiable"[11].

So, according to the theory of reinforced reasoning, it becomes unavoidable to go through certain logic-argumentative steps that are indispensable for the concretization of a given juridical case – a juridical case that we can therefore call "a reinforced reasoning juridical case".

To be clear, let me give an example. We can talk about precautionary measures and more exactly pre-trial detention in prison. In this hypothesis, a necessary step in judicial reasoning is the examination – obviously, after having already ascertained all the other prerequisites for the application of a precautionary measure: *i.e.* general conditions of applicability (art. 273 CPC) and precautionary requirements (art. 274 CPC) – of the possibility to adopt a less afflictive measure than imprisonment: such as, for instance, house arrest (with or without an electronic bracelet) or other coercive or interdictory measures (also applied cumulatively). Solely after the evaluation of this salient/fundamental profile, it is permissible to command custody in prison. If this logic-argumentative step is not crossed, the measure is unlawful – null under art. 292 § 2 CPC.

The judge, with autonomous assessment and in the light of the criteria (widely shared and/or consolidated, and intersubjectively verifiable) of proportionality, adequacy and gradualness (art. 275 CPC), must examine this inescapable argument, which can be summarized as follows: "Is it possible to apply a precautionary measure milder than custody in prison, or not?".

This is, in fact, the question that arises from *a contrariis* reading of the letter of art. 292 § 2, lett. c-*bis*) CPC, according to which the order of pre-trial detention in prison must contain "an exposition and independent assessment of the reasons why the elements provided by the defence were considered irrelevant, as well as, in the event of the application of the measure of custody in prison, an exposition and independent assessment of the concrete and specific reasons why the needs referred to in art. 274 cannot be satisfied with other measures".Which other measures? Those referred to in art. 275 §§ 3 and 3-*bis* CPC: "other coercive or disqualifying measures" in general, also cumulative; or "the measure of house arrest with the control procedures referred to in art. 275-*bis* § 1" CPC.

In this 'reinforced reasoning juridical case' – among the various arguments that the judicial authority has to take into consideration – an inevitable logic-argumentative step consists of evaluating (and, consequently, expressly justifying) reasons why pre-trial detention in prison represents the lone adequate and suitable precautionary measure to respond to the pre-trial needs emerging in the concrete case.[12]

[11] Cecchi, 2021, p. 437.

[12] Cecchi, 2021, pp. 549-550.

Well, this way of evaluation and justification of the decision constitutes a model of *stylus curiae* in clear expansion, that involves a plurality of hypotheses in which there are legally relevant situations demanding effective protection and finding their guarantee precisely in the reinforced reasoning of one or more specific and salient/fundamental legal-argumentative profiles of the case.

The reinforced reasoning on atypical evidence is, trivially, the application of the *m(eth) modus decided et justificandi* now exposed in the subject of this paper. Here, the arguments to be necessarily appreciated – oriented by widely shared and/or consolidated parameters and criteria, and inter-subjectively verifiable – are those useful to probe the legitimacy of atypical evidence and, at the same time, the respect of fundamental rights and freedoms.

We are going to show this in the next paragraph.

3. THE REINFORCED REASONING ON A-TYPICAL EVIDENCE; WITH JUST A FEW EXAMPLES

It is time to recall considerations I have already had the opportunity to develop elsewhere.[13].

The theory of reinforced reasoning applied to atypical evidence represents a strengthened protection aimed at avoiding, or at least at making it easier to identify and then penalize, the following two occurrences: a) improper use of art. 189 CPC to circumvent evidentiary rules and typical evidence; b) the unfair infringement of fundamental constitutional rights or freedoms.

It seems consolidated (surely in the pronouncements of apex judicial authorities: *i.e.* Constitutional Court and Supreme Court of Cassation) the pattern of evaluation and justification conceptualized by Prof. Carlotta Conti.[14], with regard to evidence potentially damaging fundamental rights or freedoms safeguarded by the Constitution, and also pertaining to evidentiary activities that could surreptitiously bypass the legislative provisions set for their functioning.

This is an evaluative-justificatory module that can be placed within the paradigmatic theory of reinforced reasoning because it outlines a path with obligatory logic-argumentative steps, oriented by parameters and criteria widely shared and/or consolidated, and inter-subjectively verifiable. Moreover, in this sense, we could also say that we are facing "a complex formation evidence"[15].

---

[13] I dealt this topic in Cecchi, 2021, pp. 575-585; and the following reflections largely reproduce what is written there.

[14] The model is an extrapolation and a refinement operated by Carlotta Conti from the "Cartesian clarity" (Conti, 2019, p. 1579; see also Baccari & Conti, 2021, pp. 718-722 and Conti, 2018, p. 1210) decisions of the Constitutional Court (sentences no. 135/2002 and no. 149/2008) and of the Supreme Cour of Cassation (Un. Sec., March 28, 2006, no. 26795, Prisco) about video filming.

[15] We find this expression in Iannucci, 2023, p. 610, who uses it referring to expert evidence; but we think the concept is re-adaptable to our discourse insofar as it refers to "multi-steps/different phases evidence formation".

Adhering to the proposed reconstruction, the mandatory passages of the decisional reasoning are three.[16]; let us see them[17].

(1) Firstly, it is necessary to verify the typicality of evidence or evidentiary activity under discussion. If there is a typical discipline, then art. 189 CPC is not applicable (… unless one wishes to circumvent the law: but then it operates the non-substitutability principle – see no. 9). This latter provision, in fact, works on a residual basis: and represents both the 'release valve' (which includes evidentiary activities and related evidence not regulated by law) and the closing rule of the system (which limits evidentiary activities and related evidence already regulated by law, that cannot be surreptitiously circumvented). So, the first step concerns the identification of a typical discipline within which evidence or evidentiary activity can be framed. If it is identified, it is applied. If it is not identified, one moves on to the next step: the application, or not, of art. 189 CPC.

(2) Secondly, hence, there is a check of art. 189 CPC's applicative prerequisites. Once the requirements of this rule have been verified[18], if the 'atypicality route' is practicable, the final step is opened; otherwise, the assessment is closed at this second level with the affirmation of the legal irrelevance[19] (or, as the case may be, even the illegitimacy) of evidence or evidentiary activity in question – not regulated by law; not classifiable under art. 189 CPC.

(3) Thirdly, and finally, when we can legitimately move within the category of atypical evidence, then it is necessary to make a further examination of the existence of any 'systemic-constitutional evidentiary limits'[20] – *i.e.* limits placed to protect fundamental rights or freedoms safeguarded by the Constitution, the violation of which leads to evidence's unusability: so-called "unconstitutional evidence".

In short, once the preliminary screening has led to the recognition of an effective and legitimate atypicality of the instrument (means or means of obtaining evidence), understood as the impossibility of framing it within the acts already regulated by law, it is essential to carry out a supplementary assessment on limitation of fundamental rights or freedoms provoked by the atypical evidence (act or activity). The *cliché* characterising this third logic-argumentative step unfolds in a judgement that can be further subdivided into three other passages.

---

[16] The hypothesis in question represents one of those hypotheses of reinforced reasoning in which the obligatory steps are prodromal to each other. The peculiarity (in terms of argumentation) of this type of assessment also consists in the fact that the three steps are linked to each other by a bond of bias, in the sense that, depending on the result obtained by passing through the antecedent step, one moves on to a subsequent step (consisting of certain arguments and reference parameters) or to another subsequent step (consisting of certain other arguments and reference parameters) or, more drastically, one stops.

[17] See Tonini & Conti, 2014, pp. 196-204.

[18] The requirements are those seen above: aptness to determine the facts; not compromised of moral freedom; duty, for the judge, of hearing the parties on the methods of gathering evidence.

[19] Actually, not every imaginable (non-statutory) instrument is admissible merely because the evidentiary results flowing from it appear useful to the ascertainment.

[20] The question that needs to be asked (and then answered) is "Are there legally relevant situations, interests or juridical relevant goods behind the atypical evidence (act or activity), worthy of protection at constitutional level?".

I) If one is in the presence of a constitutionally enshrined fundamental right or freedom, in the absence of a law regulating the "cases" and the "manners/ways" in which the right or the freedom may be undermined, an injury thereto is not admissible: under penalty of unusability of the (unconstitutional) evidence deriving from illegitimate probative activity.

II) If one is in the presence of an emerging fundamental right or freedom (protected/protectable *ex* art. 2 IC – *e.g.* privacy/confidentiality), it is sufficient a congruously justified measure adopted by a judge or simply by the prosecutor to carry out the evidentiary activity and to derive the relevant evidence. Anyway, the degree of injury suffered by the emerging right or freedom remains open to be reviewed in terms of reasonableness and proportionality.

III) If no fundamental right or freedom provided for or emerging from the Constitutional Charter is involved, then no issues arise as to the 'systemic-constitutional evidentiary limits'. Consequently, the evidence or evidentiary activity, after having surpassed the two previous steps, may legitimately manifest itself in criminal proceedings without crossing this final step.

This is, in summary, the reinforced reasoning on a-typical evidence.

Now, exemplifying with just a few theoretical-practical cases, we can apply what has just been said to some evidentiary activities carried out with atypical means of obtaining evidence that is widespread today: video recordings and, *mutatis mutandis*, virus trojan; the secret agent equipped for sound; tracking by GPS[21].

About video recordings[22], a distinction must be made between communicative and non-communicative videotaped behaviours. We are in the presence of a probative activity that is only apparently atypical if the video recordings result in a mere caption of conversations (communicative behaviour) not accompanied by images: in this case, in fact, the video recordings can be classified as interceptions/wiretapping and, thus, the applicable rules are to be found in art. 266 ff. CPC, which provides full legislative coverage of the right under art. 15 IC. In this hypothesis, therefore, we stop at the first step. On the other hand, if the video recordings apprehend non-communicative behaviour (*i.e.* if they take images and scenes of a person's life), we are in the presence of an evidentiary activity that is to all intents and purposes atypical. In this case, video recordings are an atypical means of obtaining evidence because they are not regulated by law (step 1). Undoubtedly, they represent an instrument that has a significant ascertaining capacity, and they are not detrimental to the moral freedom of those who are unknowingly filmed (step 2). At this point, one must assess the harmfulness of the instrument with respect to constitutionally protected fundamental personal rights or freedom at stake (step 3). Following the statements of the Constitutional Court (sentences no. 135/2002 and no. 149/2008) and the Supreme Court of Cassation (United Sections, March 28, 2006, no. 26795, Prisco), we derive that:

[21] We report, shortly, what can be read in Tonini & Conti, 2014, pp. 466-483, to which we recall also for bibliographical references contained therein.

[22] Video recordings made by video surveillance systems installed by public or private persons are not included in these considerations, because they remain outside of the interceptions' category and they constitute documentary evidence, acquired at trial under conditions established by art. 234 CPC.

I) If video recordings capture life within the home, then they affect the freedom of personal domicile (art. 14 IC) and, in the absence of a specific legal regulation establishing the "cases" and the "ways/manners" in which this fundamental right can be restricted, they cannot be ordered;

II) If the video recordings capture what is happening in reserved places (*e.g.* toilets of a public place; privy of a disco; etc.), then they infringe the right to privacy/confidentiality (an emerging fundamental right, protected under art. 2 IC). Their use is permitted, and evidence gathered in this way may be used, if it is authorized by a judicial authority (judge or prosecutor) with a suitably reasoned order/measure;

III) If the video recordings capture what happens in a place open to the public[23], they do not impact any constitutionally protected fundamental right or freedom and, therefore, they constitute an atypical evidentiary activity that can peacefully be directly realized by police. Having gone through the first two steps, in the latter circumstance, the third step is practically unimportant because no fundamental right is impaired.

About the virus trojan, the remarks made on video recordings are *mutatis mutandis* applicable: starting with the distinction between communicative and non-communicative behaviour captured. In particular, the evaluation and justification grid just outlined must be adapted to the peculiarities of each evidentiary activity that can be carried out by such means of obtaining evidence. Some of these activities (in reality, at present, only communicative acquisitions) have been regulated by law and therefore, since they are no longer atypical evidence, do not concern the three-step reinforced reasoning module that we are going to describe: or rather, we stop at the first step of this module and, having regard to the communicative acquisitions by virus trojan, we refer to the specific legislative discipline (art. 266 §§ 2 and 2-*bis* CPC). The other potential activities of the virus trojan, left out of the codification (*e.g.* keyloggers; screenshots; screencasts; online surveillance; etc.), are instead declinable into the reinforced reasoning format exposed above: each one, obviously, according to its peculiarities.[24].

About secret agents equipped for sound, based on case law (in particular, Constitutional Court, sentence no. 320/2009), it can be said that it is a typical means of obtaining evidence if the investigating authority's listening takes place at the same time as the recording since the presence of the third hidden ear (*i.e.* the investigators' ear) allows the assimilation to wiretap and makes the rules under art. 266 ff. CPC applicable. On the contrary, it is

[23] Constitutional Court (sentence no. 149/2008) has made it clear that non-communicative behaviour *in fact* not confidential, as happens when a window or door is left open and whoever can look inside, even if carried out within the home, is not covered by art. 14 IC.

[24] Let's take videorecording of computer screens (screenshot/screencast) or spying on what one is typing on the keyboard (keylogger). Here, the first two steps are positively overcome and the problem of providing a more or less guaranteeing interpretation of the fundamental rights and freedoms involved opens up with regard to the third step. Two divergent interpretations are possible: one can argue that the usability regime depends on the type of data typed or displayed, which can be considered more or less public (*e.g.* Facebook post ≠ email saved in drafts in the mailbox); one can adopt a lecture that is more sensitive to protection of constitutional rights and freedoms and then consider the aforementioned atypical activities invasive – in constitutionally more (art. 15 IC) or less (art. 2 IC) marked terms – regardless of the type of data captured; and depending on the interpretation one choices, the consequences are quite different.

an atypical evidentiary activity if what is recorded is listened to deferred and not while the secret agent is communicating and recording. In this case, we fall into the category of atypicality because we are outside the hypothesis of interceptions: there is no perception of the communication by a third party extraneous to it (step I). It is evident that the investigative tool is suitable for ascertaining the facts and that there isn't prejudice to the moral freedom of the person subjected to it, voluntarily participating in the communication recorded (step II). The fundamental right involved, as the person recording is not a stranger to the conversation but rather actively contributes to it, is not secrecy (art. 15 IC) but privacy/confidentiality (art. 2 IC). So, an authorization act – if correctly justified – by the prosecutor is sufficient to perform the activity (step III), which generally is realized, on delegation, by police.

Tracking by GPS, it can be observed that is an atypical instrument since that is not regulated by law nor can be included within any typical means of obtaining evidence (step I). Then, tracking by GPS does not affect the behaviour of the subject being followed: the person, on the contrary, is unaware of the following; and insofar as it is related to relevant moments in relation to the crime committed, the evidence is eligible to determine the facts (step II). Furthermore, such probative activity does not violate the secrecy of communications (art. 15 IC), because the flow picked up by the satellite system does not concern secret conversations; it could be argued, however, that there is an impact on freedom of movement (art. 16 IC): with the consequence that such an invasion requires, to be legitimate, a reasoned measure by the judicial authority that authorizes it (step III). Well, Italian jurisprudence – unlike American jurisprudence – does not go through this last step or, even if going through it, does not detect violations of fundamental rights or freedoms. Thus, at a praxeological level, tracking by GPS is currently considered a mere atypical activity workable by police, for which no particular guarantees are required. Theoretically and *de jure contendo* speaking, on the contrary, it should be subject to the scheme we have just outlined *supra*: and, therefore, be authorized in advance by a reinforced reasoning measure that shows the crossing of the essential above-mentioned logic-argumentative passages – especially the third step.

We can stop here with exemplifications.

Beyond whether or not one agrees with the legal choices with which we have illustratively filled in the content of the necessary logic-argumentative steps in the hypotheses listed[25], we believe we can state that the form of reinforced reasoning applied to atypical evidence (act or activity) is extremely functional to resolve in a linear manner the thorny application problems that usually occur in this matter[26].

[25] For example, examining the reconstructive solution put forward with reference to the secret agent equipped for sound, we could ask ourselves whether or not, within the third step, it is reasonable to argue that the presence of the secret agent as a co-participant in the conversation degrades, even for the other participant (unaware of the recording in progress), the protection of the communication: instead of being guaranteed by the secrecy of art. 15 IC, protected in the milder terms of privacy/confidentiality by art. 2 IC.

[26] On closer inspection, the adoption of this method of evaluation and justification does not change the way in which a decision is already made. Indeed, in judgements dealing with atypical evidence, the assessment and the reasoning unfold – at least – in the three obligatory steps we have set out. However, much of this process very often remains in the pen of the decider/judge; and consequently, cannot be reviewed either by the parties (endo-procedural function of the statement of reasons) nor by the public (extra-procedural function of the statement of reasons).

If this method of evaluation and justification is accepted, the judicial decision becomes more transparent and thereby more guaranteed, being more controllable. Indeed, the unwinding of the decisional assessment within mandatory logic-argumentative passages makes the legally legitimate reasons underlying the measure emerge clearly. This greater visibility allows a more open confrontation with arguments put forward by judicial authority: so that, where the interpretative positions taken appear questionable (as in our opinion is, for example, questionable the jurisprudential reconstruction that considers tracking by GPS an instrument not invasive of the right protected under art. 16 IC), it becomes easier to face them and perhaps overcome them with counter-arguments.

All this, in the end, ends up contributing to a better administration of justice.

LIST OF REFERENCES

Baccari, G. M. & Conti, C. 2021. La corsa tecnologica tra Costituzione, codice di rito e norme sulla privacy: uno sguardo d'insiem. *Diritto penale e processo*, 6, pp. 717-723.

Cecchi, M. 2021. *La motivazione rafforzata del provvedimento. Un nuovo modello logico-argomentativo di stilus curiae*. Padova: CEDAM.

Conti, C. 2018. Prova informatica e diritti fondamentali: a proposito di captatore e non solo. *Diritto penale e processo*, 24(9), pp. 1210-1221.

Conti, C. 2019. Sicurezza e riservatezza. *Diritto penale e processo*, 11, pp. 1572-1585.

Gialuz, M., Lupária, L. & Scarpa, F. 2017. *The Italian Code of Criminal Procedure. Critical Essays and English Translation*. Padova: Kluwer, CEDAM.

Iannucci, C. 2023. La "circolazione" della prova peritale: un tentativo di lettura costituzionalmente orientata a fronte di una giurisprudenza oscillante. *Il processo: rivista giuridica quadrimestrale*, 2, pp. 603-627

Tonini, P. & Conti, C. 2014. *Il diritto delle prove penali*. Milano: Giuffrè.

UDC: 343.268 DOI: 10.56461/iup_rlrc.2024.5.ch11

Melinda HENGL*
Faculty of Law, University of Pécs, Hungary

THE IMPORTANCE OF (PRELIMINARY) COMPULSORY PSYCHIATRIC TREATMENT IN THE SUPPRESSION OF CRIMINALITY

The paper examines the regulation of (preliminary) compulsory psychiatric treatment in three countries (Hungary, Serbia and Slovakia), applying a legal comparative approach. It compares, along five aspects, the applicable three pieces of criminal law legislation most relevant to the subject in Hungary, Serbia and Slovakia respectively.

The paper intends to draw attention to the shared and different paths taken by the three countries under analysis in their examined pieces of legislation with a view to achieving an effective regulation of (preliminary) compulsory psychiatric treatment.

The analysis also endeavours to shed light, from the given aspects of comparison, on the detailed rules contained in the regulations of the examined countries relating to (preliminary) compulsory psychiatric treatment and how these rules may contribute to the reduction of crime.

Keywords: compulsory psychiatric treatment, suppression of criminality, Hungary, Serbia, Slovakia.

1. INTRODUCTION

The paper uses a legal comparative approach to analyse some of the main issues relating to (preliminary) compulsory psychiatric treatment – as listed under point 2 – by comparing the relevant regulatory backgrounds in *Hungary* – Act C of 2012 on the Criminal Code (hereinafter: Hungarian CC / HCC), Act XC of 2017 on the Code of Criminal Procedure (hereinafter: Hungarian CPC / HCPC) and Act CCXL of 2013 on the execution of punishments, measures, certain coercive measures and confinement for infractions (hereinafter: HE), *Serbia* – the Criminal Code of 2019 (hereinafter: Serbian CC / SCC), the Criminal Procedure Code of 2019 (hereinafter: Serbian CPC / SCPC) and the 2020 Law on Execution of Criminal Sanctions (hereinafter: SE), and *Slovakia*

* PhD, Assistant Professor, ORCID: 0000-0001-6366-9885, e-mail: *hengl.melinda@ajk.pte.hu*

– Act No. 300/2005 Coll. Criminal Code (hereinafter: Slovakian CC / SKCC), Act No. 301/2005 Coll. Code of Criminal Procedure (hereinafter: Slovakian CPC / SKCPC) and Act No. 368/2008 Coll. on the Execution of Imprisonment (hereinafter: SKE), in the (Latin) alphabetical order of the name of the countries (in English).

2. THE REGULATION OF (PRELIMINARY) COMPULSORY PSCYCHIATRIC TREATMENT IN HUNGARY, SERBIA AND SLOVAKIA

Main points of analysis to be covered include: (2.1.) the effects of mental state on criminal responsibility, (2.2.) the effects of mental state on criminal proceedings, (2.3.) possible legal remedies, (2.4.) the main rules of executing (preliminary) compulsory psychiatric treatment and (2.5.) the need for reviewing (preliminary) compulsory psychiatric treatment.

2.1. The Effects of Mental State on Criminal Responsibility

The Hungarian CC discusses mental disorder among the reasons for excluding or limiting liability to punishment (besides infancy, coercion and threat, error, justifiable defence, necessity, permission by law and any other reason specified in an Act) (HCC, § 15). Pursuant to the HCC, a person is not liable to punishment if he commits a punishable act in a state of mental disorder that renders him unable to recognise the consequences of his act or to act according to such recognition (HCC, § 17 (1)). However, the measures of confiscation (HCC, § 72 (4) a)), forfeiture of assets (HCC, § 75 (2) a)) and rendering electronic data permanently inaccessible (HCC, § 77 (2)) must be ordered even against a perpetrator who is not liable to punishment due to his mental disorder. The punishment may be reduced without limitation if the perpetrator's mental disorder limits his ability to recognise the consequences of his act or to act according to such recognition (HCC, § 17 (2)). The HCC lays it down as an exception that non-punishability and reduction of the punishment without limitation cannot apply to a person who commits a criminal offence in a drunken or otherwise intoxicated state induced due to his own fault (HCC, § 18). On the other hand, if a person (perpetrator) fulfils the statutory elements of an intentional criminal offence by using a person who is not liable to punishment for this act due to mental disorder, that person is considered an indirect offender (HCC, §§ 12, 13 (2)).

The Serbian CC specifies, in its third chapter on "Criminal Offence," the cases in which there is no crime and the cases in which it is possible to reduce the punishment, these include: self-defence (SCC, Article 19), extreme necessity (SCC, Article 20), force and threat (SCC, Article 21), mistake of fact (SCC, Article 28), mistake of law (SCC, Article 29) and mental incompetence (SCC, Article 23). Pursuant to the SCC, a perpetrator is considered mentally incompetent if he was unable to understand the significance of his act or was unable to control his actions (due to mental illness, mental retardation, temporary mental disorder or other severe mental disorder), and in such cases the offender concerned may be given a mitigated sentence (SCC, Article 23). The SCC lays down in a separate article (Self-induced Incompetence) that a perpetrator may not receive mitigated punishment if he committed a crime in such a state of mind induced on himself

through his own fault by consumption of alcohol, drugs or otherwise that he could not understand the significance of his act or control his actions (SCC, Article 24). The SCPC states that confiscation (SCPC, Article 535) and forfeiture of assets (SCPC, Article 541) may be ordered against a mentally incompetent defendant as well.

Table 1: The effects of mental state on criminal liability
(compiled by the author based on the relevant pieces of legislation)

<table>
<tr><th colspan="2">Hungarian CC</th><th colspan="2">Serbian CC</th><th colspan="2">Slovakian CC</th></tr>
<tr><td colspan="2">reasons for excluding / limiting liability to punishment</td><td colspan="2">in which cases it is possible to reduce the punishment / what does not constitute a criminal offence</td><td colspan="2">circumstances excluding criminal liability / conditions excluding the punishability of an act</td></tr>
<tr><td colspan="2">mental disorder</td><td colspan="2">mental incompetence</td><td colspan="2">mental disorder</td></tr>
<tr><td>↓
perpetrator is not liable to punishment, but confiscation, forfeiture of assets and rendering electronic data permanently inaccessible are possible</td><td>↓
punishment may be reduced without limitation</td><td></td><td>↓
punishment may be reduced</td><td>↓
perpetrator is (generally) not liable to punishment</td><td>↓
special reduction / waiver of punishment is possible</td></tr>
<tr><td colspan="2">unless:
he/she commits a criminal offence in a drunken / intoxicated state induced due to his/her own fault</td><td colspan="2">unless:
he/she committed a crime in a state of mind induced through his/her own fault by consumption of alcohol, drugs or otherwise</td><td></td><td>unless:
in a state of diminished responsibility under the influence of an addictive substance (in case of waiver)</td></tr>
<tr><td colspan="2">infancy</td><td colspan="2"></td><td colspan="2">age</td></tr>
<tr><td colspan="2">coercion and threat</td><td colspan="2">force and threat</td><td colspan="2"></td></tr>
<tr><td colspan="2" rowspan="2">error</td><td colspan="2">mistake of law</td><td colspan="2" rowspan="2"></td></tr>
<tr><td colspan="2">mistake of fact</td></tr>
<tr><td colspan="2">justifiable defence</td><td colspan="2">self-defence</td><td colspan="2">self-defence</td></tr>
<tr><td colspan="2">necessity</td><td colspan="2">extreme necessity</td><td colspan="2">extreme emergency</td></tr>
<tr><td colspan="2">permission by law</td><td colspan="2"></td><td colspan="2">exercising rights and obligations</td></tr>
<tr><td colspan="2">any other reason specified in an Act</td><td colspan="2"></td><td colspan="2"></td></tr>
<tr><td colspan="2"></td><td colspan="2"></td><td colspan="2">authorized use of weapon</td></tr>
<tr><td colspan="2"></td><td colspan="2"></td><td colspan="2">admissible risk</td></tr>
<tr><td colspan="2"></td><td colspan="2"></td><td colspan="2">consent of victim</td></tr>
<tr><td colspan="2"></td><td colspan="2"></td><td colspan="2">fulfilment of the role of secret agent</td></tr>
</table>

The Slovakian CC deals with mental disorder (SKCC, § 23) and age (SKCC, § 22) among circumstances excluding criminal liability (SKCC, Subdivision Three), while it mentions extreme emergency (SKCC, § 24), self-defence (SKCC, § 25), authorised use of weapons (SKCC, § 26), admissible risk (SKCC, § 27), exercising rights and obligations (SKCC, § 28), consent of the victim (SKCC, § 29), fulfilment of the role of secret agent (SKCC, § 30) among conditions excluding the punishability of an act (SKCC, Subdivision Four). Pursuant to the SKCC, a person who, due to a mental disorder, could not identify the illegal nature of an act otherwise criminal at the time of its commission or control his conduct, is not criminally liable for such act (unless the SKCC provides otherwise) (SKCC, § 23). Special reduction of the punishment is possible (the court may reduce the punishment below the lower limit of the criminal penalty provided for by the SKCC), if the offender committed the offence in a state of diminished responsibility (SKCC, § 39 (2) c)). The punishment of the offender for an offence, if it did not cause death or grievous bodily harm, may be waived if he committed the offence in a state of diminished responsibility unless he caused the state of diminished responsibility under the influence of an addictive substance (SKCC, § 40 (1) c)). The SKCC also mentions the possibility of imposing confiscation even in the case of mental disorder (SKCC, § 83).

For better comparison, the information set out above has been summarized in Table 1.

The analysis provided in the Table 1 shows that mental state has an effect on liability to punishment in all three countries. The punishment of perpetrators with a mental disorder may be reduced in all three countries, moreover, such a perpetrator may not even be liable to punishment at all under the Hungarian and Slovakian regulation. In addition, all three regulations emphasize that: the punishment may not be reduced in the case of a perpetrator who inflicted the state of mental incompetence on himself through his own fault (under Hungarian law – the drunken or intoxicated state; under Serbian law – a mental state induced under the influence of alcohol or drugs or otherwise; under Slovakian law – a state of diminished responsibility under the influence of an addictive substance); and that confiscation, for example, may be applied.

2.2. The Effects of Mental State on Criminal Proceedings

The Hungarian CPC distinguishes between two groups of coercive measures: coercive measures affecting personal freedom (including preliminary compulsory psychiatric treatment besides custody, restraining order, criminal supervision, pre-trial detention) and coercive measures affecting assets (search, body search, seizure, sequestration, and rendering electronic data temporarily inaccessible) (HCPC, § 272). Preliminary compulsory psychiatric treatment may be ordered by the judge before a final and binding conclusive decision is adopted where it is necessary that the defendant affected by a mental disorder is deprived of his personal freedom (HCPC, § 301 (1)). Preliminary compulsory psychiatric treatment may be ordered (in a proceeding conducted for a criminal offence punishable by imprisonment) in order to eliminate the possibility of reoffending if it is reasonable to assume that the defendant should be subjected to compulsory psychiatric treatment (HCPC, §§ 276-277). No bail may be set if preliminary compulsory psychiatric treatment is ordered (HCPC, § 285 (6) a)).

The Hungarian CPC specifies, among the means of evidence, expert opinions (besides witness testimonies, defendant testimonies, opinions by a probation officer, means of physical evidence, including documents and deeds, and electronic data – HCPC, § 165) and regulates the expert opinion on the observation of the mental state of the defendant in a separate section (HCPC, § 195). The court may order the observation of the mental condition of the defendant if the expert opinion concludes that observing the mental condition of the defendant for an extended period by an expert is necessary. In such a case, the defendant must be referred to the forensic psychiatric and mental institution (if detained), or to a psychiatric in-patient institute specified by law (if at liberty). The observation period may last up to 1 month; this time limit may be extended by up to 1 month on the basis of the opinion of the institute (HCPC, § 195 (1)).

The Serbian CPC provides for compulsory psychiatric treatment as a security measure. With regard to a defendant committing a criminal offence in a state of mental incompetence, the public prosecutor may submit a motion to the court to impose on the defendant a security measure of compulsory psychiatric treatment and confinement in a medical institution or compulsory psychiatric treatment at liberty (SCPC Article 522). Detention (confinement in a secure mental institution) – before the conclusion of the proceedings of the first instance court – is justified if, should the defendant remain at liberty, there is a justifiable danger that he might commit a criminal offence as a result of his mental incompetence (SCPC Article 524).

The Serbian CPC also deals with expert examination among means of evidence (Chapter VII) and lays down several types of such examination. One of them is the psychiatric expert examination, which may be ordered, for example, when suspicion arises regarding the defendant's mental competency (SCPC Article 131).

The Slovakian CPC regulates compulsory psychiatric treatment under coercive measures (SKCPC, § 445). Such treatment may be ordered in the form of out-patient care or as confinement in a secure inpatient institution (even in the case of a convicted defendant serving his sentence of imprisonment, on the basis of a medical expert opinion) (SKCPC, § 446b).

The Slovakian CPC deals with experts in Chapter 6 on evidence and also lays down rules regarding the examination of the mental state of the defendant. The mental state of the defendant may be examined by a psychiatric expert in out-patient care or observed in a secure medical institution (SKCPC, § 148).

From the above, it may be concluded that (preliminary) compulsory psychiatric treatment is regulated as a coercive measure under the Hungarian CPC and Slovakian CPC, and as a security measure under the Serbian CPC. Moreover, all three CPCs provide for the expert examination of the defendant's mental state (in the parts on evidence/means of evidence).

As a further similarity one may mention that, in all three countries under analysis, the participation of a defence counsel in the criminal proceedings is compulsory: under the HCPC, if the defendant or the person reasonably suspected of having committed a criminal offence has a mental disorder or is subject to preliminary compulsory psychiatric treatment (HCPC, § 44 b) c)); under the SCPC, if proceedings for compulsory

psychiatric treatment are being conducted against the defendant (SCPC Article 74. 7)); and under the SKCPC, if the defendant is under observation in a medical institution (SKCPC, § 37 a)).

2.3. Possible Legal Remedies

Pursuant to the Hungarian CPC, the spouse or cohabitant of the defendant is entitled to file an appeal against ordering, extending, or maintaining preliminary compulsory psychiatric treatment (HCPC, § 301 (3), and they are entitled to file a motion to terminate such treatment (HCPC, § 301 (4)). Recompense may be provided for preliminary compulsory psychiatric treatment if certain conditions are met (HCPC, § 845).

Pursuant to the provisions of the Hungarian CPC, the spouse or cohabitant of the defendant may: file an appeal against a judgment of a court of first instance ordering compulsory psychiatric treatment (HCPC, § 581 e)), file a motion for retrial (HCPC, § 639 (2) e)) or submit a motion for review (HCPC, § 651 (2) e)) to the benefit of a defendant against the order of compulsory psychiatric treatment.

Pursuant to the HE, an order about the review of compulsory psychiatric treatment may be appealed by the spouse, cohabitant or lawful representative of the person subjected to compulsory psychiatric treatment (HE, 69/B (9)).

According to the Serbian CPC, the ruling pronouncing compulsory psychiatric treatment may be appealed (within 8 days after the date of receipt of the ruling) (SCPC, Article 528): by the spouse of the defendant, the person with whom he/she lives in a common law marriage or other permanent personal association, the lineal consanguine relations, the adopter, the adoptee, the sibling and foster parent, the legal representative, the defence counsel and the injured party (SCPC, Article 433).

Under the Slovakian CPC (SKCPC, § 186 (2)), a complaint may be filed against the decision imposing compulsory psychiatric treatment by persons entitled to file an appeal on behalf of the person concerned by the compulsory psychiatric treatment (the spouse, cohabitant, lineal relative, sibling, adopter, adoptee or defence counsel of the defendant – SK, § 308 (2)).

In the light of the foregoing, it may be stated that all three regulations emphasize the possibilities of the spouse and cohabitant of the defendant for legal remedy, in addition, the Serbian CPC and Slovakian CPC specify further persons who may file for legal remedy.

2.4. The Main Rules of Executing (Preliminary) Compulsory Psychiatric Treatment

The HE refers to the person under compulsory psychiatric treatment as "patient" (HE, § 325 (2)) and lays down that his rights relating to psychiatric treatment are mainly governed by the general provisions of the Healthcare Act and the rules applicable to the rights of psychiatric patients (HE, § 325 (3)). Compulsory psychiatric treatment must be executed in such a way so as to ensure that the patient is provided with proper treatment in view of the current state of medical science, the deterioration of his health is prevented and his health is restored to the extent possible within the shortest time (HE, § 325 (4)). The costs of compulsory psychiatric treatment are to be borne by the State (HE,

§ 325 (5)). The place of execution of compulsory psychiatric treatment is the Forensic Psychiatric and Mental Institution (IMEI) (HE, § 326 (1), HE, § 19 e), the execution of the treatment cannot be interrupted (HE, § 327 (3)), the patient may leave the institution only under supervision (HE, § 337) or exceptionally if he has been granted permission to be released on reintegration leave, accompanied by the person undertaking his care (HE, § 338). The patient is to be released from the IMEI on the day when the notification about the termination of the compulsory psychiatric treatment (issued by the penal enforcement judge) arrives at the IMEI (HE, § 341).

Pursuant to the HE, the rules relating to the execution of compulsory psychiatric treatment are applicable (with exceptions and derogations) also to the execution of preliminary compulsory psychiatric treatment, which is also to be executed in the IMEI (HE, § 424).

The Serbian CC distinguishes between 4 types of compulsory medical treatment: compulsory psychiatric treatment and confinement in a medical institution, compulsory psychiatric treatment at liberty, compulsory drug addiction treatment and compulsory alcohol addiction treatment (SCC Article 79 (1)). Out of them, 2 types of compulsory medical treatment may be ordered regarding mental disorder: (1) the compulsory psychiatric treatment and confinement in a medical institution is ordered by the court in the case of a perpetrator who committed a criminal offence in a state of substantially impaired mental capacity if there is a risk that the offender may commit a more serious criminal offence and that in order to eliminate this risk the offender requires medical treatment in such institution (SCC Article 81 (1)). (2) The compulsory psychiatric treatment at liberty is also ordered by the court in the case of an offender who has committed a criminal offence in a state of mental incapacity if there is a danger that the offender may again commit another criminal offence, but in order to prevent this there is no need for the offender's confinement (SCC Article 82 (1)). The SE lays down that professional supervision over the execution of compulsory psychiatric treatment is to be carried out by the Ministry in charge of health (SE Article 200). Pursuant to the SCC, the limitation period for enforcing decisions on compulsory psychiatric treatment is 5 years from the decision becoming binding (SCC, Article 106 (2)).

The SKE distinguishes 5 types of compulsory medical treatment: compulsory psychiatric treatment, compulsory drug treatment, compulsory alcohol treatment, compulsory sexual addiction treatment and compulsory gambling addiction treatment (SKE, § 80 (3)). If several types of compulsory medical treatment have been ordered against the convict, then compulsory psychiatric treatment must be executed first (SKE, § 81 (3)). Pursuant to the SKE, compulsory psychiatric treatment may be executed in the form of out-patient care or in a secure inpatient institution as well, in a special section of the penal enforcement institution or the psychiatric department of a healthcare institution (SKE, § 80 (1)).

Based on the examples selected from the regulations of the 3 countries, it may be concluded that, although the execution of compulsory psychiatric treatment is regulated in all 3 countries, there is a difference in the depth and detailedness of the regulation. It is an essential difference that the Serbian and Slovakian regulations distinguish between several types of compulsory medical treatment, while the Hungarian regulation only provides for

compulsory psychiatric treatment for mental disorder as compulsory medical treatment. The Hungarian regulation also contains other types of medical treatments (that are different from the one for mental disorder), but they are not regulated as compulsory medical treatment. For example, it lays down: if a person is arrested for drug possession, the person may be granted the possibility to participate in medical treatment to cure his drug-addiction or to receive some other assistance to treat his drug use or preventive counselling service (HE, § 394 (2a)); it is to be ascertained whether, in the case of conditional suspension by the prosecutor, the suspect consents to undergoing the planned alcohol treatment (HCPC, § 418 (8b)); and the person arrested for committing an offence against sexual freedom and sexual morality must be offered the possibility of voluntary participation in proper psychotherapy or other programming aimed at reducing the likelihood of recidivism (HE, § 394 (2)).

2.5. The Need for Reviewing (Preliminary) Compulsory Psychiatric Treatment

The Hungarian CC lays down that compulsory psychiatric treatment is to be terminated if it is no longer necessary (HCC, § 78 (2)).

Under the regulation in the Hungarian CPC, preliminary compulsory psychiatric treatment (ordered prior to the indictment) is to remain in effect until a decision is adopted by the court of first instance during the preparation of a trial, but for no longer than 6 months; the court may extend the period of preliminary compulsory psychiatric treatment before the indictment, by up to 6 months each time (HCPC, § 301 (5–6)). If terminating the preliminary compulsory psychiatric treatment is justified, the institute enforcing preliminary compulsory psychiatric treatment is to inform the prosecution service, before the indictment, or the court, after the indictment, without delay (HCPC, § 301 (7)). In the case of military criminal proceedings, the commander must notify the prosecution service without delay if he considers it necessary to terminate the preliminary compulsory psychiatric treatment (HCPC, § 709 (1) b)).

The HE regulates the review of compulsory psychiatric treatment specifically in Section 69/B: Within 6 months from the commencement of the treatment, the judge is to review, ex officio, the necessity of such treatment, and do so repeatedly every 6 months (if he has not terminated the treatment). The conduct of the procedure may come within the competence of the penal enforcement judge of the Budapest Environs Regional Court (if the first-instance procedure was not conducted by a court seated in Budapest), or that of the Budapest-Capital Regional Court. The review may be initiated by the prosecution service or put forward by the head physician and general director of the IMEI or petitioned by the person undergoing compulsory psychiatric treatment, his spouse, cohabitant, lawful representative or defence counsel (but their application may be rejected without examination on the merits if filed repeatedly within 3 months without reference to a new circumstance). During review, at the hearing, the prosecutor, the defence counsel and the person under compulsory psychiatric treatment – if his condition renders it possible – are to be heard. Prior to the review, a forensic psychiatric expert opinion must be obtained (unless the person was subject to preliminary compulsory psychiatric treatment, as in that case the forensic psychiatric expert opinion made available during the criminal case may be used). The physician of the IMEI

may participate as one of the experts in the elaboration of the expert opinion. The detailed medical case report of the patient is to be forwarded by the head physician and general director of the IMEI during the 3rd month calculated from the patient's admission to the IMEI (and every 6 months until the patient's release) to the competent penal enforcement judge to conduct a review of the compulsory psychiatric treatment (HE, § 329 (1)).

The Serbian CC lays down that compulsory psychiatric treatment and confinement in a medical institution must be terminated by the court if it determines that the need for treatment and confinement of the offender in a medical institution no longer exists (SCC, Article 81 (3)), moreover, compulsory psychiatric treatment at liberty is to last until it is necessary, but for a maximum of 3 years (SCC, Article 82 (5)).

Pursuant to the Serbian CPC, the need for compulsory psychiatric treatment is to be reviewed by the court delivering the first-instance decision at the request of the medical institution or the person subjected to such treatment or ex officio within 9 months. The court will adopt its ruling on the basis of the medical expert opinion. If the proposal to discontinue the measure is rejected, it may be submitted again after the expiry of 6 months from the date of issuance of the ruling (SCPC, Article 531).

Pursuant to the Slovakian CC, compulsory psychiatric treatment must last as long as its purpose requires it (SKCC, § 74 (2)), and compulsory psychiatric treatment in a detention institution must continue until the protection of society against the offender can be ensured through more lenient means (SKCC, § 82 (2)).

According to the SKCC, the court is to review the need for further treatment in a detention institution at least once a year upon the petition of the detention institution. During this procedure, based on expert medical opinion, it may decide: on the further continuation of the detention or on the release of the offender from the detention institution if the reasons for the detention no longer exist. In the case of release from the detention institution, the court is also to decide on further execution of the punishment of imprisonment (SKCC, § 82 (3)).

Pursuant to the SKCPC, the competent court must review the need for continuing compulsory psychiatric treatment minimum once every year, and the procedure for review may also be initiated by the prosecution service, the person under treatment and the general director of the medical institution (SKCPC, § 448 (2–3)).

Based on the above, it may be stated that the laws of all three countries are similar in laying down that compulsory psychiatric treatment is to last until it is necessary, its continuance or termination is to be decided during a review procedure, and the medical expert opinion plays an important role in the adoption of such decision. The difference lies in the timing of ex officio review: it must be conducted every 6 months (in Hungary), after 9 months (in Serbia) or minimum once a year (in Slovakia).

I also share the view that it is essential to provide a well-defined and strict regulation concerning the review of the need to continue compulsory psychiatric treatment and the conditions for terminating such treatment, for example: to ensure the effectiveness of criminal law, the suppression of criminality, the effective medical treatment of the offender and the protection of society. In the effort to reduce crime and protect society, it may be significant to eliminate or decrease the possibility of the offender being released from compulsory

psychiatric treatment unjustifiably or too early and, thus, committing another criminal offence on release. Therefore, I also attribute great importance to the medical expert opinion, which is also provided for by the regulations, in the adoption of the ruling on the continuance or termination of compulsory psychiatric treatment. In the light of the foregoing, it may be stated that the precise and strict regulation of the review and termination of compulsory psychiatric treatment may also contribute to the reduction of crime by potentially decreasing recidivism. The scope of the article does not allow for the exhaustive examination of all the issues concerning the subject, so the analysis could not extend to examining the situation where the convicted offender does not comply with compulsory psychiatric treatment or does not cooperate, or to post-release supervision, which might also be relevant.

3. CLOSING REMARKS

Due to the constraints of limited scope, the paper could not undertake to provide an exhaustive and comprehensive comparison of all the details of the Hungarian, Serbian and Slovakian regulatory backgrounds relating to (preliminary) compulsory psychiatric treatment. Therefore, the purpose of writing this paper was: on the one hand, to raise several points of comparison and, concerning them, to draw attention to the main similarities and differences of the regulatory backgrounds, and on the other hand, to highlight how (preliminary) compulsory psychiatric treatment may contribute to the effectiveness of criminal law and what significance it has in the suppression of criminality.

LIST OF REFERENCES

Legal Sources

2012. évi C. törvény a Büntető Törvénykönyvről (Act C of 2012 on the Criminal Code) (HCC) Available at: https://net.jogtar.hu/jogszabaly?docid=A1200100.TV (28. 3. 2024.)

2017. évi XC. törvény a büntetőeljárásról (Act XC of 2017 on the Code of Criminal Procedure) (HCPC) Available at: https://net.jogtar.hu/jogszabaly?docid=a1700090.tv (28. 3. 2024.)

2013. évi CCXL. törvény a büntetések, az intézkedések, egyes kényszerintézkedések és a szabálysértési elzárás végrehajtásáról) (Act CCXL of 2013 on the execution of punishments, measures, certain coercive measures and confinement for infractions) (HE) Available at: https://net.jogtar.hu/jogszabaly?docid=A1300240.TV (28. 3. 2024.)

Krivični zakonik Republike Srbije (Criminal Code of 2019) (SCC) Available at: https://www.mpravde.gov.rs/files/Criminal%20%20%20Code_2019.pdf (10. 3. 2024.)

Trestný Zákon (Act No. 300/2005 Coll. Criminal Code) (SKCC) Available at: https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2005/300/ (28. 3. 2024.)

Trestný Poriadok (Act No. 301/2005 Coll. Code of Criminal Procedure) (SKCPC) Available at: https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2005/301/20240320 (28. 3. 2024.)

Zakonik o krivičkom postupku Republike Srbije (Criminal Procedure Code) of 2019 (SCPC) Available at: https://mpravde.gov.rs/files/CRIMINAL%20PROCEDURE%20CODE%20%202019.pdf (10. 3. 2024.)

Zakon o izvršenju krivičnih sankcija (Law on Execution of Criminal Sanctions) (SE) Available at: https://www.mpravde.gov.rs/files/LAW_ON_EXECUTION_OF_CRIMINAL_SANCTIONS.pdf (10. 3. 2024.)

Trestný Zákon (Act No. 300/2005 Coll. Criminal Code) (SKCC) Available at: https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2005/300/ (28. 3. 2024.)

Trestný Poriadok (Act No. 301/2005 Coll. Code of Criminal Procedure) (SKCPC) Available at: https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2005/301/20240320 (28. 3. 2024.)

Vyhláška Ministerstva spravodlivosti Slovenskej republiky z 3. septembra 2008, ktorou sa vydáva Poriadok výkonu trestu odňatia slobody (Act No. 368/2008 Coll. on the Execution of Imprisonment) (SKE) Available at: https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2008/368/ (28. 3. 2024.)

UDC: 004.8:34(4-672EU) DOI: 10.56461/iup_rlrc.2024.5.ch12

David MOLNAR*
Faculty of Law, University of Pécs, Hungary

AI UNLEASHED: MASTERING THE MAZE OF THE EU AI ACT

The European Union's Artificial Intelligence Act represents a pioneering endeavour to align the utilization of artificial intelligence (AI) with stringent ethical and safety norms, heralding a transformative phase for various professions. This paper delves into the Act's deliberate attempt to strike a delicate equilibrium between encouraging technological innovation and imposing strict accountability measures, especially in contexts where AI is deemed high-risk. By analyzing the repercussions for critical sectors including healthcare, finance, and technology, we expose the paradoxical nature of compliance: it poses a formidable challenge necessitating comprehensive ethical guidelines, yet simultaneously acts as a stimulus for the development of groundbreaking ethical AI methodologies. Furthermore, we accentuate the worldwide influence of the EU's regulatory framework, providing key strategic recommendations for adeptly manoeuvring through the dynamic AI regulatory environment. In essence, "AI Unleashed: Mastering the Maze of the EU AI Act" encapsulates the transformative potential of regulatory obstacles as avenues for fostering ethical innovation and propelling professional growth.

Keywords: AI regulation, ethical innovation, high-risk AI, compliance, global impact.

1. INTRODUCTION: OVERVIEW OF AI AND ITS SIGNIFICANCE IN MODERN SOCIETY

Artificial intelligence (AI) represents one of the most transformative technologies of the 21st century, profoundly impacting various aspects of modern society. AI refers to the simulation of human intelligence processes by machines, particularly computer systems. This encompasses the processes of learning (the acquisition of information and rules for using the information), reasoning (using rules to reach approximate or definite conclusions), and self-correction (Russell & Norvig, 2021, p. 25). The applications of AI are diverse and pervasive, extending across a range of fields, including healthcare (Jiang

* LLM, ORCID: 0009-0000-5836-4825, e-mail: *molnardavid836@gmail.com*

et al., 2017, p. 235), finance (D'Acunto, Prabhala, & Rossi, 2019, p. 225), transportation (Goodall *et al.*, 2017, p. 210), and entertainment (Sharma & Kumar, 2021, p. 115). This underscores the technology's pervasive influence and ubiquitous presence.

In the field of healthcare, AI technologies have transformed diagnostic processes, personalized treatment plans, and predictive analytics, resulting in enhanced patient outcomes and operational efficiency. For instance, AI-driven diagnostic tools can analyse medical images with remarkable accuracy, often exceeding human capabilities in detecting abnormalities such as tumours (Esteva *et al.*, 2017, p. 117). Similarly, AI-driven predictive analytics in finance facilitate risk assessment and fraud detection, thereby ensuring economic stability and improving decision-making processes (Ngai *et al.*, 2011, p. 565).

Moreover, AI's role in autonomous vehicles and smart infrastructure is poised to reshape urban mobility and logistics, offering solutions to longstanding challenges such as traffic congestion and environmental sustainability (Litman, 2018, p. 5). In the entertainment industry, AI algorithms curate personalized content, thereby transforming user experiences and redefining content consumption patterns (Gomez-Uribe & Hunt, 2015, p. 10).

The societal implications of AI extend beyond mere efficiency and convenience. AI has the potential to address complex global challenges, including climate change, resource management, and public health crises. For example, AI models can predict environmental changes and optimize resource allocation, thereby contributing to sustainable development goals (Rolnick *et al.*, 2019, p. 12). Additionally, during the COVID-19 pandemic, AI played a critical role in tracking the virus's spread, developing vaccines, and managing public health responses (Bullock *et al.*, 2020, p. 810).

However, the rapid advancement of AI also raises significant ethical and safety concerns. Issues such as bias in AI algorithms, data privacy, and the displacement of human labour necessitate robust regulatory frameworks to ensure that AI technologies are developed and deployed responsibly. The European Union's Artificial Intelligence Act represents a pioneering effort to address these challenges, aiming to balance the promotion of technological innovation with the imposition of stringent ethical and safety standards.

This paper explores the EU AI Act's structured approach to regulating AI, focusing on its three-tier framework and the implications for high-risk AI applications. By examining the impact on critical sectors and the broader global context, this study seeks to provide strategic insights for navigating the dynamic regulatory landscape and fostering ethical AI innovation.

2. HISTORICAL CONTEXT

2.1. The Evolution of Artificial Intelligence Technologies

The development of artificial intelligence (AI) technologies has a rich history, marked by significant milestones that have transformed it from a theoretical concept to a practical and influential tool in modern society. The term "artificial intelligence" was first used in 1956 by John McCarthy, who is regarded as one of the founding figures of AI. This period, known as the Dartmouth Conference, is widely regarded as the birth of artificial intelligence as a field of research (McCarthy *et al.*, 1955). The initial research

in the field of artificial intelligence concentrated on symbolic AI, which involved the manipulation of symbols and the creation of rule-based systems that simulated human thought (Moor, 2006, p. 88).

The 1960s and 1970s saw the development of fundamental algorithms and the first AI programs capable of performing tasks such as playing chess and solving algebraic problems. Notable examples include Logic Theorist, which was capable of proving mathematical theorems (Newell & Simon, 2016, p. 285), and ELIZA, an early natural language processing program designed to simulate conversation (Weizenbaum, 1966, p. 40).

The 1980s marked the advent of the expert systems era, which aimed to emulate the decision-making abilities of human experts in specific domains. These systems, such as MYCIN for medical diagnostics, demonstrated the potential of artificial intelligence to handle complex, specialized tasks (Feigenbaum, 1981, p. 95). However, the limitations of rule-based systems and the computational power required led to a decline in enthusiasm, often referred to as the "artificial intelligence winter" (Smith & Tsotsos, 1998, p. 21).

The 1990s and 2000s saw a resurgence in artificial intelligence, brought about by the development of machine learning, a subfield of artificial intelligence that focuses on developing algorithms that allow computers to learn from data and make predictions based on that data. The advancement of more powerful computers and the accessibility of voluminous data facilitated breakthroughs in neural networks, leading to the modern era of deep learning (LeCun, Bengio & Hinton, 2015, p. 438).

The incorporation of these AI technologies into a wide range of applications is a current trend. These include autonomous vehicles like Teslas, health diagnostics, financial modelling, and personalized digital assistants like Amazon's Alexa or Apple's Siri on iPhones. These advances are underpinned by sophisticated algorithms, vast amounts of data, and significant computational resources. This highlights the transformative potential of AI across sectors (Russell & Norvig, 2021, p. 580).

2.2. Previous Regulatory Experiments and Their Results

The rapid development and widespread deployment of AI technologies have necessitated the development of regulatory frameworks to address the ethical, legal, and societal implications. Early regulatory attempts focused primarily on data protection and privacy, exemplified by the European Union's General Data Protection Regulation (GDPR), which entered into force in 2018. The GDPR established rigorous guidelines for data collection, processing, and storage, with the objective of safeguarding individuals' privacy rights in the context of the growing prevalence of big data and artificial intelligence (Center for Information Policy Leadership - Hunton Andrews Kurth, 2020, p. 3).

One of the earliest significant initiatives to directly address AI was the publication of the European Commission's High-Level Expert Group on Trusted AI Ethical Guidelines in 2019. These guidelines emphasized principles such as human agency, transparency, accountability, and robustness, laying the groundwork for more comprehensive regulatory action (European Commission, 2019).

In 2020, the European Commission presented a White Paper on Artificial Intelligence, which outlined policy options to foster the development of AI, while also addressing the potential risks. This document served as a precursor to the proposed AI law, emphasizing the necessity for a risk-based regulatory approach that differentiates between various applications of AI based on their potential societal impact (European Commission, 2020).

The outcomes of these regulatory experiments have been somewhat inconsistent. While the General Data Protection Regulation (GDPR) has significantly enhanced data protection standards on a global scale, it has also imposed significant compliance costs on organizations. The ethical guidelines for trusted AI have been lauded for their comprehensive approach, yet they have also been criticized for their non-binding nature, which limits their enforceability (Binns, 2018, p. 152).

The proposed AI Act seeks to build upon previous efforts by introducing binding regulations that address the specific challenges posed by AI technologies. The Act establishes a legal framework that categorizes AI applications according to their level of risk, thereby attempting to achieve a balance between the need to promote innovation and the need to protect public interests and fundamental rights. The emphasis on harmonized regulations across the EU is designed to prevent market fragmentation and ensure legal certainty for AI developers and users (EU AI Act, 2024).

3. THE STRUCTURE OF THE EU AI ACT

The structure of the EU legal act is based on a three-tier framework for categorizing AI systems according to their level of risk. This approach provides a balanced regulatory framework that allows for innovation while simultaneously protecting the public interest, ethical standards, and safety norms. The framework categorizes AI applications into three distinct categories: minimal and limited risk, high risk, and unacceptable risk. Each category is associated with specific regulatory requirements and consequences (EU AI Act, 2024).

3.1. Level 1 and 2: Low-Risk AI Systems (Minimal and Limited Risk)

Artificial intelligence systems classified under Level 1 are deemed to present minimal or limited risk to users and society at large. These systems are not associated with significant implications for fundamental rights, safety, or the well-being of individuals like the high-risk and unacceptable systems. Consequently, they are subject to the most lenient regulatory requirements. This level is further subdivided into two categories: minimal risk and limited risk AI systems. Each category is subject to distinct regulatory implications (Menengola, Gabardo & González Sanmiguel, 2023, p. 50).

Minimal-risk AI systems are those that pose virtually no risk to users and society. Examples of these systems include applications such as AI-enabled video games and spam filters. These systems are free to be used without regulatory intervention, as they represent only minimal or no risk to citizens' rights or safety. The vast majority of AI

systems currently used in the EU fall into this category. For instance, spam filters help manage and organize email inboxes by filtering out unwanted or harmful messages, while AI-powered games offer entertainment without posing significant risks to players (European Commission, 2024a).

The implications of this classification for minimal-risk AI systems are profound for both developers and users. Developers benefit from a reduced regulatory burden, facilitating rapid innovation and deployment of a wide range of AI applications. For users, this translates to enhanced services and products that are safe and trustworthy, without the delay often associated with stringent compliance processes. The EU AI Act's approach to minimal-risk AI systems reflects a broader trend in technology regulation, where flexibility and innovation are encouraged in areas deemed to pose lower risks (Labadze, Grigolia & Machaidze, 2023; Finocchiaro, 2024; Ebers & Schaar, 2023).

While still considered low-risk, limited-risk AI systems are subject to minimal transparency obligations. This classification includes applications like customer service chatbots, which enhance user experience without making critical decisions. These chatbots must disclose their AI nature, allowing users to decide whether to continue using them. The regulatory approach for limited-risk AI systems ensures that users are informed about the AI they interact with, which is essential for building trust and maintaining ethical standards (European Commission, 2024b; Labadze, Grigolia & Machaidze, 2023; Finocchiaro, 2024; Ebers & Schaar, 2023).

The EU AI Act provides a balanced approach to regulation, distinguishing between minimal and limited-risk AI systems. Minimal risk systems enjoy regulatory freedom, fostering innovation, while limited-risk systems must meet basic transparency requirements to ensure user trust. This framework allows developers to create valuable AI applications without excessive regulation, while users can trust in their safety and ethical compliance.

3.2. Level 3: High-Risk AI Systems

Artificial intelligence systems classified as Level 3 are regarded as posing a considerable risk or systemic risk due to their capacity to exert a profound impact on the rights, security, and well-being of individuals and they can also impact the Union's market significantly. These systems are typically utilized in critical sectors such as healthcare, finance, and transportation, where errors or biases can have grave consequences. Examples of high-risk AI applications include medical diagnostic tools, automatic credit authorization systems, and autonomous driving technologies (EU AI Act, 2024; European Commission, 2024b).

High-risk AI systems are those that can affect essential aspects of people's lives and liberties. For example, an AI system used in healthcare to diagnose diseases must be accurate and reliable because a wrong diagnosis can lead to inadequate treatment, posing serious health risks to patients (Rajkomar *et al*., 2018, p. 868). Similarly, AI applications in finance, such as those used for credit scoring, must ensure fairness and transparency to prevent discriminatory practices that could unjustly deny individuals access

to financial services (Bono, Croxon & Kites, 2020, p. 590). The significant influence of these systems on critical decisions underscores the need for rigorous oversight and stringent regulatory measures.

High-risk AI systems are subject to rigorous regulatory requirements to ensure their safe and ethical deployment. These include mandatory risk assessments, transparency obligations, and robust data governance measures. Providers of high-risk AI systems must ensure that their products are designed and implemented in a manner that mitigates potential risks. This often involves adhering to specific standards for accuracy, robustness, and cybersecurity. The European Commission highlights in the regulation that these requirements are essential for maintaining the integrity and reliability of AI systems in critical applications (EU AI Act, 2024).

Compliance also entails continuous monitoring and reporting of the AI system's performance and impact. Developers must establish mechanisms for human oversight and intervention to address any unforeseen issues that may arise during the system's operation. These stringent requirements are intended to prevent harm and promote trust in AI technologies deployed in sensitive areas. The focus on transparency and accountability helps ensure that high-risk AI systems are used responsibly and that their benefits are maximized while minimizing potential harm (EU AI Act, 2024).

The EU AI Act mandates that high-risk AI systems undergo conformity assessments to verify that they meet the necessary standards before they can be deployed. These assessments are designed to evaluate the system's compliance with regulatory requirements and to identify and address any potential risks. By implementing these measures, the EU aims to create a safe and trustworthy environment for the use of high-risk AI systems. This comprehensive approach is intended to mitigate the risks associated with high-impact AI applications, ensuring that they operate within defined ethical and safety boundaries (EU AI Act, 2024).

For example, in the healthcare sector, AI diagnostic tools must be rigorously tested to ensure they do not produce false positives or negatives, which could lead to serious medical consequences. The EU AI Act stipulates that such systems must be transparent in their decision-making processes, providing clear information on how diagnoses are determined. This transparency allows medical professionals to understand and trust the AI's recommendations, integrating them effectively into patient care (Antun *et al.*, 2020, p. 30092; EU AI Act, 2024).

In the financial sector, AI systems used for credit scoring must be designed to prevent bias and discrimination. The Act requires that these systems undergo regular audits to ensure compliance with fairness standards. Transparency is also crucial here, as individuals affected by AI decisions must be able to understand and challenge those decisions if necessary. By mandating these practices, the EU AI Act aims to prevent the perpetuation of existing biases and promote equitable treatment across all demographic groups (EU AI Act, 2024).

Autonomous driving technologies represent another high-risk application of AI. These systems must adhere to the highest standards of safety and reliability, as any failure could result in significant harm to individuals and property. The EU AI Act requires

that autonomous vehicles be subject to rigorous testing and continuous monitoring to ensure they operate safely in all conditions. Moreover, the Act mandates the inclusion of fail-safe mechanisms that allow human intervention if the AI system encounters unforeseen issues (EU AI Act, 2024).

The EU's approach to regulating high-risk AI systems is informed by a broader commitment to ethical AI development. As noted by Floridi *et al*. (2018, pp. 689-707), ethical guidelines for AI emphasize the need for transparency, accountability, and fairness in AI applications. These principles are embedded within the regulatory framework of the EU AI Act, ensuring that high-risk AI systems are developed and deployed in a manner that respects fundamental rights and societal values (EU AI Act, 2024).

3.3. Level 4: Unacceptable Risk AI Systems

Unacceptable risk AI systems are defined in the AI Act as those that pose a significant and irreparable threat to security, fundamental rights and public interests. These systems are banned outright due to their potential to cause significant harm. The law identifies several specific applications of AI that fall into this category, reflecting the EU's commitment to protecting human rights and societal values. Examples of AI systems that are considered to pose unacceptable risks include (EU AI Act, 2024; MIT Technology Review, 2024):

Social Scoring Systems: AI systems used for social scoring, which evaluate or classify individuals based on their social behaviour, economic status, or personal characteristics, are strictly prohibited. This prohibition is based on the potential for such systems to lead to widespread discrimination, social exclusion, and violation of privacy (EU AI Act, 2024; MIT Technology Review, 2024).

Biometric Surveillance: Real-time biometric identification systems deployed in public spaces without explicit user consent are also banned. The use of facial recognition and other biometric technologies in public surveillance raises significant concerns about privacy, mass surveillance, and the potential misuse of personal data (Clifford Chance, 2021).

Exploitation of Vulnerabilities: AI systems designed to exploit vulnerabilities of specific groups, such as children, the elderly, or individuals with disabilities, are prohibited. These systems pose unacceptable risks as they can manipulate vulnerable populations in ways that undermine their autonomy and well-being (Züehlke, 2023).

Automated Behavioral Manipulation: AI systems intended to manipulate human behaviour in a way that causes physical or psychological harm are also banned. This includes systems that can subtly influence users' decisions through subliminal techniques or deceptive practices (Brookings, 2024).

The rationale behind these prohibitions is rooted in the need to protect fundamental human rights and ensure that AI technologies are developed and deployed in a manner that upholds ethical standards and societal values. The AI Act's focus on preventing the deployment of AI systems with unacceptable risks is a reflection of the broader regulatory philosophy that prioritizes human dignity, privacy, and fairness. By categorically banning these high-risk applications, the AI Act aims to prevent scenarios where AI technologies could be used to harm individuals or society at large. This regulatory stance is aligned with

the EU's broader commitment to ethical AI and is intended to set a global benchmark for responsible AI governance (Shafafi & Sabel, 2024; European Commission, 2019).

In conclusion, the classification and regulation of AI systems that present unacceptable risks under the AI Act represents a rigorous and ethically informed approach to the management of the potential harms associated with advanced AI technologies. The Act's categorical prohibition of AI applications that pose significant risks to fundamental rights and public safety is intended to safeguard individuals and society from the most egregious abuses of AI.

4. THE INNOVATION PARADOX OF REGULATION IN THE CONTEXT OF THE AI ACT

In a rapidly evolving field of artificial intelligence, the EU AI Act plays a pivotal role in establishing a regulatory framework that ensures the ethical development and deployment of AI technologies, while safeguarding public interests. However, this regulatory imperative also highlights the so-called "innovation paradox of regulation" which posits an inherent tension between promoting innovation and regulating to achieve a balance that ensures safety, transparency, and accountability (Sabl, 2021, p. 3).

On the one hand, the regulations pertaining to AI are designed to mitigate the aforementioned risks associated with these technologies. Among the potential risks associated with AI technologies are the possibility of algorithmic bias, privacy threats, and other unintended consequences that could have adverse effects. It is imperative that regulations establish clear guidelines and standards to ensure the responsible development and use of AI systems, with the aim of protecting individuals and society from potential harm. In our case, the AI Act of the European Union is designed to establish a legal framework wherein AI systems are organized based on the risks they pose. This framework imposes more rigorous requirements for high-risk AI applications, with the aim of preventing their misapplication and ensuring their ethical use (Turk, 2024, p. 92; Pehlivan, 2024, p. 15).

On the other hand, the regulatory environment has the potential to impede innovation. The extensive compliance requirements pertaining to risk management, data governance, and technical documentation, among other aspects, are particularly onerous for developers. It is not uncommon for such requirements to necessitate significant investments in time, resources, and expertise, which can sometimes result in increased development costs and extended lead times for the commercialization of AI systems. Consequently, this could result in a reduction in the rate of innovation and an unfavourable competitive environment for companies, particularly smaller organizations and startups, in comparison to larger or more established entities (Sabl, 2021, p. 5; Wagner *et al.*, 2024, p. 24).

The paradox is even more striking when it comes to high-risk AI systems, which include some of the most innovative and impactful AI uses. These systems should be strictly regulated because of their potential to have a strong impact on fundamental rights, safety, and public interests. While these regulations are important for ensuring

ethical and safe AI deployment, they significantly raise the barrier of entry to any innovation, allowing very few new inventions to make it into the marketplace and establish a foothold. This can dampen diversity and dynamism in the field of AI and concentrate market power in the hands of a few large and established firms (Pehlivan, 2024, p. 20; de Graaf & Veldt, 2022, p. 832).

Furthermore, the inflexibility of the regulatory framework is ill-suited to accommodate the rapid advancements in AI technologies. As artificial intelligence continues to advance at a rapid pace, new risks and ethical challenges are emerging that existing regulations may be unable to fully address. This discrepancy may impede firms' capacity to continue innovating freely and responding to emerging challenges, thereby hindering the growth and development of the AI sector (Mendes, Doneda & Almeida, 2023, p. 35).

Notwithstanding these obstacles, the EU AI Act is oriented towards rigorous regulation rather than the promotion of innovation. The principal objective of the Act is to guarantee public confidence in AI systems among the citizens of the European Union, although this is achieved at a significant cost. The Act's objective is to establish a framework that prioritizes safety, transparency, and accountability in order to foster public trust in AI technologies. Nevertheless, this process of fostering trust entails extensive regulatory oversight, which imposes a considerable burden on developers and companies. The emphasis on ethical AI development and the protection of fundamental rights is laudable; however, it can also result in a rigid environment that may impede the dynamic nature of AI innovation (Pehlivan, 2024, p. 22; Turk, 2024, p. 52).

The EU AI Act's rigorous compliance requirements, which encompass detailed risk management, data governance, technical documentation, transparency, human oversight, robustness, and cybersecurity, necessitate significant investments in time, resources, and expertise. This comprehensive regulatory approach results in elevated development costs and extended timeframes for the introduction of AI systems to the market. This may impede innovation and diminish the competitive edge of European AI enterprises on a global scale (Turk, 2024, p. 55).

5. CONCLUSIONS: THE WAY FORWARD

The EU AI Act is a significant step towards creating a comprehensive regulatory framework for Artificial Intelligence, balancing its benefits with ethical and safety standards. This regulatory environment, however, will be challenging and will require constant adjustments to promote innovation while protecting public interests.

The stringent compliance requirements burden developers, especially smaller enterprises and startups. Continuous review and revision of the process are necessary. To keep the regulatory framework relevant, there should be ongoing dialogue between policymakers, developers, and stakeholders. A flexible regime of regulations that can adapt to technological improvements, incorporating research and feedback from the AI community, is essential (Mancheva, 2022).

Despite the stringent environment, regulations must support innovation. Providing financial incentives, grants, and technical assistance can help SMEs comply with

regulations without stifling their innovative potential. This support allows startups to focus on innovation while meeting regulatory requirements (Mancheva, 2022).

Continuous monitoring and stakeholder feedback in AI systems are crucial for early issue detection and ensuring safety and reliability. These measures, conducted periodically, can modify and enhance regulations, with performance evaluations through audits and user feedback systems (Figalist *et al.*, 2021, p. 106460).

In conclusion, while the AI Act is a pioneering legislative initiative, it requires ongoing analysis and adaptation. Continuous improvement of this regulatory regime will ensure AI technologies develop in a way that safeguards fundamental rights and enhances quality of life. The rapid pace of innovation demands an equally rapid evolution of regulatory frameworks. This involves balancing innovation and compliance, promoting ethical AI development, facilitating cross-border collaboration, and establishing robust monitoring and feedback mechanisms. Such measures are vital for creating a regulatory environment that supports innovation while protecting public interests and fostering responsible and beneficial AI development.

LIST OF REFERENCES

Antun, V. *et al*. 2020. On instabilities of deep learning in image reconstruction and the potential costs of AI. *Proceedings of the National Academy of Sciences*, 117(48), pp. 30088-30095. https://doi.org/10.1073/pnas.1907377117

Binns, R. 2018. Fairness in Machine Learning: Lessons from Political Philosophy. *Proceedings of the 1st Conference on Fairness, Accountability and Transparency, PMLR*, 81, pp. 149-159.

Bono, T., Croxson, K. & Giles, A. 2021. Algorithmic fairness in credit scoring, *Oxford Review of Economic Policy*, 37(3), pp. 585–617. https://doi.org/10.1093/oxrep/grab020

Bullock, J. *et al*. 2020. Mapping the landscape of artificial intelligence applications against COVID-19. *Journal of Artificial Intelligence Research*, 69, pp. 807-845. https://doi.org/10.1613/jair.1.12162

Clifford Chance. 2021. The future of AI regulation in Europe and its global impact. Available at: https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2021/05/the-future-of-ai-regulation-in-europe-and-its-global-impact.pdf (11. 7. 2024).

D'Acunto, F., Prabhala, N. & Rossi, A. 2019. The Impact of Artificial Intelligence on the Financial Services Industry. *Journal of Financial Economics*, 133(2), pp. 223-251.

de Graaf, T. & Veldt, B. 2022. The AI Act and Its Impact on Product Safety, Contracts and Liability, *European Review of Private Law*, 30(5), pp. 803-834. https://doi.org/10.54648/erpl2022038

Esteva, A. *et al*. 2017. Dermatologist-level classification of skin cancer with deep neural networks. *Nature,* 542(7639), pp. 115-118. https://doi.org/10.1038/nature21056

Ebers, M. & Schaar, P. 2023. Risk Management in the Artificial Intelligence Act. *European Journal of Risk Regulation*, 14(1), pp. 34-58.

Feigenbaum, E. A. 1981. Knowledge engineering: The applied side of artificial intelligence. *Annals of the New York Academy of Sciences*, 426(1), pp. 91-107. https://doi.org/10.1111/j.1749-6632.1984.tb16513.x

Figalist, I. *et al*. 2021. Fast and curious: A model for building efficient monitoring- and decision-making frameworks based on quantitative data. *Information & Software Technology*, 130, 106458. Available at: https://www.sciencedirect.com/science/article/abs/pii/S0950584920302044 (10. 10. 2024). https://doi.org/10.1016/j.infsof.2020.106458

Finocchiaro, G. 2024. The regulation of artificial intelligence. *AI & SOCIETY*, 39, pp. 1961-1968. https://doi.org/10.1007/s00146-023-01650-z

Floridi, L. *et al*. 2018. AI4People—An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations. *Minds & Machines*, 28, pp. 689–707. https://doi.org/10.1007/s11023-018-9482-5

Goodall, N. J. *et al*. 2017. AI in Transportation: Current and Future Developments. *Transportation Research Part C: Emerging Technologies*, 77, pp. 207-225. https://doi.org/10.1016/j.trc.2017.01.022

Gomez-Uribe, C. A. & Hunt, N. 2015. The Netflix Recommender System: Algorithms, Business Value, and Innovation. *ACM Transactions on Management Information Systems*, 6(4), pp. 1-19. https://doi.org/10.1145/2843948

Jiang, F. *et al*. 2017. Artificial intelligence in healthcare: past, present and future. *Stroke and Vascular Neurology*, 2(4), pp. 230-243. https://doi.org/10.1136/svn-2017-000101

Labadze, L., Grigolia, M. & Machaidze, L. 2023. Role of AI chatbots in education: systematic literature review. *Educational Technology Journal*, 15(2), pp. 123-145. https://doi.org/10.1186/s41239-023-00426-1

LeCun, Y., Bengio, Y. & Hinton, G. 2015. Deep learning. *Nature*, 521(7553), pp. 436-444. https://doi.org/10.1038/nature14539

Mancheva, G. (2022). European regulatory framework on artificial intelligence in the SME sector – a risk based approach. In: *Artificial intelligence in the field of security – advantages and threats*, Plovdiv, pp. 175-179.

McCarthy, J. *et al*. 1955. A proposal for the Dartmouth summer research project on artificial intelligence. Available at: https://www-formal.stanford.edu/jmc/history/dartmouth/dartmouth.html (3. 7. 2024).

Menengola, E., Gabardo, E. & González Sanmiguel, N. N. 2023. The proposal of the European regulation on artificial intelligence. *Sequência: Estudos Jurídicos e Políticos*, 44(91), pp. 45-66. https://doi.org/10.5007/2177-7055.2022.e91435

Mendes, L. S., Doneda, D. & Almeida, V. 2023. On the Development of AI Governance Frameworks. *IEEE Internet Computing*, 27(1), pp. 32-40. https://doi.org/10.1109/MIC.2022.3186030

MIT Technology Review. 2024. What's next for AI regulation in 2024? Available at: https://www.technologyreview.com/2024/01/05/1086203/whats-next-ai-regulation-2024/ (11. 7. 2024).

Moor, J. 2006. The Dartmouth College Artificial Intelligence Conference: The Next Fifty Years. *AI Magazine*, 27(4), pp. 87-89. https://doi.org/10.1609/aimag.v27i4.1911

Newell, A. & Simon, H. A. 2016. GPS, a program that simulates human thought. *Computers and Thought*, 4, pp. 279-293.
Ngai, E. W. *et al*. 2011. The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. *Decision Support Systems*, 50(3), pp. 559-569. https://doi.org/10.1016/j.dss.2010.08.006
Pehlivan, C. N. 2024. The EU Artificial Intelligence (AI) Act: An Introduction. *Global Privacy Law Review*, 5(1), pp. 12-28. https://doi.org/10.54648/GPLR2024004
Rajkomar, A. *et al*. 2018. Ensuring Fairness in Machine Learning to Advance Health Equity. *Annals of Internal Medicine*, 169(12), pp. 866-872. https://doi.org/10.7326/M18-1990
Rolnick, D. *et al*. 2019. Tackling climate change with machine learning. *ACM Computing Surveys*, 55(2), pp. 1-96. https://doi.org/10.1145/3485128
Russell, S. J. & Norvig, P. 2021. *Artificial Intelligence: A Modern Approach*. New York: Pearson Education.
Sabl, A. 2021. The paradox of innovation. *Journal of Economic Behavior and Organization*, 183, pp. 1-16.
Shafafi, P. & Sabel, M. 2024. So far in 2024: AI innovation, regulation, and the ethical frontier. Designit. Available at: https://www.designit.com/stories/point-of-view/so-far-in-2024-ai-innovation-regulation-ethical (11. 7. 2024).
Sharma, A. & Kumar, A. 2021. Applications of AI in Various Sectors: A Review. *International Journal of Advanced Research in Artificial Intelligence*, 10(3), pp. 112-125.
Smith, C. & Tsotsos, J. K. 1998. The History of Artificial Intelligence. *AI Magazine*, 19(3), pp. 19-31.
Turk, Ž. 2024. Regulating artificial intelligence: A technology-independent approach. *European View*, 23(1), pp. 89-104. https://doi.org/10.1177/17816858241242890
Wagner, M. *et al*. 2024. Navigating the Upcoming European Union AI Act. *IEEE Software*, 41(1), pp. 22-30. https://doi.org/10.1109/MS.2023.3322913
Weizenbaum, J. 1966. ELIZA—a computer program for the study of natural language communication between man and machine. *Communications of the ACM*, 9(1), pp. 36-45. https://doi.org/10.1145/365153.365168

Internet Sources

Brookings. 2024. Regulating general-purpose AI: Areas of convergence and divergence across the EU and the US. Available at: https://www.brookings.edu/articles/regulating-general-purpose-ai-areas-of-convergence-and-divergence-across-the-eu-and-the-us/ (11. 7. 2024).
Center for Information Policy Leadership - Hunton Andrews Kurth. 2020. How GDPR Regulates AI'. Information Policy Centre. Available at: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl-hunton_andrews_kurth_legal_note_-_how_gdpr_regulates_ai__12_march_2020_.pdf (9.7.2024).
European Commission. 2019. Ethics guidelines for trustworthy AI. Available at: https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai (9. 7. 2024).

European Commission. 2020. White Paper on Artificial Intelligence: a European approach to excellence and trust. Available at: https://commission.europa.eu/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en (11. 7. 2024).
European Commission. 2024a. Excellence and Trust in Artificial Intelligence. Available at: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/excellence-and-trust-artificial-intelligence_en (11. 7. 2024).
European Commission. 2024b. Regulatory framework proposal on artificial intelligence. Available at: https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai (11. 7. 2024).
Züehlke. 2023. EU AI Act: how AI law will impact innovation. Available at: https://www.zuehlke.com/en/insights/how-will-the-eu-ai-act-impact-ai-innovation (11. 7. 2024).

Legal Sources

EU AI Act. 2024. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonized rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2018/2002 Chapter I: General Provisions Article 1: Subject Matter) Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401689 (3. 7. 2024).

UDC: 342.72/.73:004.8 DOI: 10.56461/iup_rlrc.2024.5.ch13

*Miloš STANIĆ**
Institute of Comparative Law, Belgrade, Serbia
*Ljubomir TINTOR***
Institute of Comparative Law, Belgrade, Serbia

HUMAN RIGHTS AND ARTIFICIAL INTELLIGENCE – INTERNATIONAL PUBLIC LAW AND CONSTITUTIONAL ASPECTS***

We are witnessing that society and social relations are changing particularly rapidly in the last few decades. Evidently, it is a continuous trend that places numerous challenges before the law. One of those aspects is the development of artificial intelligence, which has a special impact on the matter of human rights, in its international public law and constitutional aspects. The authors in this paper pay special attention to three groups of questions. The first deals with the current normative situation in this area and potential problems in that sense. The second group of questions refers to possible problems that could arise in the future, which, to the extent possible, are perceived by the authors themselves. The third is the consideration of these issues, from the aspect of the situation in the Republic of Serbia and in Europe.

Keywords: human rights, artificial intelligence, international public law, constitutional law.

* PhD, Senior Research Associate, ORCID: 0000-0001-8849-7282, e-mail: *m.stanic@iup.rs*

** LLM, Research Associate, ORCID: 0009-0005-7565-154X, e-mail: *lj.tintor@iup.rs*

*** This paper is a result of the research conducted at the Institute of Comparative Law financed by the Ministry of Science, Technological Development and Innovation of the Republic of Serbia under the Contract on realisation and financing scientific research of SRO in 2024 registered under no. 451-03-66/2024-03/200049.

Miloš Stanić, PhD, was appointed mentor to Ljubomir Tintor, LLM, a Research Associate at the Institute of Comparative Law and a PhD candidate at the Faculty of Law, University of Belgrade by the Decision of the Scientific Council of the Institute of Comparative Law No. 772 of 5 October 2023. This paper is one of the results of mentoring with the mentioned candidate.

1. INTRODUCTION

Despite its expanding presence across numerous aspects of our lives, there is no extensively accepted description of artificial intelligence (Reddy, 2022, pp. 1–44). John McCarthy and colleagues first coined the term "artificial intelligence" in 1956. They described it as follows: "An attempt will be made to find how to make machines use language, form abstractions and concepts, solve kinds of problems now reserved for humans, and improve themselves (…). For the present purpose, the artificial intelligence problem is taken to be that of making a machine behave in ways that would be called intelligent if a human were so behaving." (Lee, 2022, p. 6). AI is the simulation of intelligence processes by machines, especially computer systems. As some authors say (Reddy, 2022, p. 4), artificial intelligence (AI), in other words, Computer Wisdom, is one analogous technical field that's converting society into one among robots and machines. AI includes machine knowledge, language processing, big data analytics, algorithms, and far more. This term is used in a broad manner in diverse contexts. The Oxford Dictionary defines AI as "the theory and development of computer systems able to perform tasks normally requiring human intelligence" (Lee, 2022, p. 1). Nicolau (2019, p. 64) stated that artificial intelligence is a smart digital system that learns on its own, develops its own search and learning systems, can even have its own language without being understood by humans, develops its own artificial neural networks, can write its own programs, but most important is the fact that it has decision-making power. Depending on the knowledge it has, it can decide the actions that it does or does not do, being able to predict their result. In other words, AI is no longer dependent on human command.

As some other authors say (Muller, 2020, p. 3) artificial intelligence systems are software and possibly also hardware systems designed by humans that, given a complex goal, act in the physical or digital dimension by perceiving their environment through data acquisition, interpreting the collected structured or unstructured data, reasoning on the knowledge, or processing the information, derived from this data and deciding the best actions to take to achieve the given goal. Often, AI is described as a collection of technologies that combine data, algorithms and computing power. OECD defines an artificial intelligence system as a machine-based system that is designed to operate with varying levels of autonomy and that can, for explicit or implicit objectives, generate output such as predictions, recommendations, or decisions influencing physical or virtual environments. Anyway, AI has immense potential to enhance human capabilities and improve decision-making processes (Al-Taj, Polok & Rana, 2023, p. 94). As Quintavalla and Temperman claimed (2023a, p. 569), the use of artificial intelligence has considerably affected most, if not all, domains of human life, cause AI has a myriad of applications that have already been introduced into society: biometric recognition, object recognition, risk and success prediction, algorithmic decision making or support, automatic translation, recommender systems, and so on. These applications have found their way into sectors such as law enforcement, justice, human resource management, financial services, transport, healthcare, public services (Muller, 2020, p. 3).

As a consequence of all these processes, some authors (Quintavalla & Temperman, 2023b, p. 4) say that artificial intelligence and human rights are currently interacting within one and the same world and their inevitable dynamics no longer goes unnoticed, though such dynamics simultaneously poses tremendous and tremendously pertinent legal, ethical, technological, and societal questions. Human rights are essential to all or any people, regardless of the race, commerce, nation, language, religion, or the other status (Reddy, 2022, p. 4) and in Western thought, they are regarded as the supreme norm of law and form the basis for most legal systems. According to the majority of experts on international law, human rights are not merely an enumeration of individual rights, but rather form a self-contained regime. The integral pillar of this regime is an anthropology based on the self-determination and autonomy of the human being. According to this understanding, human rights oblige the state and other social organizations to observe certain principles and procedures when dealing with subordinates (Kriebitz & Lütge, 2020, p. 86). As Quintavalla and Temperman stated (2023a, p. 569), the relationship between AI technology and human rights is a web of multilateral coexisting relationships. Human rights principles can provide an effective standard for measuring the societal acceptance of AI technology. Human rights can have an impact on AI, as well. AI technology and human rights can be in principle both friends and foes. However, it is the society which decides what type of impact AI technology makes, that is, whether it will become a friend or a foe of human rights.

Back in the history, both early artificial intelligence milestones and the modern human rights codification process have their origins in the 1940s. In the 1940s, important early AI foundations saw the light of day, while on 10 December 1948, the General Assembly of the newly founded United Nations created as per the 1945 UN Charter and aiming to prevent the atrocities the League of Nations helplessly failed to avert, adopted the Universal Declaration of Human Rights (UDHR), positing in the Preamble 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" (Quintavalla & Temperman, 2023b, p. 3). The UDHR, consisting of a combination of civil and political rights on the one hand, and social, economic, and cultural rights on the other, serves as the milestone for contemporary human rights instrument up until today, also influencing numerous subsequent international and national bills of rights. Their overlapping history notwithstanding the fact that the two phenomena, AI and human rights, led fairly separate existences for their first fifty or sixty years or so. It is only in the last decade that their paths have converged, that the two forces meet, that they support each other, or, as may happen as well, that they conflict, causing small or major clashes (Quintavalla & Temperman, 2023b, p. 3).

2. INTERNATIONAL PUBLIC LAW AND AI

As some authors say (Martsenko, 2022, p. 317), the legal regulation of AI requires the hard work of lawyers both at the global and regional levels. Some others claim (Lane, 2022, p. 918) that the ongoing development of AI technologies presents international law with a number of challenges. These include the need for new laws, legal certainty,

incorrect scope of existing laws and legal obsolescence. There are, however, several important initiatives that could have an impact on the protection of human rights and contribute to clarifying applicable standards (Lane, 2022, p. 927). Within international fora, pioneering benchmarking has gradually commenced in the form of guidelines and recommendations at both international and regional levels (Quintavalla & Temperman, 2023b, p. 4). Discussion related to the impact of AI on human rights has been present in global forums for many years. In 2021 UN Commissioner for Human Rights said countries should expressly ban AI applications that did not comply with the international human rights law (Al-Taj, Polok & Rana, 2023, p. 97).

AI-related concerns into that framework have so far been piecemeal and fragmented. Despite pleas to update international law in light of AI challenges, international organizations have not produced binding treaties; instead, they have issued multiple resolutions and directives to address business responsibility, data governance, privacy, and so on. The United Nations system offers a broad range of applicable, if vaguely defined, rights that can be interpreted as AI-relevant. Already mentioned, the Universal Declaration of Human Rights is broadly cited as a generic, flexible, and agreed-upon document to derive a set of rights and obligations for the age of AI. The Declaration is an intentionally generic document; thus, the specification of rights and obligations is left to other instruments. The International Covenant on Civil and Political Rights comes closest to an international treaty capable of anticipating some of the concerns around today's new and emerging technologies, AI included. Finally, arguably, the most consequential document from the standpoint of regulating private business is a set of guidelines: as calls to consider businesses alongside state actors as duty-bearers with human rights obligations has gained traction in the recent past, the UN Guiding Principles on Business and Human Rights (2011) have stepped in to set the standards for the roles and responsibilities of businesses with implications for their development and deployment of technology (Bakiner, 2023, p. 4). The Universal Declaration of Human Rights is an absolute cornerstone of the human rights regime and is considered the most significant human rights document. Thus, already during the work on the declaration, the international community noticed the need to prepare binding documents. This task was completed in 1966 when the International Covenant on Civil and Political Rights (ICCPR) and the International Covenant on Economic, Social, and Cultural Rights (ICESCR) were adopted by the UN General Assembly. These documents are known by the collective name International Bill of Human Rights (Al-Taj, Polok & Rana, 2023, p. 95). Another important example is the work of the UN Educational, Scientific and Cultural Organization (UNESCO). UNESCO appointed a group of 24 experts to draft a "Recommendation on the Ethics of Artificial Intelligence," to provide "an ethical guiding compass and a global normative bedrock allowing to build a strong respect for the rule of law in the digital world." After receiving input from various stakeholders on earlier drafts, the final text of the Recommendation was adopted in November 2021. Although framed as an ethics-based initiative, an objective of UNESCO's Recommendation is "to protect, promote and respect human rights and fundamental freedoms, human dignity and equality," (Lane, 2022, p. 930).

2.1. Regional Initiatives and AI

At the regional level, the European Union (EU) has taken the lead in legislating digital and AI regulation. Thus, in Resolution 2015/2103 (INL) of the European Parliament dated 16 February 2017 with the recommendations of the European Commission on the civil law regulation of robotics, which is not a universally binding act, it is indicated that at this stage of technology development, AI should be recognized as the only object of social relations (Martsenko, 2022, p. 322). In terms of legally binding instruments, the European Union General Data Protection Regulation (GDPR) is perhaps the most obvious example. Like many initiatives targeting privacy and data protection, the GDPR is not specific to AI, but applies more generally to data processing activities. Aiming to protect Europeans from the privacy risks of data-intensive technologies, the GDPR includes punitive ex post regulation with the principle of data protection by design and Data Protection Impact Assessment plans. The EU has also developed the well-known Ethics Guidelines for Trustworthy AI, adopted by the High-Level Expert Group on Artificial Intelligence established by the European Commission. The Guidelines set out seven requirements for trustworthy AI, based on four ethical principles (Roumate, 2021, p. 6; Lane, 2022, p. 932). In April 2021, the European Commission published the draft "Artificial Intelligence Act" which sets out a proposed legal framework for AI. The proposed Act aimed to ban a small number of AI systems that pose unacceptably high risks to fundamental rights while mitigating the risks arising from other systems through a mixture of *ex ante* impact and conformity assessments and *ex post* penalties. The Artificial Intelligence Act was built on ethics-based initiatives such as the Ethics Guidelines for Trustworthy AI and the Resolution on a Framework of AI Ethics. The goal of this initiative is to prepare European countries for the tangible and intangible impact of artificial intelligence, ensured by a European ethical and legal framework. Within the Council of Europe, the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data is also noteworthy. The instrument is not an AI initiative *per se* but, similar to the GDPR, it would have an impact on some aspects of the development and deployment of AI (Roumate, 2021, p. 6; Lane, 2022, p. 932; Bakiner, 2023, p. 4). Lane claimed (2022, p. 935) that the Protocol takes the approach typical of the Council of Europe in placing positive obligations on State Parties which include the obligation to ensure the protection of individuals from violations by the private sector.

On 22 May 2019, the OECD adopted a recommendation on AI. The Recommendation consistent with value-based principles also provided five recommendations. Only 40 countries have adopted these principles including 36 OECD member countries, including the world's major economies, but excepting China and six non-member countries (Cataleta, 2021, p. 19; Roumate, 2021, p. 5). In 2019, the Council of Europe created an *ad hoc* Committee on AI (CAHAI), which is working on the feasibility and potential elements based on broad multi-stakeholder consultations, of a legal framework for the development, design, and application of artificial intelligence, based on the Council of Europe's standards on human rights**,** democracy and the rule of law (Roumate, 2021, p. 6).

Recently, the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law was adopted on 17 May 2024 by the Committee of Ministers of the Council of Europe at its 133th Session held in Strasbourg, and will be opened for signature at the Conference of Ministers of Justice in Vilnius on 5 September 2024 (Committee on Artificial Intelligence (CAI)). With the formal adoption by the Committee of Ministers, the Framework Convention is now definitely the first binding international treaty on AI and waiting to be signed and ratified by countries. In contrast to hopes and fears to the contrary, the negotiating parties have neither intended to create new substantive human rights nor to undermine the scope and content of the existing applicable protections. The intention of the parties negotiating the instrument has been to make sure that each party's existing protection levels of human rights, democracy and rule of law would also apply to current and future challenges raised by AI. In addition to the 46 Council of Europe member States, a number of countries from several regions (Argentina, Australia, Canada, Costa Rica, the Holy See, Israel, Japan, Mexico, Peru, Uruguay and the Unites States) participated in the negotiations, along with the European Union. In addition, the process was set up in an inclusive manner with many CoE bodies, other IGOs such as the OECD, OSCE, UNESCO and around 70 representatives from civil society, business and the technical and academic community actively participating and using the ability to make comments and text proposals to the draft treaty until the very last day of the negotiations (Committee on Artificial Intelligence (CAI)).

The Framework Convention formulates fundamental principles and rules which not only safeguard human rights, democracy and the rule of law but at the same time are conducive to progress and technological innovations. It is complementary to the already existing international human rights, democracy and rule of law standards and aims at filling-in any legal gaps that may have formed as a result of rapid technological advances in the sphere of human rights law but also with regard to the protection of democracy. Given the high level at which it is operating and in order to remain future-proof, the Framework Convention does not regulate technology and is essentially technology neutral. The Framework Convention and its implementation should follow the logic of a graduated and differentiated approach, in view of the severity and probability of adverse impacts on human rights, democracy and the rule of law (Committee on Artificial Intelligence (CAI)). It sets out a legal framework that covers AI systems throughout their lifecycles, from start to end, and will be a global instrument, open to the world. After its adoption, countries from all over the world will be eligible to join it and meet the high ethical standards it sets (Council of Europe, 2024).

In Asia, no instruments have been adopted by the Association of South East Asian Nations (ASEAN) but various national initiatives have been adopted within this region. The same can be said regarding the Inter-American human rights system (Lane, 2022, p. 936). In Africa, we can find the declaration by the African Union's Working Group on AI, adopted by African ministers responsible for communication and information and communication technologies (CICT) in Egypt on 26 October 2019 (African Union). This important legal framework confirms that international society is dedicated to the importance of ethics in AI, including the development of rules and strategic actions to face challenges imposed by AI and the importance of updating international law in the age of AI (Roumate, 2021, p. 7).

3. CONSTITUTIONAL – STATE LAW AND AI

As some authors (Pollicino & De Gregorio, 2021, p. 5) say, new technologies have always challenged, if not disrupted, the social, economic, legal, and, to a certain extent, ideological *status quo*. Such transformations impact constitutional values, as the state formulates its legal response to new technologies based on constitutional principles which meet market dynamics, and as it considers its own use of technologies in light of the limitation imposed by constitutional safeguards. Constitutions have been designed to limit public, more precisely governmental powers, and protect individuals against any abuse from the state. The shift of power from public to private hands requires rethinking and, in case, revisiting some well-established assumptions. In recent years, however, the rise of the algorithmic society has led to a paradigmatic change where public power is no longer the only source of concern for the respect of fundamental rights and the protection of democracy. This requires either the redrawing of the constitutional boundaries so as to subject digital platforms to constitutional law or to revisit the relationship between constitutional law and private law, including the duties of the state to regulate the cybernetic complex, within or outside the jurisdictional boundaries of the state. Within this framework, the rise of digital private powers challenges the traditional characteristics of constitutional law, thus encouraging to wonder how the latter might evolve to face the challenges brought by the emergence of new forms of powers in the algorithmic society (Pollicino & De Gregorio, 2021, p. 6).

We need to be aware of one more fact, which is of the utmost importance. Namely, constitutional law, i.e. *materia constitutionis*, has one characteristic, which is conservatism. In other words, constitutional law will react only in the case that the basic values of a legal order cannot be ensured or protected, by norms which are below the constitution. We have to keep in mind that AI is something new, when we speak about the law. So, it is fully expected that the constitutional norms do not yet fully recognise it. However, at the same time, this does not mean that human rights are not protected when it comes to artificial intelligence. On the contrary, constitutional law ensures the protection of human rights through the general regime of human rights protection within democratic systems. Bearing that in mind, in that interim period, it should be emphasized that an extremely important and active role can be expected from the courts, especially the constitutional courts, which should set clear boundaries.

In the meantime, a number of countries have now adopted national strategies concerning AI, and some of these have adopted legislation. However, some instruments include more general references to the protection of human rights, such as in Australia, New Zealand and Germany which also contain standards that can have an impact on the protection of human rights without being framed as such. Other states, such as the United States, China and the United Kingdom are also working on regulatory frameworks, though without having produced coherent legal frameworks so far. Private institutions have contributed to the gradual formation of more de-centralized regulatory schemes, although they cannot be substitutes for fully elaborated, legal schemes (Tzimas, 2020, p. 549; Lane, 2022, p. 940). Other legislative initiatives have been taken at

the subnational level, such as legislation adopted in Washington State in the US regarding governmental use of facial recognition and a bill concerning discrimination and the use of automated decision-making. Overall, many countries are making strides in the introduction of legislation or regulation concerning AI, including through the adoption of national AI strategies, and non-binding national measures sometimes reference the broad range of human rights found at the international level. This is positive, but beyond data protection and privacy, the protection of human rights has not yet been thoroughly embedded in national legislation related to AI. Nonetheless, there are some positive contributions that enhance legal certainty for both States and businesses in the national initiatives (Tzimas, 2020, p. 549; Lane, 2022, p. 940). In Serbia, the importance of artificial intelligence is recognized at the state level. In this sense, significant steps are being taken in order to keep pace with world and European trends. The Working Group for Drafting the Artificial Intelligence Law of the Republic of Serbia was formed. The formation of the Working Group marks the beginning of a significant process in drafting the Artificial Intelligence Law. The Working Group comprises representatives from various government bodies, the scientific and professional community, law firms, and business entities involved in the field of artificial intelligence. The participation of a large number of experts from diverse fields aims to ensure a comprehensive view of all aspects of AI regulation (National AI Platform, 2024).

4. CONCLUSION

It is more than evident that fundamental rights and democratic values seem to be under pressure in the information society (Pollicino & De Gregorio, 2021, p. 10). The ongoing development of AI technologies presents international law with a number of challenges (Lane, 2022, p. 940). On one hand, when we talk about the legal steps, especially the constitutional ones, one must consider that enactment takes many years. This is alarming considering the fact that over the course of a decade two entire technological generations can pass. As the matter of fact, the pace of regulatory change is too slow to keep up with that of technology. It is evident that regulatory systems are always outdated in respect of technological progress (Cataleta, 2021, p. 9). Future discussion, therefore, should take up this issue and provide clarity to it as soon as possible. Overall, transformation of law should not be delayed any further. AI technologies and machines are progressing by leaps and bounds while the legal norms applicable to them are either stuck in the analogue age or are moving forward at snail's pace. It should be changed before it is too late (Lee, 2022, p. 261).

On the other hand, technology is also an opportunity, since it can provide better systems of enforcement of legal rules but also a clear and reliable framework compensating the fallacies of certain processes. Indeed, new technologies like automation should not be considered as a risk *per se*. At the same time, it is well-known that hard law can represent a hurdle to innovation, leading to other drawbacks for the development of the internal market, precisely considering the global development of algorithmic technologies (Pollicino & De Gregorio, 2021, p. 12). Technologies may contribute

to the advancement of human rights. For instance, the use of machine learning (ML) in healthcare could improve precision medicine and eventually provide better care to patients. On the other hand, they can pose an obvious risk to human rights. In other words, AI presents both benefits and risks (Quintavalla & Temperman, 2023b, p. 4). As Quintavalla and Temperman stated (2023a, p. 570), it is very difficult to account for all the consequences that the development and deployment of a given AI application can have on human rights protection.

Therefore, a fully harmonised approach would constitute a sound solution to provide a common framework and avoid fragmentation, which could undermine the aim of ensuring the same level of protection of fundamental rights. Besides, coregulation in specific domains could ensure that public actors are involved in determining the values and principles underpinning the development of algorithmic technologies while leaving the private sector room to implement these technologies under the guidance of constitutional principles. The principle of the rule of law constitutes a clear guide for public actors which intend to implement technologies for public tasks and services. To avoid any effect on the trust and accountability of the public sector, consistency between the implementation of technology and the law is critical for legal certainty. Nonetheless, it is worth stressing that this is not an easy task (Pollicino & De Gregorio, 2021, p. 13).

Most notably, it is necessary to design a frame that describes the relationship between the three parties: platforms, states, and individuals. In other words, a *digital habeas corpus* of substantive and procedural rights should be identified, which can be enforced by the courts as they are inferred from existing rights protected under current digital constitutionalism (Pollicino & De Gregorio, 2021, p. 20). This is why it is critical to understand the role of regulation in the field of artificial intelligence, where cooperative efforts between the public and private sector could lead to a balanced approach to risk and innovation (Pollicino & De Gregorio, 2021, p. 24). Given their importance for institutionalizing justice and expressing as well as preserving the human focus of the rule of law, human rights can set the ultimate checks and balances regarding AI development. More specifically, the suggestion is that human rights can and must contribute to a regulatory framework promoting "friendly" AI and prohibiting undesirable as well as enabling desirable AI developments and applications (Tzimas, 2020, p. 549).

LIST OF REFERENCES

Al-Taj, H., Polok, B. & Rana, A. A. 2023. Balancing Potential and Peril: The Ethical Implications of Artificial Intelligence on Human Rights. *Multicultural education*, (6), pp. 94-99.

Council of Europe. 2024. Artificial Intelligence, Human Rights, Democracy and the Rule of Law Framework Convention. Available at: https://www.coe.int/en/web/artificial-intelligence/-/artificial-intelligence-human-rights-democracy-and-the-rule-of-law-framework-convention (11. 7. 2024).

Bakiner, O. 2023. The promises and challenges of addressing artificial intelligence with human rights. *Big Data & Society*, 10(2), pp. 1-10. https://doi.org/10.1177/20539517231205476

Cataleta, M. S. 2021. Humane Artificial Intelligence The Fragility of Human Rights Facing AI. *East West Center*, Working paper 2, pp. 1-31.

Council of Europe. Committee on Artificial Intelligence (CAI), Available at: https://www.coe.int/en/web/artificial-intelligence/cai (11. 7. 2024).

National AI Platform. 2024. First Meeting of the Working Group for Drafting the Artificial Intelligence Law of the Republic of Serbia Held. Available at: https://www.ai.gov.rs/vest/en/948/first-meeting-of-the-working-group-for-drafting-the-artificial-intelligence-law-of-the-republic-of-serbia-held.php (12. 7. 2024).

Kriebitz, A. & Lütge, C. 2020. Artificial intelligence and human rights: A business ethical assessment. *Business and Human Rights Journal*, *5*(1), pp. 84-104. https://doi.org/10.1017/bhj.2019.28

Lane, L. 2022. Clarifying Human Rights Standards through Artificial Intelligence Initiatives. *International and Comparative Law Quarterly*, (71), pp. 915-944. https://doi.org/10.1017/S0020589322000380

Lee, J. 2022. *Artificial Intelligence and International Law*. Singapore: Springer. https://doi.org/10.1007/978-981-19-1496-6

Martsenko, N. 2022. Artificial intelligence and human rights: a scientific review of impacts and interactions. *Studia Prawnoustrojowe*, (58), pp. 315-329. https://doi.org/10.31648/sp.8245

Muller, C. 2020. *The Impact of Artificial Intelligence on Human Rights, Democracy and the Rule of Law.* Available at: https://allai.nl/wp-content/uploads/2020/06/The-Impact-of-AI-on-Human-Rights-Democracy-and-the-Rule-of-Law-draft.pdf (6. 7. 2024).

Nicolau, I. I. 2019. Human Rights and Artificial Intelligence. *Journal of Law and Administrative Sciences*, (12), pp. 64-70.

Pollicino, O. & De Gregorio, G. 2021. Constitutional law in the algorithmic society. In: Micklitz, H.-W. *et al.* (eds.), *Constitutional Challenges in the Algorithmic Society.* Cambridge: Cambridge University Press, pp. 3-24. https://doi.org/10.1017/9781108914857.002

Quintavalla, A. & Temperman, J. 2023a. Conclusion. In: Quintavalla, A. & Temperman, J. (eds.), *Artificial Intelligence and Human Rights*. Oxford: Oxford University Press, pp. 569-570. https://doi.org/10.1093/law/9780192882486.003.0037

Quintavalla A. & Temperman J. 2023b. Introduction. In: Quintavalla, A. & Temperman, J. (eds.), *Artificial Intelligence and Human Rights*. Oxford: Oxford University Press, pp. 3-15. https://doi.org/10.1093/law/9780192882486.003.0001

Reddy, B. 2022. Warning the UK on Special Purpose Acquisition Companies (SPACs): Great for Wall Street but a Nightmare on Main Street, *Journal of Corporate Law Studies,* 22, pp. 1-44.

Roumate, F. 2021. Artificial intelligence, ethics and international human rights law. *The International Review of Information Ethics*, 29, pp. 1-7. https://doi.org/10.29173/irie422

Tzimas, T. 2020. Artificial intelligence and human rights: their role in the evolution of AI. *Heidelberg Journal of International Law — ZaöRV*, (80), pp. 533-557.

UDC: 004.8:34 DOI: 10.56461/iup_rlrc.2024.5.ch14

Bogdana STJEPANOVIĆ*
Institute of Comparative Law, Belgrade, Serbia

LEVERAGING ARTIFICIAL INTELLIGENCE IN eDISCOVERY: ENHANCING EFFICIENCY, ACCURACY, AND ETHICAL CONSIDERATIONS**

Developments in digital technologies over the past few decades have profoundly affected every area of law, from the practice of individual lawyers to court procedures. Today, systems can draft documents, conduct legal research, disclose documents in litigation, conduct due diligence, provide legal guidance, and even resolve litigation online. The traditionally conservative legal profession is now compelled to embrace these changes to stay relevant in the changing world.

Discovery is a crucial part of court procedure in common law jurisdictions. It allows each party to obtain the information needed to prepare for trial, evaluate the strengths and weaknesses of their case, and develop strategies for success. As more information is stored electronically, the need for an electronic form of this litigation phase emerged. Since 2006, electronic discovery (eDiscovery) has been officially recognized.

Electronic discovery, or eDiscovery, refers to the process of identifying, collecting, and producing electronically stored information (ESI) in response to a request for production in a lawsuit or investigation. ESI encompasses a wide range of digital data, including emails, online documents, spreadsheets, databases, digital images, presentations, audio and video files, social media posts, and websites.

The primary purpose of eDiscovery is to support litigation, but the processes of identifying, preserving, collecting, and analyzing ESI are applicable to any organization facing legal or regulatory compliance requirements. Companies in EMEA and APAC regions, even without formal eDiscovery rules, use the technology in anticipation of litigation or regulatory action, to redact sensitive information, conduct internal investigations, perform fact-finding audits, and manage company data.

* PhD, Research Associate, ORCID: 0000-0002-9504-473X, e-mail: *b.stjepanovic@iup.rs*

** This paper is a result of the research conducted at the Institute of Comparative Law financed by the Ministry of Science, Technological Development and Innovation of the Republic of Serbia under the Contract on realisation and financing scientific research of SRO in 2024 registered under no. 451-03-66/2024-03/200049.

In this article we are going to analyze the eDiscovery process in general, including its phases, advantages, and disadvantages. It will also examine the impact of Artificial Intelligence (AI) on eDiscovery. Given that both AI and eDiscovery are highly complex and rapidly evolving fields, the aim of this article is to provide a preliminary overview of AI's use in eDiscovery and to explore potential future developments.

Keywords: artificial intelligence (AI), eDiscovery, Legaltech, data privacy, digital technologies.

1. INTRODUCTION

A traditionally conservative legal profession is undergoing tremendous changes with the introduction of new technologies. The pace at which technology has been displacing outdated processes has varied over the years, but the real acceleration of the digital transformation in the legal profession happened with the COVID-19 pandemic in 2020. From then on, new technologies have been rapidly transforming our world, requiring the legal sector to reinvent itself to keep up.

The transformation of the legal industry has led to the emergence of new concepts, one of which is Legaltech. The term "Legaltech" refers to the application of new technologies to the legal field to carry out tasks that, until recently, were performed by lawyers or other personnel working in law firms. Legaltech encompasses various tools and systems that can draft documents, conduct legal research, disclose documents in litigation, conduct due diligence, provide legal guidance, and even resolve litigation online.[1]

Today, digital technologies have been successfully applied to many areas of law, including due diligence, contract review, legal research, e-discovery, prediction technology, and document automation. Additionally, tools such as client portals and intranet-based collaborative platforms are becoming more sophisticated every day.[2]

One of the most recent technologies revolutionizing our world is artificial intelligence (AI). AI is rapidly and profoundly transforming almost all aspects of the existing

[1] Salmerón-Manzano, E. 2021. Legaltech and Lawtech: Global Perspectives, Challenges and Opportunities. In: Salmeron-Manzano, E. (ed.), *Laws and Emerging Technologies*, p. 62.

When it comes to the future of Legal Tech there are some predictions: paperless legal practice; more remote work; more AI; court appearances by video; online filing of pleadings and payments of fees as well as full access to docket sheets and PDFs of filed documents; less reliance on lawyers, etc. Matich, T. 2021. 10 Predictions for the Next 10 Years of Legal Tech. Clio. Available at: https://www.clio.com/blog/10-predictions-10-years/ (2. 6. 2024).

Legal tech, as Colin points out, extends beyond sophisticated AI and robotics; it includes simpler, yet impactful tools like billing software. The ultimate goal is to make legal work more efficient, productive, and less burdensome for professionals. This clarification is crucial in distinguishing between legal tech and legal innovation. While legal tech encompasses the tools and software developed to address specific legal tasks, legal innovation involves a broader approach, encompassing new ways of thinking, business models, and methodologies that fundamentally change how legal services are conceived and delivered. Percipient. n. d. Bridging the Gap: Legal Tech vs Legal Innovation. Available at: https://percipient.co/bridging-the-gap-legal-tech-vs-legal-innovation/ (2. 6. 2024).

[2] Caserta, S. & Rask Madsen, M. 2019. The Legal Profession in the Era of Digital Capitalism: Disruption or New Dawn? *Laws*, 8(1), pp. 1-17.

world, including the legal sector. Generative AI, for example, is transforming legal practice by assisting with tasks such as contract review, document retrieval, case management, legal research, and contract drafting. There are even predictions that AI might eventually overtake the legal profession and replace legal professionals in certain roles.[3]

An integral part of Legaltech and legal innovation is eDiscovery. Electronic discovery (e-discovery, ediscovery, eDiscovery, or e-Discovery) refers to the electronic aspect of identifying, collecting, and producing electronically stored information (ESI) in response to a request for production in a lawsuit or investigation.[4] With the growing volume of electronic data and rapidly evolving technologies—such as Chat GPT-4[5], which can almost perfectly mimic human voice and many other capabilities—new challenges have emerged for eDiscovery, particularly concerning the accuracy of the obtained information.

AI has emerged as a crucial tool in addressing some of these challenges and solving both old and new problems in eDiscovery. AI is already widely used in the eDiscovery process for document categorization (e.g., technology-assisted review or predictive coding), identification of personally identifiable information (PII), investigations, and some forms of early case assessment.[6] When used correctly by experienced individuals with a critical approach to the results, AI can offer significant cost and time savings compared to previous unautomated methods. The ability of AI and machine learning (ML) technologies to extract meaningful insights from vast datasets has led to significant transformations in eDiscovery.[7]

In this article we are going to analyze the eDiscovery process in general (its phases, pros and cons, etc.) and explore the impact that the introduction of AI has had on it. Given that both AI and eDiscovery are complex and rapidly evolving fields, our aim is to provide a preliminary overview of the use of AI in eDiscovery and to suggest potential future developments.

2. THE EDISCOVERY PROCESS: AN OVERVIEW

In common law jurisdictions, discovery is a fundamental phase of civil litigation. It allows both parties to obtain evidence and information relevant to their case, which is crucial for preparing for trial. Discovery enables parties to evaluate the strengths and weaknesses of their case and develop effective trial strategies.

With the exponential increase in data volumes, the concept of the global "datasphere" has emerged, reflecting the vast amount of digital data generated worldwide. This includes newly created, captured, and duplicated data. Experts predict that global data creation will

---

[3] Caserta & Rask Madsen, p. 1.

[4] CDS. n. d. The Basics: What is e-Discovery? Available at: https://cdslegal.com/knowledge/the-basics-what-is-e-discovery/ (15. 6. 2024).

[5] ChatGPT is not a standalone technology per se, but rather a specific application of broader artificial intelligence (AI) and natural language processing (NLP) technologies.

[6] EDRM. 2020. The use of artificial intelligence in eDiscovery. Available at: https://edrm.net/wp-content/uploads/dlm_uploads/2021/02/20210203-EDRM-AI-Paper-v-14.pdf (17. 6. 2024).

[7] EDRM. 2020. The use of artificial intelligence in eDiscovery. Available at: https://edrm.net/wp-content/uploads/dlm_uploads/2021/02/20210203-EDRM-AI-Paper-v-14.pdf (17. 6. 2024).

exceed 180 zettabytes by 2025.[8] This explosion in data necessitates advanced tools for managing and processing information, particularly in the context of eDiscovery.[9]

EDiscovery, officially became a part of court procedures with the 2006 amendments to the Federal Rules of Civil Procedure. These amendments recognized the growing relevance of electronic documents and ESI in litigation, altering how parties, their lawyers, and courts handle the discovery of such information.[10] This shift impacted how companies manage, preserve, and produce ESI.[11]

[8] Logikcull. eDiscovery Disrupted: The Potential Effects of AI. Available at: https://www.logikcull.com/blog/ediscovery-disrupted-the-potential-effects-of-ai (3. 6. 2024). A zettabyte is one sextillion or 1,000,000,000,000,000,000,000 bytes.

[9] Growing importance of eDiscovery shows its value as well. In 2023 the global eDiscovery market was valued at USD 15.45 billion and is projected to be worth USD 16.98 billion in 2024 and reach USD 39.91 billion by 2032, exhibiting a CAGR of 11.3%. North America dominated the global market with a share of 39.16% in 2023. See: Fortune Business Insights. 2024. eDiscovery Market Size, Share & Industry Analysis, By Component (Solutions and Services) By Deployment Model (Cloud and On-premises), By Enterprise Type (Large Enterprises and SMEs), By End-user (BFSI, Retail & Consumer Goods, Government & Public Sector, Healthcare & Life Sciences, IT & Telecommunications, Legal, and Others), and Regional Forecast, 2024-2032. Available at: https://www.fortunebusinessinsights.com/industry-reports/ediscovery-market-101503 (15. 6. 2024).

The market is split into cloud and on-premises. In 2023, the cloud segment accounted for a larger market share and is projected to grow with a high CAGR during the forecast period. The cloud environment growth is attributed to an increase in remote work due to the pandemic and centralized structure, which is accelerating the demand for cloud. Cloud electronic discovery solutions offer better convenience and collaboration as they can be accessed from anywhere, and allow organizations to share and process files in real-time which leads to reducing the cost of data storage and ease of use in AI and automation technologies, thus increasing demand for cloud-based solutions. *Ibid*.

[10] Before 2006, ESI were used and analyzed but there were no strict procedures that had to be followed. Advantages of EDiscovery compared to discovery process:

- EDiscovery significantly enhances the efficiency and speed of the discovery process. Traditional manual document review is labour-intensive and time-consuming. By utilizing automated data processing and review technologies, eDiscovery tools allow legal teams to manage vast amounts of data more swiftly. This efficiency is essential in the face of rapidly growing data volumes in the digital era. Logikcull. eDiscovery Disrupted: The Potential Effects of AI. Available at: https://www.logikcull.com/blog/ediscovery-disrupted-the-potential-effects-of-ai (3. 6. 2024). - EDiscovery can lead to substantial cost savings. Automating data collection, processing, and review reduces labor costs associated with manual document review. Technologies such as predictive coding and technology-assisted review (TAR) streamline these processes, thereby lowering litigation expenses. Additionally, AI and machine learning further enhance cost-efficiency by minimizing the need for manual intervention. Industry trends. Available at: https://cloudnine.com/tag/industry-trends/ (5. 6. 2024).
- Advanced eDiscovery tools improve the precision of data retrieval and analysis. Predictive coding, for instance, uses algorithms to identify relevant documents, thus enhancing the accuracy of the review process. These technological advancements help reduce human error and ensure that critical evidence is not overlooked. Create Progress. 2024. The Role of AI in E-Discovery: Enhancing Litigation with Efficient and Cost-Effective Solutions. Available at: https://createprogress.ai/the-role-of-ai-in-e-discovery-enhancing-litigation-with-efficient-and-cost-effective-solutions/ (8. 6. 2024).
- Finally, eDiscovery improves electronic data management through frameworks like the Electronic Discovery Reference Model (EDRM). The EDRM provides a structured approach to handling electronically stored information (ESI), aiding in data organization and maintaining integrity throughout the legal process. KLDiscovery. What is eDiscovery? Available at: https://www.kldiscovery.com/uk/resources/what-is-ediscovery (8. 6. 2024).

[11] DeBono, J. 2008. Preventing and Reducing Costs and Burdens Associated with E-discovery: The 2006 Amendments to the Federal Rules of Civil Procedure. *Mercer Law Review*, 59(3), pp. 963-990. Available at:

ESI is dynamic and often contains metadata[12] such as time-date stamps and author information. This complexity, along with the volume of data, necessitates the use of advanced technology to handle eDiscovery effectively. Key to eDiscovery is the preservation of original content and metadata to avoid claims of spoliation or tampering with evidence.[13]

The eDiscovery process is typically guided by the Electronic Discovery Reference Model (EDRM). The EDRM outlines a structured approach to handling ESI, from identification and preservation to processing, review, and presentation. The first stage of EDRM is **Information Governance**. This stage involves setting up policies and procedures for managing electronic data throughout its lifecycle. It ensures data is handled consistently and in compliance with regulations, thereby reducing legal risks and improving data management. The second stage is **Identification** of ESI. In this stage, the locations of relevant electronic data are determined and accessed. This helps businesses quickly locate and retrieve data, saving time and resources in the eDiscovery process. After ESI is identified, the **Preservation** stage starts**.** This step involves safeguarding relevant electronic data to maintain its integrity and authenticity, preventing data loss or tampering. This ensures that the information remains reliable for audits or legal proceedings. Next step is **Collection** of ESI. Relevant electronic data is gathered in a way that supports legal requirements while minimizing disruptions to business operations, allowing companies to maintain productivity during the eDiscovery process. Fifth stage is **Processing**. In this stage collected electronic data is converted into a format suitable for review and analysis. This step facilitates the extraction of valuable insights while ensuring compliance with legal and regulatory standards. Sixth stage is a **Review** stage. The collected data is evaluated to determine its relevance and privilege status. This enables organizations to focus on pertinent information and streamline the eDiscovery process. One of the key stages of EDRM is **Analysis.** It involves examining the data to identify key information and insights, helping companies make informed, data-driven decisions. After it is done, relevant data is generated in a format that meets legal and regulatory requirements, ensuring that the information is presented accurately and in a legally acceptable manner. This stage is named **Production**.

---

https://digitalcommons.law.mercer.edu/jour_mlr/vol59/iss3/6 (9. 8. 2024).

First, electronically stored information is now included in permissible discovery. Second, parties are required to "meet and confer" about the discovery of electronically stored information at the onset of litigation. Third, issues pertaining to claims of privilege and waiver of privilege for electronically stored information are addressed. Fourth, matters relating to the production and form of production of electronically stored information are discussed. Fifth, limitations are imposed on the discovery of electronically stored information where a substantial burden or cost is imposed on the producing party. Sixth, a safe harbor provision is created to prevent sanctions from being imposed when electronically stored information is inadvertently destroyed or "lost as a result of the routine, good-faith operation of an electronic information system". DeBono, J. 2008. Preventing and Reducing Costs and Burdens Associated with E-discovery: The 2006 Amendments to the Federal Rules of Civil Procedure. *Mercer Law Review,* 59(3), pp. 963-990. Available at: https://digitalcommons.law.mercer.edu/jour_mlr/vol59/iss3/6 (9. 8. 2024).

[12] Metadata, or data about data can be used to organize information to make it easier to review large volumes of ESI. Besides that, metadata may be necessary to confirm the authenticity of information. Matich, T. 2024. What Lawyers Need to Know About eDiscovery. Clio. Available at: https://www.clio.com/blog/need-to-know-ediscovery/ (2. 6. 2024).

[13] CDS. n. d. The Basics: What is e-Discovery? Available at: https://cdslegal.com/knowledge/the-basics-what-is-e-discovery/ (15. 6. 2024).

And the last stage of EDRM is **Presentation**. This final stage involves delivering the relevant data in a clear and organized manner, making it easy for stakeholders to understand and use the information for decision-making purposes.[14]

2.1. Advantages of eDiscovery

E-discovery offers numerous advantages that enhance the legal process by making the collection, analysis, and management of evidence more efficient, accurate, and accessible. Here are some of the key advantages:

1. Improved Evidence Authentication: E-discovery tools allow for the verification of electronic evidence through metadata, which includes timestamps, author details, and modification histories. This ensures the authenticity and reliability of digital documents, reducing the chances of tampering or forgery.[15]
2. Faster Processing: The automation capabilities of e-discovery tools enable quicker collection and analysis of large volumes of electronically stored information (ESI). This speeds up legal proceedings by reducing the time spent on manually handling physical documents and evidence.[16]
3. Enhanced Data Recovery: Even if electronic data has been deleted or altered, e-discovery tools can often retrieve or reconstruct it. This is especially valuable in cases where crucial information might otherwise be lost or destroyed, ensuring that all relevant evidence is accessible.
4. Comprehensive Record of Changes: E-discovery systems keep meticulous records of any modifications or deletions made to electronic documents. This ensures transparency and accountability, as all changes are documented and visible to the parties involved in the case.
5. Broader Access to Evidence: E-discovery allows for the examination of various types of digital evidence, such as emails, text messages, social media posts, and website data. This wider range of evidence sources provides a more comprehensive understanding of the case and can reveal critical insights that might not be available through traditional evidence gathering methods.
6. Increased Efficiency and Cost-Effectiveness: By streamlining the discovery process, e-discovery reduces the time and labor required to manage evidence. This leads to more efficient case management and can lower the overall costs of litigation.
7. Facilitates Collaboration: E-discovery tools support better collaboration between legal teams, investigators, and law enforcement by allowing data to be shared remotely and analyzed in real-time. This is particularly beneficial in complex cases involving multiple jurisdictions or international teams.

---

[14] Veritas. EDRM: What It Is, Why It Matters, and How to Use It? Available at: https://www.veritas.com/information-center/edrm (15. 6. 2020).

[15] Klaff, T. 2007. Authenticating E-Discovery As Evidence. *CCB Journal*. Available at: https://ccbjournal.com/articles/authenticating-e-discovery-evidence (15. 6. 2024).

[16] Infosys BPM. E-Discovery automation: Challenges and opportunities. Available at: https://www.infosysbpm.com/blogs/legal-process-outsourcing/e-discovery-automation-challenges-and-opportunities.html (15. 6. 2024.)

These advantages make e-discovery a vital tool in modern legal practice, improving both the speed and accuracy of evidence collection and management.[17]

2.2. Challenges in eDiscovery

Despite its unbeatable benefits for legal field, as a multifaceted process eDiscovery has several challenges that legal professionals must navigate. Here are some key challenges:

1. Data Volume: A primary challenge in eDiscovery is the management of vast data volumes. Modern organizations generate extensive quantities of electronic data. This data is dispersed across various devices, servers, and cloud platforms, complicating the task of locating and identifying pertinent information. The sheer volume of data can necessitate substantial time and resources to process, particularly in the context of large-scale litigation or regulatory scrutiny.[18]
2. Data Security: Handling sensitive and confidential information requires robust security measures to prevent data breaches and unauthorized access. Legal teams must ensure compliance with data protection regulations and implement stringent security protocols.[19]
3. Cost Management: While technology can reduce some costs, eDiscovery can still be expensive, particularly in complex cases with vast amounts of data. Effective budgeting and cost management strategies are essential to control expenses.[20]
4. Technical Expertise: The complexity of eDiscovery tools and processes necessitates a certain level of technical expertise. Legal professionals must stay informed about the latest advancements and receive adequate training to effectively leverage these technologies.
5. Ethical Considerations: The use of AI and automation in eDiscovery raises ethical questions about bias, transparency, and accountability. Ensuring that AI tools are used responsibly and that their decision-making processes are transparent is crucial to maintaining fairness and integrity in the legal process.[21]
6. Risk of over-relying on technology: While AI and machine learning can enhance accuracy and efficiency, they are not infallible. Over-reliance on these technologies without proper oversight can lead to issues such as incomplete or incorrect data analysis.[22]

---

[17] See more: Scheindlin, S. & Conference, S. 2015. *Electronic Discovery and Digital Evidence in a Nutshell*. St. Paul: West Academic Publishing.

[18] Sakthivel, R. 2023. Complexities of eDiscovery. LinkedIn. Available at: https://www.linkedin.com/pulse/complexities-ediscovery-ravi-sakthivel/ (9. 8. 2024).

[19] Schwartz, P. M. & Solove, D. J. 2011. The PII Problem: Privacy and a New Concept of Personally Identifiable Information. *New York University Law Review*, 86, p. 1814.

[20] The document review process is particularly costly, often accounting for over 80% of total litigation expenses, equivalent to approximately $42 billion annually. Cloud nine. 2022. Managing the Unpredictability of eDiscovery Costs. Available at: https://cloudnine.com/ediscoverydaily/managing-unpredictability-of-ediscovery-costs-with-cloudnine/ (14. 7. 2024). See more: EDRM. 2022. How to Evaluate and Control Ediscovery Costs. Available at: https://edrm.net/2022/04/how-to-evaluate-and-control-ediscovery-costs/ (17. 6. 2024).

[21] Mittelstadt, B. D. *et al*. 2016. The Ethics of Algorithms: Mapping the Debate. *Big Data & Society*, 3(2), p. 2.

[22] Troy, T. 2023. Examining the Impacts, Both Positive and Negative, of Artificial Intelligence on Businesses. Medium. Available at: https://medium.com/@timothytroy/examining-the-impacts-both-positive-

3. AI AND EDISCOVERY

Artificial intelligence (AI) refers to a branch of computer science concerned with creating intelligent agents, which are systems that can reason, learn, and act autonomously. AI encompasses a broad range of techniques, from narrow AI, which excels at specific tasks, to the theoretical concept of general AI, which would possess human-level intelligence across all domains.[23]

Currently, there is no universally accepted definition of AI.[24] For the purpose of this paper, we define AI as an automated process used to classify, categorize, summarize, make predictions, or provide information regarding data or information using statistical, rule-based, or other algorithmic means.[25]

---

and-negative-of-artificial-intelligence-on-businesses-ac17758d787e (22. 6. 2024).

[23] Rouse, M. 2024. What Is Artificial Intelligence (AI)? Available at: https://www.techopedia.com/definition/190/artificial-intelligence-ai (7. 4. 2024); Paloalto Networks. What Is Artificial Intelligence (AI)? Available at: https://www.paloaltonetworks.com/cyberpedia/artificial-intelligence-ai (7. 4. 2024).

[24] In Art. 3 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance), OJ L, 2024/1689: "AI system" means a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments". The concept of AI was created by computer scientist Alan Turing in 1950 when he speculated that "thinking machines" could reason at the level of human beings. In order to prove that Turing proposed an "imitation game," (further known as a "Turing test") as a means of deciding whether a computer was intelligent. For a machine to pass the Turing test, it must be able to talk to somebody and fool them into thinking it is human. The term "artificial intelligence" was introduced by John McCarthy in a proposal for a 1956 workshop on building machines to emulate human intellectual capacity. This workshop was intended to investigate "the conjecture that every aspect of learning or any other feature of intelligence can in principle be so precisely described that a machine can be made to simulate it. An attempt will be made to find how to make machines use language, form abstractions and concepts, solve the kinds of problems now reserved for humans, and improve themselves." McCarthy, J. *et al.* 1955. A proposal for the Dartmouth Summer Research Project on Artificial Intelligence. JMC Stanford. Available at: http://jmc.stanford.edu/articles/dartmouth/dartmouth.pdf (9. 8. 2024). A proposal for the Dartmouth Summer Research Project on Artificial Intelligence (http://jmc.stanford.edu/articles/dartmouth/dartmouth.pdf).

Seven decades after introducing the Turing test, we have been presented with information that ChatGPT 4 has passed it. Scientists decided to replicate this test by asking 500 people to speak with four respondents, including a human and the 1960s-era AI program ELIZA as well as both GPT-3.5 and GPT-4, the AI that powers ChatGPT. The conversations lasted five minutes—after which participants had to say whether they believed they were talking to a human or an AI. In the study, published May 9 to the preprint arXiv server, the scientists found that participants judged GPT-4 to be human 54% of the time, ELIZA, a system pre-programmed with responses but with no large language model (LLM) or neural network architecture, was judged to be human just 22% of the time. GPT-3.5 scored 50% while the human participant scored 67%. GPT-4 has passed the Turing test, researchers claim. Turney, D. 2024. GPT-4 has passed the Turing test, researchers claim. Live Science. Available at: https://www.livescience.com/technology/artificial-intelligence/gpt-4-has-passed-the-turing-test-researchers-claim (9. 8. 2024). The fact that there could be mimic human voice and conversation leads to many problems when conducting eDiscovery as well.

[25] EDRM. 2020. The use of artificial intelligence in eDiscovery. Available at: https://edrm.net/wp-content/uploads/dlm_uploads/2021/02/20210203-EDRM-AI-Paper-v-14.pdf (17. 6. 2024).

AI is rapidly transforming various industries, and eDiscovery is no exception. AI-powered tools are being increasingly used to streamline the eDiscovery process, improve accuracy, and reduce costs.

3.1. AI Techniques in eDiscovery

AI encompasses a range of techniques that have found applications in eDiscovery.

Clustering is an unsupervised ML technique employed in eDiscovery to group similar documents based on shared characteristics or topics. This process enables users to identify patterns within the dataset and take actions on clusters of related documents. While clustering does not require pre-labeled data, the selection of features for similarity measurement and the determination of the optimal number of clusters remain crucial decisions for the analyst.[26]

Email Threading is a process that identifies and groups related emails within a conversation, streamlining the review process. By organizing emails into threads, eDiscovery practitioners can efficiently analyze email communications and reduce redundancy in review efforts.[27]

Concept Search is an NL processing technique that allows users to search for documents based on semantic meaning rather than exact keywords. By understanding the context of words and their relationships, concept search can enhance the precision and recall of search results. This approach can be particularly useful in overcoming the challenges posed by synonyms, polysemy, and complex query formulations.[28]

Technology-Assisted Review (TAR) or predictive coding, is a supervised machine learning technique that trains a computer system to distinguish between relevant and irrelevant documents. By leveraging human-in-the-loop feedback, TAR algorithms continuously improve their accuracy over time. This technology has become a cornerstone of modern eDiscovery practices, enabling efficient and cost-effective document review.[29]

Entity Recognition is an NLP technique that identifies and classifies named entities within text, such as person names, organizations, locations, dates, and numerical values. In eDiscovery, entity recognition can be used to extract relevant information, protect sensitive data, and facilitate advanced analytics.[30]

Sentiment Analysis is an NLP technique that determines the emotional tone of text, categorizing it as positive, negative, or neutral. In eDiscovery, sentiment analysis can be

---

[26] Cloud nine. Document Clustering for eDiscovery Review. Available at: https://cloudnine.com/legacy/document-clustering/ (14. 7. 2024).

[27] EDRM. 2020. The use of artificial intelligence in eDiscovery. Available at: https://edrm.net/wp-content/uploads/dlm_uploads/2021/02/20210203-EDRM-AI-Paper-v-14.pdf (17. 6. 2024).

[28] EDRM. 2020. The use of artificial intelligence in eDiscovery. Available at: https://edrm.net/wp-content/uploads/dlm_uploads/2021/02/20210203-EDRM-AI-Paper-v-14.pdf (17. 6. 2024).

[29] EDRM. Technology Assisted Review. Available at: https://edrm.net/resources/frameworks-and-standards/technology-assisted-review/ (15. 6. 2024).

[30] Deloitte. 2018. Entity recognition: How electronic discovery can benefit. Available at: https://www2.deloitte.com/us/en/pages/advisory/articles/entity-recognition-how-electronic-discovery-can-benefit.html (15. 7. 2024).

applied to emails, social media posts, and other unstructured data to identify potential evidence or assess the overall sentiment surrounding a case.[31]

Machine Translation is the process of automatically translating text from one language to another. While not a perfect substitute for human translation, machine translation can be used as a preliminary step in the eDiscovery process to identify foreign language documents and provide initial insights into their content.[32]

Anonymization and Identity Masking are techniques used to protect sensitive information by removing or replacing PII. AI-powered tools can automate these processes, improving efficiency and accuracy while ensuring compliance with data privacy regulations.[33]

By leveraging these AI techniques, eDiscovery practitioners can enhance the efficiency, accuracy, and cost-effectiveness of the discovery process while mitigating risks associated with data privacy and security.

3.2. Beyond AI: Complementary Technologies

Besides AI some other technologies are also revolutionizing eDiscovery. One of them is **Natural Language Processing** (NLP). NLP enables eDiscovery tools to understand and interpret human language. This allows for more intuitive search queries, where users can input conversational prompts instead of relying on rigid keywords. NLP enhances the accuracy and efficiency of document review by identifying relevant information based on context and meaning.[34] **Cloud-based eDiscovery platforms** offer scalable and flexible solutions for managing large volumes of data. These platforms enable secure collaboration among legal teams, streamline data collection and processing, and provide robust analytics capabilities. Cloud computing also reduces the need for expensive on-premises infrastructure, making eDiscovery more accessible to organizations of all sizes.[35] **Advanced data analytics tools** provide deeper insights into ESI, allowing legal teams to uncover hidden patterns and relationships within the data. These tools can identify key players, track communication flows, and detect anomalies that may be relevant to the case. Data analytics enhances the ability to build robust legal strategies and uncover critical evidence.[36]

---

[31] EDRM. 2020. The use of artificial intelligence in eDiscovery. Available at: https://edrm.net/wp-content/uploads/dlm_uploads/2021/02/20210203-EDRM-AI-Paper-v-14.pdf (17. 6. 2024).

[32] EDRM. 2020. The use of artificial intelligence in eDiscovery. Available at: https://edrm.net/wp-content/uploads/dlm_uploads/2021/02/20210203-EDRM-AI-Paper-v-14.pdf (17. 6. 2024).

[33] EDRM. 2020. The use of artificial intelligence in eDiscovery. Available at: https://edrm.net/wp-content/uploads/dlm_uploads/2021/02/20210203-EDRM-AI-Paper-v-14.pdf (17. 6. 2024).

[34] Grand View Research, Inc. 2023. Legal AI and the Crucial Role of Natural Language Processing. Decoding Markets & Trends. Available at: https://www.linkedin.com/pulse/legal-ai-crucial-role-natural-language-processing-9wvsf/ (15. 6. 2024).

[35] JDSUPRA. 2023. Modern eDiscovery Solutions: The Case for the Cloud in 2023. Available at: https://www.jdsupra.com/legalnews/modern-ediscovery-solutions-the-case-7455173/ (3. 7. 2024).

[36] Doclime. How is Data Analytics Improving E-Discovery for Paralegals? Available at: https://doclime.com/blog/data-analytics-improving-e-discovery-for-paralegals (15. 7. 2024).

3.3. AI Revolutionizing eDiscovery

As seen in previous chapters eDiscovery is facing many challenges and is about to face even more in future (with exponential growth of data volume). The exponential growth of electronic data has transformed the legal landscape, making eDiscovery an increasingly complex and resource-intensive process. Traditional eDiscovery methods are struggling to keep pace with the sheer volume of data generated daily. To address these challenges, the legal industry is turning to AI. AI is revolutionizing eDiscovery by enhancing efficiency, improving accuracy, reducing costs, and providing deeper insights into data.

Enhancing Efficiency and Speed - AI's capacity to enhance efficiency and speed represents one of its most substantial contributions to eDiscovery. Traditional eDiscovery methodologies necessitate extensive manual labor to review vast datasets and identify pertinent information. AI technologies, including ML and natural language processing (NLP), can automate these tasks, significantly reducing the time required for document review and data processing.[37] AI-powered tools facilitate rapid analysis of terabytes of data, identifying relevant documents and streamlining the review process. This allows legal professionals to concentrate on strategic tasks, thereby augmenting productivity.[38]

Improving Accuracy and Reducing Errors – The accuracy of eDiscovery is critical, as errors can lead to significant legal and financial consequences. AI enhances the accuracy of eDiscovery by analyzing large datasets with high precision, thereby reducing the likelihood of errors that human reviewers might introduce. AI algorithms can detect inconsistencies, anomalies, and potential risks within documents, ensuring a thorough and reliable review process, which is paramount in legal proceedings.[39]

Cost-reduction – As being said eDiscovery is a quite costly due to the labor-intensive nature of document review. AI offers a cost-effective alternative by automating routine tasks, reducing the necessity for extensive human involvement, and consequently yielding substantial cost savings for legal teams. [40]

Advanced Document Analysis – AI's advanced analytical capabilities signify a major advancement in document analysis. Beyond mere keyword searches, AI can identify complex patterns, relationships, and themes within datasets, uncovering hidden connections and insights that might elude human reviewers.[41]

---

[37] Create Progress. 2024. The Role of AI in E-Discovery: Enhancing Litigation with Efficient and Cost-Effective Solutions. Available at: https://createprogress.ai/the-role-of-ai-in-e-discovery-enhancing-litigation-with-efficient-and-cost-effective-solutions/ (8. 6. 2024).

[38] Deloitte. 2024. The future of legal work? The use of Generative AI by legal departments. Available at: https://www.deloitte.com/content/dam/assets-shared/docs/services/legal/2024/dttl-genai-legal-work-full-report.pdf (15. 7. 2024).

[39] Complex Discovery. 2024. AI Trends in eDiscovery: Comparative Analysis of Recent Survey Results. Available at: https://complexdiscovery.com/ai-trends-in-ediscovery-comparative-analysis-of-recent-survey-results/ (14. 7. 2024).

[40] Nawaz, N. *et al*. 2024. The Adoption of Artificial Intelligence in Human Resources Management Practices. *International Journal of Information Management Data Insights*, 4(1), p. 100208.

[41] Blessing, E., Klaus, H., Potter, K. (2023) Utilizing AI and Data Analytics to Derive Insights from Large Datasets, Aiding in Decision-making Processes. Available at: https://www.researchgate.net/

Adapting to Natural Language Processing (NLP) NLP is one of the most exciting developments within AI. NLP tools, such as ChatGPT, enable users to interact with technology using conversational prompts and queries. This capability is transforming eDiscovery by allowing legal professionals to search for and retrieve information in a more intuitive manner. Instead of relying on rigid search terms, legal professionals can input natural language queries, and AI can interpret and execute these queries, retrieving relevant documents more efficiently than traditional keyword-based searches. This adaptability enhances the accessibility and user-friendliness of eDiscovery tools.[42]

3.4. Challenges and Considerations

While AI offers numerous advantages, there are challenges and considerations that must be addressed. **Data privacy and security** are paramount concerns, as handling sensitive information necessitates stringent safeguards to prevent breaches and unauthorized access. **Ensuring the ethical use of AI**, particularly in avoiding biases and maintaining fairness in automated decision-making, is another critical issue. Integrating AI with existing systems and workflows presents complexities. Legal professionals must be trained to effectively utilize AI tools, and organizations must manage the transition from traditional methods to AI-driven processes. Addressing these challenges is essential to maximizing the benefits of AI while ensuring compliance with legal and ethical standards.[43]

4. THE FUTURE OF EDISCOVERY

As technology continues to evolve, the future of eDiscovery promises even greater advancements and efficiencies. Emerging technologies such as blockchain for secure data verification, augmented reality for enhanced data visualization, and more sophisticated AI algorithms will further transform the landscape of eDiscovery. Legal professionals must remain adaptable and proactive in embracing these innovations to stay ahead in an increasingly digital world.[44] As AI and automation technologies continue to mature, their integration into eDiscovery processes will become more seamless. This will further reduce the reliance on manual review, enhance accuracy, and lower costs. AI-powered predictive coding and automated document classification are expected to become standard practices.[45] With

publication/376650485_Utilizing_AI_and_data_analytics_to_derive_insights_from_large_datasets_aiding_in_decision-making_processes

[42] Kmetz, R. 2024. Unveiling the Power of NLP: ChatGPT and the Evolution of Natural Language Processing. Available at: https://ryankmetz.medium.com/unveiling-the-power-of-nlp-chatgpt-and-the-evolution-of-natural-language-processing-010e9f0235f7 (16. 7. 2024.).

[43] Karthik Devineni, S. (2024) AI in Data Privacy and Security. International Journal of Artificial Intelligence and Machine Learning 3(1):35-49.

[44] Hassan *et al*. 2019. Blockchain and the Future of E-Discovery. Preprint. Available at: https://www.researchgate.net/publication/331730251_Blockchain_And_The_Future_of_the_Internet_A_Comprehensive_Review (26. 7. 2024).

[45] Business Network Solutions. 2024. How AI and Automation are Revolutionizing Document Management for Law Firms. Available at: https://bnsasia.biz/how-ai-and-automation-are-revolutionizing-document-management-for-law-firms/ (15. 6. 2024).

the growing emphasis on data privacy and security, eDiscovery practices will need to adapt to comply with stricter regulations. Organizations will need to implement robust data protection measures and ensure that their eDiscovery processes are compliant with laws such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA).[46] It is assumed that legal standards and best practices for eDiscovery will continue to evolve in response to technological advancements and changing regulatory landscapes. Courts and regulatory bodies will likely provide more guidance on the use of AI and automation in eDiscovery, setting new precedents and shaping industry practices.[47] Collaboration and communication tools will play a crucial role in the future of eDiscovery. As legal teams become more distributed, the ability to securely share and collaborate on ESI will be essential. Advanced collaboration platforms will facilitate real-time communication, document sharing, and joint analysis, improving the overall efficiency of the eDiscovery process.[48]

5. CONCLUSION

eDiscovery has revolutionized the handling of electronic evidence in the legal profession, offering significant benefits in terms of efficiency, cost reduction, and accuracy. However, it also presents challenges, such as high initial costs, complexity, data security risks, and the potential for over-reliance on technology. A balanced approach that leverages the advantages of eDiscovery while addressing its limitations is essential for optimizing its effectiveness in legal proceedings.

AI, in particular, is poised to further transform the legal industry. By automating routine tasks, enhancing accuracy, and uncovering hidden patterns, AI has the potential to significantly improve the eDiscovery process. However, challenges such as data privacy, algorithmic bias, and the need for specialized expertise must be carefully addressed to fully realize AI's benefits.

The broader implications of AI for the legal profession are profound. By automating mundane tasks, AI frees up legal professionals to focus on higher-value activities, such as strategic thinking and client counseling. However, the ethical implications of AI cannot be ignored. Developing robust legal frameworks and ethical guidelines will be crucial to ensuring that AI is used responsibly and beneficially.

The future of the legal profession will undoubtedly be shaped by AI and other emerging technologies. To thrive in this evolving landscape, legal professionals must embrace continuous learning and adapt their practices accordingly. By understanding the potential of AI and addressing its limitations, the legal industry can harness its power to deliver more efficient, accurate, and just outcomes.

---

[46] ZZapproved. 2022. The Ultimate Guide to GDPR and Ediscovery. Available at: https://zapproved.com/blog/general-data-protection-regulation-gdpr-need-to-know-how-to-prepare/ (26. 7. 2024).

[47] Jaloudi, R. 2024. The Future of eDiscovery: Navigating Legal Tech Advancements in the Digital Age. Medium. Available at: https://medium.com/@rjaloudi/the-future-of-ediscovery-navigating-legal-tech-advancements-in-the-digital-age-da57ee1d7b55 (15. 6. 2024).

[48] Purdue Global Law School. 2022. Collaboration Tools Are Making E-Discovery More Complex. Available at: https://www.purduegloballawschool.edu/blog/news/collaboration-tools-make-ediscovery-complex (27. 7. 2024).

LIST OF REFERENCES

Literature

Blessing, E., Klaus, H. & Potter, K. 2023. Utilizing AI and data analytics to derive insights from large datasets, aiding in decision-making processes. ResearchGate. Available at: https://www.researchgate.net/publication/376650485_Utilizing_AI_and_data_analytics_to_derive_insights_from_large_datasets_aiding_in_decision-making_processes (9. 8. 2024).

Caserta, S. & Rask Madsen, M. 2019. The Legal Profession in the Era of Digital Capitalism: Disruption or New Dawn? *Laws,* 8(1), pp. 1-17. https://doi.org/10.3390/laws8010001

DeBono, J. 2008. Preventing and Reducing Costs and Burdens Associated with E-discovery: The 2006 Amendments to the Federal Rules of Civil Procedure. *Mercer Law Review*, 59(3), pp. 963-990. Available at: https://digitalcommons.law.mercer.edu/jour_mlr/vol59/iss3/6 (9. 8. 2024).

Hassan *et al*. 2019. Blockchain and the Future of E-Discovery. Preprint. Available at: https://www.researchgate.net/publication/331730251_Blockchain_And_The_Future_of_the_Internet_A_Comprehensive_Review (26. 7. 2024).

Nawaz, N. *et al*. 2024. The Adoption of Artificial Intelligence in Human Resources Management Practices. *International Journal of Information Management Data Insights*, 4(1), p. 100208. https://doi.org/10.1016/j.jjimei.2023.100208

McCarthy, J. *et al.* 1955. A proposal for the Dartmouth Summer Research Project on Artificial Intelligence. JMC Stanford. Available at: http://jmc.stanford.edu/articles/dartmouth/dartmouth.pdf (9. 8. 2024).

Mittelstadt, B. D. *et al*. 2016. The Ethics of Algorithms: Mapping the Debate. *Big Data & Society*, 3(2), pp. 1-21. https://doi.org/10.1177/2053951716679679

Kmetz, R. 2024. Unveiling the Power of NLP: ChatGPT and the Evolution of Natural Language Processing. Available at: https://ryankmetz.medium.com/unveiling-the-power-of-nlp-chatgpt-and-the-evolution-of-natural-language-processing-010e9f0235f7 (16. 7. 2024).

Sakthivel, R. 2023. Complexities of eDiscovery. LinkedIn. Available at: https://www.linkedin.com/pulse/complexities-ediscovery-ravi-sakthivel/ (9. 8. 2024).

Salmerón-Manzano, E. 2021. Legaltech and Lawtech: Global Perspectives, Challenges and Opportunities. In: Salmeron-Manzano, E. (ed.), *Laws and Emerging Technologies*, pp. 61-71. https://doi.org/10.3390/laws10020024

Schwartz, P. M. & Solove, D. J. 2011. The PII Problem: Privacy and a New Concept of Personally Identifiable Information. *New York University Law Review*, 86, pp. 1814-1894.

Scheindlin, S. & Conference, S. 2015. *Electronic Discovery and Digital Evidence in a Nutshell*. St. Paul: West Academic Publishing.

Other Sources

Business Network Solutions. 2024. How AI and Automation are Revolutionizing Document Management for Law Firms. Available at: https://bnsasia.biz/how-ai-and-automation-are-revolutionizing-document-management-for-law-firms/ (15. 6. 2024).

CDS. n. d. The Basics: What is e-Discovery? Available at: https://cdslegal.com/knowledge/the-basics-what-is-e-discovery/ (15. 6. 2024).
Cloud nine. 2022. Managing the Unpredictability of eDiscovery Costs. Available at: https://cloudnine.com/ediscoverydaily/managing-unpredictability-of-ediscovery-costs-with-cloudnine/ (14. 7. 2024).
Cloud nine. Document Clustering for eDiscovery Review. Available at: https://cloudnine.com/legacy/document-clustering/ (14. 7. 2024).
Complex Discovery. 2024. AI Trends in eDiscovery: Comparative Analysis of Recent Survey Results. Available at: https://complexdiscovery.com/ai-trends-in-ediscovery-comparative-analysis-of-recent-survey-results/ (14. 7. 2024).
Create Progress. 2024. The Role of AI in E-Discovery: Enhancing Litigation with Efficient and Cost-Effective Solutions. Available at: https://createprogress.ai/the-role-of-ai-in-e-discovery-enhancing-litigation-with-efficient-and-cost-effective-solutions/ (8. 6. 2024).
Deloitte. 2018. Entity recognition: How electronic discovery can benefit. Available at: https://www2.deloitte.com/us/en/pages/advisory/articles/entity-recognition-how-electronic-discovery-can-benefit.html (15. 7. 2024).
Deloitte. 2024. The future of legal work? The use of Generative AI by legal departments. Available at: https://www.deloitte.com/content/dam/assets-shared/docs/services/legal/2024/dttl-genai-legal-work-full-report.pdf (15. 7. 2024).
Doclime. How is Data Analytics Improving E-Discovery for Paralegals? Available at: https://doclime.com/blog/data-analytics-improving-e-discovery-for-paralegals (15. 7. 2024).
EDRM. Technology Assisted Review. Available at: https://edrm.net/resources/frameworks-and-standards/technology-assisted-review/ (15. 6. 2024).
EDRM. 2020. The use of artificial intelligence in eDiscovery. Available at: https://edrm.net/wp-content/uploads/dlm_uploads/2021/02/20210203-EDRM-AI-Paper-v-14.pdf (17. 6. 2024).
EDRM. 2022. How to Evaluate and Control Ediscovery Costs. Available at: https://edrm.net/2022/04/how-to-evaluate-and-control-ediscovery-costs/ (17. 6. 2024).
Fortune Business Insights. 2024. eDiscovery Market Size, Share & Industry Analysis, By Component (Solutions and Services) By Deployment Model (Cloud and On-premises), By Enterprise Type (Large Enterprises and SMEs), By End-user (BFSI, Retail & Consumer Goods, Government & Public Sector, Healthcare & Life Sciences, IT & Telecommunications, Legal, and Others), and Regional Forecast, 2024-2032. Available at: https://www.fortunebusinessinsights.com/industry-reports/ediscovery-market-101503 (15. 6. 2024).
Grand View Research, Inc. 2023. Legal AI and the Crucial Role of Natural Language Processing. Decoding Markets & Trends. Available at: https://www.linkedin.com/pulse/legal-ai-crucial-role-natural-language-processing-9wvsf/ (15. 6. 2024).
Infosys BPM. E-Discovery automation: Challenges and opportunities. Available at: https://www.infosysbpm.com/blogs/legal-process-outsourcing/e-discovery-automation-challenges-and-opportunities.html (15. 6. 2024).
Jaloudi, R. 2024. The Future of eDiscovery: Navigating Legal Tech Advancements in the Digital Age. Medium. Available at: https://medium.com/@rjaloudi/the-future-of-ediscovery-navigating-legal-tech-advancements-in-the-digital-age-da57ee1d7b55 (15. 6. 2024).

JDSUPRA. 2023. Modern eDiscovery Solutions: The Case for the Cloud in 2023. Available at: https://www.jdsupra.com/legalnews/modern-ediscovery-solutions-the-case-7455173/ (3. 7. 2024).
Klaff, T. 2007. Authenticating E-Discovery As Evidence. *CCB Journal*. Available at: https://ccb-journal.com/articles/authenticating-e-discovery-evidence (15. 6. 2024).
KLDiscovery. What is eDiscovery? Available at: https://www.kldiscovery.com/uk/resources/what-is-ediscovery (8. 6. 2024).
Logikcull. eDiscovery Disrupted: The Potential Effects of AI. Available at: https://www.logikcull.com/blog/ediscovery-disrupted-the-potential-effects-of-ai (3. 6. 2024).
Matich, T. 2024. What Lawyers Need to Know About eDiscovery. Clio. Available at: https://www.clio.com/blog/need-to-know-ediscovery/ (2. 6. 2024).
Matich, T. 2021. 10 Predictions for the Next 10 Years of Legal Tech. Clio. Available at: https://www.clio.com/blog/10-predictions-10-years/ (2. 6. 2024).
Paloalto Networks. What Is Artificial Intelligence (AI)? Available at: https://www.paloaltonetworks.com/cyberpedia/artificial-intelligence-ai (7. 4. 2024).
Percipient. n. d. Bridging the Gap: Legal Tech vs Legal Innovation. Available at: https://percipient.co/bridging-the-gap-legal-tech-vs-legal-innovation/ (2. 6. 2024).
Purdue Global Law School. 2022. Collaboration Tools Are Making E-Discovery More Complex. Available at: https://www.purduegloballawschool.edu/blog/news/collaboration-tools-make-ediscovery-complex (27. 7. 2024).
Rouse, M. 2024. What Is Artificial Intelligence (AI)? Available at: https://www.techopedia.com/definition/190/artificial-intelligence-ai (7. 4. 2024).
Troy, T. 2023. Examining the Impacts, Both Positive and Negative, of Artificial Intelligence on Businesses. Medium. Available at: https://medium.com/@timothytroy/examining-the-impacts-both-positive-and-negative-of-artificial-intelligence-on-businesses-ac17758d787e (22. 6. 2024).
Turney, D. 2024. GPT-4 has passed the Turing test, researchers claim. Live Science. Available at: https://www.livescience.com/technology/artificial-intelligence/gpt-4-has-passed-the-turing-test-researchers-claim (9. 8. 2024).
Veritas. EDRM: What It Is, Why It Matters, and How to Use It? Available at: https://www.veritas.com/information-center/edrm (15. 6. 2020).
ZZapproved. 2022. The Ultimate Guide to GDPR and Ediscovery. Available at: https://zapproved.com/blog/general-data-protection-regulation-gdpr-need-to-know-how-to-prepare/ (26. 7. 2024).

Legal sources

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance), OJ L, 2024/1689.

UDC: 336.7:004(4-67 EU)(439) DOI: 10.56461/iup_rlrc.2024.5.ch15

Zsolt BUJTÁR*
Faculty of Law, University of Pécs, Hungary

THE FUTURE OF CENTRAL BANK DIGITAL CURRENCY IN THE EUROPEAN UNION AND HUNGARY

As of May 2024, 134 central banks representing 98% of the world's GDP (Atlantic Council, 2024) were already exploring the possibility of introducing central bank digital currency. The study analyses the definition of central bank digital currency, the risks involved in its introduction, and the legislative environment for its introduction in the European Union. The study also reviews the possibility of introducing central bank digital currency in the case of Hungary, an EU Member State outside the European Monetary Union, with a particular focus on the monetary policy implications. The author concludes that membership of the European Monetary Union does not materially affect the decision to introduce central bank digital currency.

Keywords: CBDC, fiat money, DLT, monetary policy.

1. INTRODUCTION

The People's Bank of China (PBoC) has been developing and testing the digital yuan since 2014 (Slawotsky, 2020). The commitment to creating central bank digital currency is illustrated by the fact that only small economies have already started experimenting with the introduction of new types of official currencies - not really prepared (the Marshall Islands in 2018, followed by Jamaica and Nigeria) and El Salvador - with the adoption of bitcoin in 2021 - as official currency (Renterina, Wilson & Strohecker, 2021).[1] In parallel with this process, major economic powers such as China, the European Union,

* PhD, Assistant Professor, ORCID: 0009-0000-0756-9337, e-mail: *bujtar.zsolt@ajk.pte.hu*

[1] The problems during implementation can be traced back to two causes. One is that a cryptocurrency, which enjoys greater credibility vis-à-vis the national currency, which will continue to function as the official currency, could be forced out of circulation, devaluing the domestic currency. Another problem is that if an independent legal entity is entrusted by the government with the issuance and management of the new currency. Haan, C. 2019. Marshall Islands Promotes its SOV National Cryptocurrency Development Fund at UN Blockchain Summit in New York. Crowdfund Insider. Available at: https://www.crowdfundinsider.com/2019/06/148086-marshall-islands-promotes-its-sov-national-cryptocurrency-development-fund-at-un-blockchain-summit-in-new-york/ (7. 4. 2024).

Japan and Canada have been weighing up the pros and cons of introducing central bank digital currency since the second half of the 2010s. In 2020, the United States entered the race to adopt central bank digital currency with the concept of the digital dollar - also flagging the US dollar's function as the world's currency, but in the last two years, central bank digital currency has been in the political spotlight in the United States of America (Tews & Harper, 2020).

In June 2023, the European Commission proposed a complex legislative package, the Digital Euro Package, which would allow the legislator to create the legal framework for the introduction of central bank digital currency. In October 2023, the Governing Council of the European Central Bank announced that, after a two-year assessment phase, it would launch a preparatory period for a further two years (European Central Bank, 2023a). In June 2024, the European Central Bank published the first progress report on the development of the digital euro.

Accordingly, the paper first reviews the concept of central bank digital currency and then outlines the risks and benefits of introducing central bank digital currency. The paper then briefly discusses the draft legislative package that serves as the legal framework for the introduction of CBDC in the European Union. As part of this, the features of the digital euro that will emerge from the new legal environment will be outlined, with a particular focus on anonymity and data protection. The author then briefly summarises the position of the Magyar Nemzeti Bank (hereinafter: MNB), the custodian of Hungarian monetary policy, on the introduction of central bank digital currency.

2. DEFINITION OF CENTRAL BANK DIGITAL CURRENCY

2.1. Definition of CBDC

Central bank digital currency is widely defined as central bank money in a digital form that differs from its traditional reserve and account balance form (Bank for International Settlements, 2020). From this definition by the BIS and the seven largest central banks, it is clear that central bank digital currency cannot be implemented as a privately issued currency. In the case of fiat money, the State, exercising the right to issue money conferred on the central bank, has a monopoly which, precisely to exercise the instruments of monetary policy, should not be abandoned in the future.

The above suggests that central bank digital currency is a digital version of the current fiat money. The important difference is that it is not just a new form of electronic money in the form of CBDCs, but an implementation of digital fiat money based on blockchain or similar technology. The technological basis is in the content of the smart contracts, in particular the fact that this form allows the implementation of the pre-programmable money feature, which allows for the very rapid and without the need for new technology, further new or differently functional issuance of money (further issuance of money) in a very short time (even minutes) instead of the current days or weeks for postal services.

3. THE RISKS OF INTRODUCING CENTRAL BANK DIGITAL CURRENCY

3.1. The Monetary Policy Risks of Introducing Central Bank Digital Currency

Central bank digital currency presents many opportunities for monetary policy, but also new challenges. A form of CBDC without a financial intermediary (centralised CBDC), where the central bank would directly hold the accounts of all entities, including households and businesses, would impose a significant administrative burden on the central bank, even with the possibilities of modern technology. The reintegration of commercial banks into central banks, i.e. a single-tier banking system, would be feasible only at considerable risk, precisely because of the diversity of the banking system and the weight of money market funds. What definitively rejects this form of CBDC is precisely the well-established system of monetary transmission in the two-tier banking system, where financial intermediaries transmit elements of the central bank's monetary policy to individual market participants. Financial intermediaries transmit monetary policy objectives through channels such as credit and monetary aggregates, interest rates, asset prices and market interest rates. Without this intermediation system, the central bank's role as lender of last resort would become impossible. The use of this instrument of last resort would open the possibility of excessive central bank intervention: in effect, direct monetary (self-)financing of the public budget, sometimes without even a proper consideration of the necessary risks (Bujtár, 2021).

Financial stability is a state to be achieved for a given economy when the subsystems of the financial system, taken together, are able to withstand an economic shock and function properly in terms of the transmission of financial resources, the management of risks and the operation of payment systems. In the Hungarian context, for example, the financial crisis of 2007-2008 highlighted the importance of financial stability, and therefore, since the last decade the Magyar Nemzeti Bank has been operating with a kind of "dual mandate", i.e. in addition to maintaining price stability as the primary central bank objective, it has been paying increasing attention to economic growth and financial stability. This double objective was extended in June 2021 to include environmental sustainability (MNB, 2021).

The emergence of central bank digital currency in the financial system may have a direct impact on market interest rates, asset prices and foreign exchange rates, and an indirect impact on monetary and credit aggregates through these sub-markets.

The main risk of digital money is a loss of confidence in the financial system. This can take the form of a lack of confidence in the new currency, but also of a loss of established financial confidence.

3.2. Possible Positive Monetary Policy Effects of the Introduction of the CBDC

The introduction of the CBDC could have a positive impact on the market interest rate channel. Indeed, central bank digital currency could reduce the need for negative interest rates and reduce the impact of the liquidity trap that is already occurring close to the zero-interest rate level. Similarly, the possibility of different interest rates

depending on the identity of the economic agents using the CBDC could work, defining a kind of smart contract for the range of interest rates per user. This solution could also ensure that, with the policy rate reduced to negative levels, there is no excessive quantitative and qualitative easing, and that the long-term government bond yield curve is kept at a permanently low level (Bujtár, 2021).

Indeed, the persistent use of these three instruments could lead to significant distortions, which could reduce financial stability by creating asset bubbles in the equity, bond or real estate markets, or in any of these together.

A continued active interest rate policy could provide a stabilising effect on the foreign exchange sub-market by raising interest rates if necessary to boost confidence in the home currency, or by selectively cutting rates to counter excessive appreciation in the case of flight currencies or carry-trade currencies. This process can have a particularly significant impact in the case of an open economy, such as the Hungarian economy, which is at the same time pursuing a high-pressure economic policy. Stable levels of market interest rates, bubble-free asset prices and a balanced exchange rate, as well as financial stability, could also have a positive impact on monetary and credit aggregates. Balanced exchange rate policies can support the prevention of excessive indebtedness and the build-up of excess money in this financial sub-market.

4. LEGAL POSSIBILITIES FOR THE INTRODUCTION OF CENTRAL BANK DIGITAL CURRENCY IN THE EUROPEAN MONETARY UNION

4.1. Legal Possibilities for the Introduction of CBDC in the European Monetary Union Prior to the Digital Euro Package

The financial system of the European Union, the European Monetary Union, in the absence of full accession by the Member States, presupposes the dual monetary system of the euro and the national currencies of the non-acceding Member States over a long period of time. The link between the two currency groups is established by the European Central Bank, with its dual governance (Executive Board and Board of Governors) and the coordination of the common monetary policy and the supervision of the financial system. It is therefore necessary to talk separately about the digital euro as a single currency and the digital currencies of the non-member countries.[2] While the digital euro is in competition for the role of global currency, the CBDCs of the non-member countries cannot participate in this competition because of their lower economic strength. However, besides the apparent disadvantage, this also serves as an advantage in that the

[2] The digital euro outlined in the Digital Euro Package will be available to natural and legal persons in all EU Member States, precisely by, payment service providers from non-euro area Member States will be subject to the rules set out in the Digital Euro Package, thus ensuring full protection against money laundering and terrorist financing. See: Proposal for a Regulation of the European Parliament and of the Council on the provision of digital euro services by payment services providers incorporated in Member States whose currency is not the euro and amending Regulation (EU) 2021/1230 of the European Parliament and the Council Preamble, sections 4-5.

non-member States (including Hungary) can continue to pursue an independent monetary policy, which the CBDC can maintain and strengthen. In the following, the paper first presents the general legal regulatory options for the digital euro.

When examining the EU acquis, the choice of primary EU law on which to base the CBDC issuance depends on the form of the digital euro and its purpose of issuance.[3] However, the clear need for and feasibility of introducing a full (retail) CBDC has already become clear. Thus, the digital euro would be issued as a dual-issue and general retail CBDC through the ESCB, i.e. through accounts held with the Eurosystem, and would thus be made available for use by households and private entities. The legal basis in the Eurosystem would then be the primary legislation governing the ECB's operations;[4] the legal basis for two-tier general issuance would be the provision on clearing and payment systems in the Statute of the ESCB and the ECB.[5]

If the digital euro were to be created in a centralised form for the clearing system and to have a limited use, i.e. to be issued only as a means of settlement for specific types of payments, processed by a dedicated payment infrastructure accessible only to eligible participants, the most appropriate legal basis would again be the primary legislation[6] and the provision on clearing and payment systems in the Statute of the ESCB and the ECB.[7]

If and when the digital euro were to be issued as an instrument equivalent to a banknote, i.e. as a token-type CBDC, the most appropriate legal basis for issuance would no longer be the above-mentioned legislation, but the TFEU provision on banknote issuance,[8] also in conjunction with the Statute of the ESCB and the ECB, which concerns the ECB's and national central banks' monopoly on the issuance of the euro.[9]

On the basis of the above, it can be concluded that the TFEU provision on the monopoly for banknote issuance[10] and the reference to it in the banknote issuance provisions of the Statute of the ESCB and the ECB[11] would give the Eurosystem a very wide margin of discretion to issue different types of CBDCs.[12] It is also important to note that within the Union, only the Governing Council of the ECB has the power to authorise the issuance of euro banknotes. Given the ECB's independence, it cannot be obliged to do so by any

---

3 European Central Bank. 2020. Eurosystem: Report on a Digital Euro, pp. 1-54. Available at: https://www.ecb.europa.eu/pub/pdf/other/Report_on_a_digital_euro~4d7268b458.en.pdf (21. 6. 2024).

4 European Central Bank, 2020.

5 TFEU Protocol No 4 on the Statute of the European System of Central Banks and of the European Central Bank Art. 17.

6 Art. 127(2) TFEU.

7 TFEU Protocol No 4 on the Statute of the European System of Central Banks and of the European Central Bank Art. 22.

8 Art. 127(2) TFEU.

9 TFEU Protocol No 4 on the Statute of the European System of Central Banks and of the European Central Bank Art. 16.

10 Art. 128(1) TFEU.

11 TFEU Protocol No 4 on the Statute of the European System of Central Banks and of the European Central Bank Art. 16.

12 European Central Bank, 2020.

other EU institution, and therefore only this ECB body can decide on the introduction of CBDCs.[13] As the ECB and the national central banks are entitled to issue banknotes accepted as legal tender, the TFEU's monopoly on banknote issuance does not allow for the introduction of a private token as legal tender with a central bank commitment, and hence the central bank commitment necessary for it to become a CBDC.

Based on the above, it can be concluded that, with the modification of the central bank regulations for the euro,[14] central bank digital currency could have been integrated even before the Digital Euro Package.

4.2. A Stand-Alone Digital Euro Package as the Next Step in the Legal Regulatory Process

In October 2023, the Governing Council of the European Central Bank announced the start of a further two-year preparation period following the two-year assessment phase (European Central Bank, 2023a).

The aim of this preparatory phase was to lay the foundations for a potential digital euro by finalising the rulebook, selecting the service providers that will develop the digital platform and defining the development framework for the infrastructure that will operate and support the digital euro.

Almost in support of this process, the European Commission published a legislative package proposal, the Digital Euro Package, in June 2023. The legislative package consists of a Regulation establishing the legal framework for a possible digital euro (Proposed Digital Euro Regulation), a Regulation on the provision of digital euro services by payment services providers incorporated in Member States whose currency is not the euro and a Regulation on the legal tender of euro coins and banknotes (Proposed Legal Tender Regulation). In the legislative process, the European Central Bank would have the option, after approval by the European Parliament and the Council, to introduce a digital euro market alongside the current fiat euro, if and when the European Central Bank takes a positive decision (Clifford Chance, 2023).

Looking at the legal framework, it is important to note that the European Commission's Digital Euro Bill proposal takes into account not only the existing PSD2,[15] but also the amendments to the Payment Services Directive 3 (PSD3) and Payment Services Regulation (PSDR), which will enter into force later, and the Directive on the prevention of the use of the financial system for the purpose of money laundering or terrorist financing (AMLD5)[16] and the amendments to the AMLD6 and AMLR, which are expected to enter into force later.

---

[13] Art. 128(1) TFEU.

[14] Art. 128(1) TFEU and Art. 16 of Protocol (No 4) on the Statute of the European System of Central Banks and of the European Central Bank, TFEU.

[15] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC.

[16] Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU.

4.2.1. Characteristics of the Digital Euro

Following the completion of the European Central Bank's test phase for the introduction of the digital euro in 2023, the main characteristics of a potential digital euro have been summarised at the end of the test phase:

- widely accepted and easy to use;
- free for basic use;
- usable for any digital payment in the euro area;
- not requiring an online connection (it could also be used offline);
- offering the highest possible protection of privacy;
- inclusive, leaving no one behind;
- settling payments instantly;
- secure;
- risk-free (as money issued by the central bank);
- usable for payments at the point of sale and person-to-person.[17]

From the above, and from the summary of the study phase, it can be concluded that the digital euro will be retail in terms of users, decentralised in terms of settlement, token-based in terms of appearance and centralised in terms of issuance, with strong cryptographic elements, but not necessarily using DLT technology.

4.3. The Data Protection Aspects

The European Central Bank's anonymity project[18] has been investigating the creation of a CBDC issued by the central bank with cash-like characteristics, using a two-tier control structure that is partially anonymous and ensures protection against money laundering and terrorist financing. This is important because it will enable it to offer a secure solution that complies with the legislation in force (and in particular with the legislation in force to combat money laundering and terrorist financing) and in which confidence can be built and maintained. This latter trust is important for two reasons: not only to ensure that the digital euro is actually used by end-users but also to ensure that it is capable of expanding the monetary toolbox and becoming part of it.

User data protection is already well supported by the digital euro infrastructure through the use of chip technology[19] and by specifically limiting the use of data by payment service providers. [20]

---

[17] European Central Bank. 2023b. Eurosystem: A stockage on the digital euro - Summary report on the investigation phase and outlook on the next phase. Available at: https://www.ecb.europa.eu/euro/digital_euro/timeline/profuse/shared/pdf//ecb.dedocs231018.en.pdf (21. 6. 2024).

[18] European Central Bank. 2019. Exploring anonymity in central bank digital currencies. In focus. 4(4-6), pp. 1-10. Available at: https://www.ecb.europa.eu/press/intro/publications/pdf/ecb.mipinfocus191217.el.pdf (21. 6. 2024).

[19] "A tamper-proof chip with pre-installed software that can store confidential and cryptographic data and run secure applications." See: European Central Bank. 2023b.

[20] "...the settlement infrastructure would not be able to trace the information to back a specific user thanks to hashing and other cryptographic techniques." See: European Central Bank. 2023b..

The digital euro will be available to a wide range of end-users following the onboarding process after the introduction of the digital euro, who will either be natural persons or business users. Onboarding is the process when an end-user uses the digital euro for the first time. For natural person end-users, when they first interact with a payment service provider with the digital euro, the payment service provider will carry out the identification process by adding the KYC function and assigning a unique digital euro account number (DEAN) to the new end-user.[21] In addition to the latter, it will also be possible to use other identifiers and to request a physical card, and access to a digital euro application for each online and offline transaction will be granted to the new natural person who joins the digital euro as a completion of the onboarding process.

The European Central Bank (ECB) in its first progress report on developing a central bank digital currency focused mainly on privacy provisions with the ECB promising pseudonymization, hashing functions, and encryption features against tracking individuals by transaction.[22]

5. HUNGARIAN MONETARY POLICY AND CENTRAL BANK DIGITAL CURRENCY

Hungarian monetary policy has a dual role in the introduction of central bank digital currency. On the one hand, like the other 133 central banks, the MNB (also in a separate volume of studies[23]) is examining the possibility of introduction and its effects on the Hungarian economy and Hungarian society. On the practical side, the MNB is actively involved in international pilot programmes, such as the mBridge wholesale CBDC project, a joint project of the BIS Innovation Hub Hong Kong and the central banks of China (PBoC), Thailand (BoT), Hong Kong (HKMA) and the United Arab Emirates (CBUAE), in which the ECB has joined as an observer, as has the Magyar Nemzeti Bank (Fáykiss, Nyikes & Szombati, 2023).

Two retail CBDC projects have been launched by the Magyar Nemzeti Bank: the Money Museum App, which is an application implementing blockchain technology in the central banking environment and operating in a live environment; and the Student Savings App, which is the first in the European Union to issue central bank digital currency to real users in May 2023 - on a pilot basis (Fáykiss, Nyikes & Szombati, 2023).

The Magyar Nemzeti Bank, examining the decision-making system for the introduction of the CBDC, concluded that the primary decisions for the introduction of central bank digital currency are a) the purpose, b) the scope of availability and c) the effective feasibility, especially from a monetary policy perspective. If and when a decision on these three issues is reached, the d) formal, e) functional, f) operational and operational and then most importantly g) anonymity and infrastructure issues could be

[21] European Central Bank. 2023b.

[22] European Central Bank. Timeline and progress on a digital euro - Introduction. Available at: https://www.ecb.europa.eu/euro/digital_euro/progress/html/ecb.deprp202406.en.html (24. 6. 2024).

[23] Magyar Nemzeti Bank - MNB. 2021. Egy új kor hajnalán – Pénz a 21. században. Available at: https://www.mnb.hu/kiadvanyok/mnb-szakkonyvsorozat/egy-uj-kor-hajnalan-penz-a-21-szazadban (21. 6. 2024).

addressed. Until an economic policy decision is taken on the first three issues, the question of deployment will remain a theoretical debate, despite the more significant practical experience described above. While the independence of monetary policy could be supported by a stand-alone central bank digital currency, the Hungarian economy is too small for this, and it will be necessary to develop the final conditions for its introduction on the basis of the larger experiences (euro, digital yuan and cross-border CBDC). For a national economy that is significantly integrated into the European and international economy, this consideration seems well founded, so perhaps unsurprisingly the digital euro could serve as a model for the future introduction of a Hungarian digital forint.

6. SUMMARY

The study examined the drivers for the introduction of central bank digital currency and the characteristics that a central bank digital currency that meets the challenges of the digital age should have. Finally, the author examined the legal environment for the introduction of the digital euro, noting that the possibilities for the introduction of the digital euro were already available before the Digital Euro Package of 2023. The ECB is not expected to decide on the introduction of the digital euro until the end of 2026 at the earliest, after a further two-year assessment period. The author concludes that membership of the European Monetary Union will not materially affect the decision on the introduction of central bank digital currency.

LIST OF REFERENCES

Atlantic Council. 2024. Central Bank Digital Currency Tracker – Scroll to Explore. Available at: https://www.atlanticcouncil.org/cbdctracker (30. 6. 2024).

Bank for International Settlements. 2020. Central bank digital currencies: foundational principles and core features. Report no. 1 in a series of collaborations from a group of central banks: The Bank of Canada, European Central Bank, Bank of Japan, Sveriges Riksbank, Swiss National Bank, Bank of England, Board of Governors of the Federal Reserve and Bank for International Settlements. Available at: https://www.bis.org/publ/othp33.pdf (21. 6. 2024).

Bujtár, Zs. 2021. The monetary policy challenges of digital central bank money. In: Bujtár, Zs. *et al.* (eds.), *The world of cryptoassets from the perspective of law and economics: conference proceedings: selected papers*. Pécs: University of Pécs, Faculty of Law and Political Sciences (PTE ÁJK), pp. 114-115.

Clifford Chance. 2023. What does the European Commission's Digital Euro Proposal mean for the Future of Money in the EU? Available at: https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2023/07/what-does-the-european-commissions-digital-euro-proposal-mean-for-the-future-of-money-in-the-eu.pdf (21. 6. 2024).

Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/

EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC.
Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU.
European Central Bank. 2019. Exploring anonymity in central bank digital currencies. *In focus*. 4(4-6), pp. 1-10. Available at: https://www.ecb.europa.eu/press/intro/publications/pdf/ecb.mipinfocus191217.el.pdf (21. 6. 2024).
European Central Bank. 2020. Eurosystem: Report on a Digital Euro, pp. 1-54. Available at: https://www.ecb.europa.eu/pub/pdf/other/Report_on_a_digital_euro~4d7268b458.en.pdf (21. 6. 2024).
European Central Bank. Timeline and progress on a digital euro - Introduction. Available at: https://www.ecb.europa.eu/euro/digital_euro/progress/html/ecb.deprp202406.en.html (24. 6. 2024).
European Central Bank. 2023a. Eurosystem proceeds to next phase of digital euro project. Available at: https://www.ecb.europa.eu/press/pr/date/2023/html/ecb.pr231018~111a014ae7.en.html (21. 6. 2024).
European Central Bank. 2023b. Eurosystem: A stockage on the digital euro - Summary report on the investigation phase and outlook on the next phase. Available at: https://www.ecb.europa.eu/euro/digital_euro/timeline/profuse/shared/pdf//ecb.dedocs231018.en.pdf (21. 6. 2024).
Fáykiss, P., Nyikes, Á. & Szombati, A. 2023. The Future of Money – Central Bank Digital Currency. *Polgári Szemle*, 19(4-6), pp. 33-47. https://doi.org/10.24307/psz.2023.1204
Haan, C. 2019. Marshall Islands Promotes its SOV National Cryptocurrency Development Fund at UN Blockchain Summit in New York. Crowdfund Insider. Available at: https://www.crowdfundinsider.com/2019/06/148086-marshall-islands-promotes-its-sov-national-cryptocurrency-development-fund-at-un-blockchain-summit-in-new-york/ (7. 4. 2024).
Magyar Nemzeti Bank - MNB. 2021. Egy új kor hajnalán – Pénz a 21. században. Available at: https://www.mnb.hu/kiadvanyok/mnb-szakkonyvsorozat/egy-uj-kor-hajnalan-penz-a-21-szazadban (21. 6. 2024).
Magyar Nemzeti Bank - MNB. 2022. Zöld jegybanki eszköztár-stratégia. Available at: https://www.mnb.hu/monetaris-politika/a-monetaris-politikai-eszkoztar/zold-jegybanki-eszkoztar-strategia (21. 6. 2024).
Proposal for a Regulation of the European Parliament and of the Council on the provision of digital euro services by payment services providers incorporated in Member States whose currency is not the euro and amending Regulation (EU) 2021/1230 of the European Parliament and the Council Preamble.
Renterina, N., Wilson, T. & Strohecker, K. 2021. In a world first, El Salvador makes bitcoin legal tender. Reuters. Available at: https://www.reuters.com/world/americas/el-salvador-approves-first-law-bitcoin-legal-tender-2021-06-09/ (24. 6. 2024).

Slawotsky, J. 2020. US Financial Hegemony: the Digital Yuan and Risks of Dollar De-Weaponization. *Fordham International Law Journal*, 44(1), pp. 39-100.

TFEU Protocol No 4 on the Statute of the European System of Central Banks and of the European Central Bank.

Tews, S. & Harper, J. 2020. The Potential of the Digital Dollar: Highlights from My Conversation with Jim Harper. AEI. Available at: https://www.aei.org/technology-and-innovation/the-potential-of-the-digital-dollar-highlights-from-my-conversation-with-jim harper/ (15. 6. 2024).

UDC: 004.78:336.226.2 DOI: 10.56461/iup_rlrc.2024.5.ch16

Alexander SZIVÓS*
Faculty of Law, University of Pécs, Hungary
EY Hungary

TAXING THE DIGITAL ECONOMY

The research explores the complex territory of taxing the digital economy, examining the challenges and opportunities arising from the application of novel tax measures and advanced tools to digitalise tax administration. In the wake of the evolving technology landscape, traditional tax frameworks face unprecedented challenges in collecting revenue from digital transactions, necessitating a reassessment of tax policy and administration methods. Key challenges include the elusive nature of digital transactions, the difficulty in establishing a fair and effective tax system, and the pervasive problem of tax evasion in the digital economy. To address these challenges, the study examines innovative tax measures and advanced tools aimed at modernising tax administration and promoting economic transparency. In the pursuit of a more transparent tax landscape, the research emphasises the use of these new taxes and tools to incentivise compliance, discourage evasion and promote economic formalisation. In addition, the study examines the OECD's Base Erosion and Profit Shifting (BEPS) 2.0 project, which is playing a key role in shaping the international response to the tax challenges posed by the digital economy. The research assesses the implications, recommendations and potential contributions of the BEPS 2.0 project to a coordinated global approach to addressing the tax issues associated with the digitalisation of economic activity.

Keywords: digital economy, technology, taxation, tax evasion, BEPS 2.0.

1. INTRODUCTION

The advent of the digital economy has revolutionized the way we conduct business, communicate, and exchange goods and services. With this transformation, however, comes a new set of challenges in many areas of our life, and also for tax authorities worldwide. Traditional tax systems, designed in an era where business activities were more tangible and geographically bound, are now grappling with the virtual and often borderless nature of digital transactions (Országgyűlés Hivatala, 2021, p. 1). The digital economy is characterized by its fluidity and the intangible nature of its transactions.

* PhD, Senior Tax Advisor, ORCID: 0000-0003-0959-5621, e-mail: *szivos.alexander@ajk.pte.hu*

Companies can operate and generate substantial revenues in jurisdictions without a physical presence, complicating the application of existing tax laws (Slemrod & Weber, 2012, pp. 25–29). This has led to significant challenges in ensuring that tax revenue is collected effectively and fairly. The elusive nature of digital transactions makes it difficult to track and tax them in the same way as traditional commerce (Consilium.europa.eu, 2024). Moreover, the rapid pace of technological advancement often outstrips the ability of tax legislation to adapt, leading to loopholes and opportunities for tax evasion (Slemrod, 2006, p. 3; Khlif & Achek, 2015, pp. 487–492).

In response to these challenges, researchers and policymakers are examining innovative tax measures and leveraging advanced tools to modernize tax administration (OECD, 2013; Perez Lopez, Delgado Rodrıguez & de Lucas Santos, 2019). These initiatives aim to enhance economic transparency and ensure that tax systems remain relevant in the digital age (Varga, 2020).

This study delves into the complex interplay of tax mechanisms within the digital economy, scrutinizing the challenges and opportunities that arise as we move towards more sophisticated tax strategies and the digitization of tax systems. It explores the complicated nature of digital transactions, the obstacles in creating an equitable tax framework, and the prevalent problem of tax avoidance in the digital sphere. Through an extensive examination of progressive tax methods and the adoption of advanced technologies, this research seeks to lay the groundwork for the evolution of tax administration and the improvement of fiscal transparency. As we navigate the intricacies of digital tax reform, the paper also addresses the significant role of the OECD's Base Erosion and Profit Shifting (BEPS) 2.0 initiative in orchestrating a collective international effort to tackle the tax issues brought forth by the digitalization of business. The study assesses the potential impacts, practical suggestions, and notable contributions of the BEPS 2.0 initiative, highlighting the endeavours to establish a harmonized global approach to taxing the digital economy. In essence, this introduction sets the stage for a comprehensive exploration into the necessity of effectively taxing the digital economy.

2. TAX EVASION IN THE DIGITAL WORLD

A “good” tax system is one that achieves the goals of equity, efficiency, and adequacy (Szilovics, 2003, pp. 55–60). Tax evasion—when individuals and firms do not pay their legally due tax liabilities in a timely manner—compromises all of these goals (Alm, 2021, p. 322). Tax evasion can be defined as any criminal activity or any offence of dishonesty punishable by civil penalties that is intended to reduce the taxation incidence, and depends on economic and tax structures, types of income, and social attitudes. The concept of tax evasion in the existing literature has been described from an economic or public finance perspective and very few studies have discussed the issue from a philosophical or ethical viewpoint. The basic theoretical model of tax evasion is a straightforward application of individual choice under uncertainty and the problem an individual faces is whether or not to evade some part of their legal tax liability, given that there is some probability of being caught if they decide to evade. Tax evasion involves

illegal activities such as deliberately not reporting or under-reporting income, falsifying records or invoices, concealing assets or income, engaging in cash economy to avoid leaving a trace of transactions, using offshore accounts to hide income or assets (Saez & Zucman, 2019; Szilovics, 2003, pp. 47–51).

Tax fraud is a broader term that encompasses tax evasion but also includes other fraudulent activities against the tax system, such as submitting false documents or making false claims to the Tax Authority, using or creating fake companies to evade taxes. engaging in VAT fraud, such as carousel fraud or missing trader fraud (Szilovics, 2024, p. 7; Allingham & Sandmo, 1972; Stiglitz, 1969).

The basic issue in tax administration has always been getting information on taxpayers and their activities, and for much of history tax administrations did not have full, complete, and timely information. Even during much of the twentieth century information has been limited, due to several factors. Many transactions were in cash, so that there was no "paper trail" that could be used to verify the accuracy of any reports. Many types of transactions were not reported via third party information, so again, there was no paper trail of transactions. Many types of income were also not subject to source withholding, which also decreased the flow of information to the tax authorities. Many types of tax shelters were shrouded in secrecy. Both companies and individuals hid income and assets in offshore accounts. Many multinationals were able to shift profits to low-tax jurisdictions via transfer prices that were largely hidden and, even when reported, that could not be independently verified. Overall, these factors generated several main strategies for tax evasion during much of the twentieth century. Taxpayers would fail to report all cash receipts and cash expenses on their tax returns; indeed, many individuals would simply fail to file a tax return. The end result was predictable: tax evasion (along with money laundering and tax avoidance) existed, persisted, and flourished in most countries around the world, largely because tax administrations did not have the information necessary to prevent these practices (Zucman, 2013, pp. 1333–1334; Alstadsæter, Johannesen & Zucman, 2019, pp. 2082–2083; Unger & van der Linde, 2015).

Technological improvements and digitalization have influenced the tax collection processes worldwide by improving the speed, quality, and accuracy of the data and changing the ways of reporting, controlling, and auditing the taxes. Tax authorities, policymakers, regulators, accountants, and taxpayers have realized the opportunities of digitalization and started to get benefits from e-services, applications, websites, software, etc. (Slemrod, 2019). Digitalization may reduce tax fraud by enhancing information collection, improving control tools, and increasing efficiency while giving new opportunities for evading the tax (Zucman, 2015; Gupta *et al.,* 2017; Yamen, Coskun & Mersni, 2023).

Digital services taxes (DSTs) have been introduced in several countries to target revenue generated from digital activities, such as online advertising and the sale of user data. DSTs are levied on income derived from online advertising, the sale of user data, and other digital services provided by large tech companies. While DSTs represent a step towards ensuring that digital businesses contribute their fair share of taxes, they have also sparked controversy and debate over their potential to cause trade disputes and market distortions (consilium.europa.eu, 2024).

Next to the DSTs, advanced tools, including artificial intelligence and big data analytics, are being deployed to improve the efficiency of tax collection and combat evasion. These technologies can analyse vast amounts of transaction data to identify patterns indicative of non-compliance. By digitalizing tax administration, authorities can streamline processes, reduce administrative burdens, and encourage voluntary compliance. The use of new taxes and tools is not only about increasing revenue but also about fostering a culture of compliance (Erdős, 2020, pp. 11–12). By creating a more transparent tax landscape, authorities can incentivize businesses to comply with tax obligations and discourage evasion. This approach promotes economic formalization, as companies recognize the benefits of operating within the legal framework, such as access to financial services and legal protections (Avi-Yonah & Clausing, 2019, p. 840).

Certainly, technological advancements are not exclusive to governmental use; they are also within reach of private entities to varying extents. The same tools that enable governments to gather, transmit, and analyse information are equally available to individuals and businesses. Consequently, these technologies bolster the capacity of private parties to conceal their income and assets from tax authorities. Technological developments facilitate profit shifting through transfer pricing strategies, the strategic placement of intangible assets in low-tax areas, the manipulation of internal group debt, treaty shopping, corporate restructuring to exploit tax benefits, and deferring tax liabilities. Additionally, technology simplifies the involvement of individuals and companies in global supply chains, which can be used both to channel profits into tax havens and to participate in tax evasion through mechanisms like money laundering (Alm, 2021, pp. 322–323).

The statistics on global tax evasion (Alstadsæter, Johannesen & Zucman, 2018, pp. 89-100) underscore the extent to which technological advancements have been leveraged by private individuals and firms to evade taxes. These figures highlight the growing challenge for tax administrations worldwide as they attempt to keep pace with the sophisticated methods employed to conceal income and assets. Multinational corporations and ultra-wealthy individuals annually precipitate a global revenue shortfall of $480 billion (Oxfam, 2022) for national treasuries through the minimization of tax liabilities by resorting to tax havens, offshore stratagems, and various other methods of tax avoidance (taxobservatory.eu, 2021). This figure can also be articulated as a critique of local solutions; therefore, in the subsequent chapter, I will examine a global approach initiated by the OECD, which currently constitutes one of the most pertinent subjects within the international tax law milieu.

3. OECD BEPS 2.0

In the context of the blooming digital economy, the nature of global commerce and business has transcended traditional boundaries, creating a pressing need for an international approach to the tax challenges that have arisen as a consequence. The digital economy's global reach has rendered national tax systems inadequate in isolation, calling for a collaborative response to ensure tax fairness and integrity across borders. Recognizing this imperative, the OECD has spearheaded the Base Erosion and Profit

Shifting (BEPS) 2.0 project, a pivotal initiative aimed at reshaping the international tax framework to better align with the realities of a digitalized world (oecd.org, 2024). The OECD's two-pillar project addresses the fair taxation of the digital economy and large enterprises. In response to global tax avoidance, the international community recognized in the 2010s that the fair taxation of digital and large businesses is a global issue that can only be resolved through broad collaboration. To address this issue, the OECD proposed a two-pillar solution: the first pillar aims to ensure the fair taxation of large enterprises with excess profits by proposing a reallocation of corporate tax bases based on the location of users, while the second pillar targets the introduction of a global minimum corporate tax (known as the "GloBe" proposal). The BEPS 2.0 project is a comprehensive endeavour to combat the strategies employed by multinational enterprises that seek to minimize their tax liabilities through base erosion and profit shifting. These tactics often involve exploiting gaps and mismatches in tax rules to shift profits to low or no-tax jurisdictions, thereby eroding the tax base of the countries where the actual economic activity takes place. The project puts forth a robust set of rules and recommendations that strive to ensure that profits are taxed in the jurisdictions where substantial economic activities are conducted and where value is genuinely created.

BEPS 2.0 seeks to redefine the allocation of taxing rights in a manner that reflects the digitalization of the economy. This includes revising the nexus rules to capture the digital presence of businesses and allocating taxing rights that may not be tied to a physical presence, thereby acknowledging the value creation that occurs through digital engagement and user participation in different markets. The project represents a concerted effort to harmonize tax policies on a global scale and to prevent the fragmentation of the international tax system. It embodies the collective will to establish a more coherent, transparent, and equitable tax regime that can withstand the challenges posed by an increasingly digital and interconnected global economy (oecd.org, 2024).

The BEPS 2.0 project is not just a theoretical exercise; it is a significant development in the international tax arena, one that has the potential to fundamentally alter the way multinational enterprises are taxed. By providing a framework for international cooperation, the project aims to prevent the rise of trade tensions and economic distortions that could result from unilateral tax measures.

However, the path to implementing the BEPS 2.0 recommendations is fraught with complexities. Achieving consensus among a diverse array of countries, each with its own unique interests and tax policies is a formidable challenge. There are also concerns regarding the potential impact on smaller economies and the capacity of developing countries to effectively participate in and benefit from the BEPS process. These countries may require additional support to implement the complex rules and to safeguard their tax bases. In the European Union, a directive proposal was prepared based on the OECD Model Rules, which was intensively negotiated throughout 2022. Following the lifting of Hungary's veto on the global minimum tax directive in December 2022, the Council Directive (EU) 2022/2023 of 14 December 2022 on ensuring a global minimum level of taxation for multinational enterprise groups and large-scale domestic enterprise groups in the Union (the "GloBE Directive") was adopted. Member States were required

to implement the GloBE Directive by 31 December 2023. The majority of the global minimum tax rules must be applied by all Member States, including Hungary, for financial years beginning from 31 December 2023, with some rules only applicable for financial years starting from 31 December 2024.

Non-EU European countries, as the United Kingdom and Switzerland have implemented the rules so far. The United Kingdom will apply the global minimum tax rules from 2024. Switzerland initially planned a full implementation in 2024; however, in December 2023, it decided to introduce only the domestic top-up tax (QDMTT) from 2024, with the other rules to be applied from a currently unknown future date. This decision was justified by the delay in implementation by significant third countries—USA, China, Brazil, India. Among other third countries, Japan will apply the income inclusion rule (IIR) for financial years following 1 April 2024, but is postponing the introduction of the domestic top-up tax (QDMTT) and the undertaxed payments rule (UTPR) to an uncertain future date. Canada and Australia will also apply global minimum tax rules from 2024, but information on the rules is limited. The USA, China, Brazil, and India will not introduce global minimum tax rules from 2024, and it is uncertain when they might do so.

Among African nations, Nigeria, Zimbabwe, South Africa, and Mauritius have previously indicated that they are considering the possibility of implementation; however, a general tendency to wait and see prevails across the continent. These countries operate extensive tax incentive schemes for multinational corporations, and thus the introduction of a global minimum tax—regardless of progress made by other countries—may only become timely after a prior transformation of the tax incentive system, whose effects could be neutralized by the global minimum tax. A similar mindset is observed in developing Asian countries. Among Asian nations, South Korea and Vietnam have adopted global minimum tax rules to be applied from 2024, with Thailand planning to do so from 2025, followed by Singapore, Hong Kong, and Malaysia. The rest of the Asian countries, much like the South American continent, maintain a position of expectancy (ado.hu, 2024).

The implementation of global initiatives is fraught with complex challenges, as the distinct political, economic, and cultural landscapes of various countries can significantly influence the successful execution of these projects. This is particularly true for projects under the auspices of the OECD, where substantial disparities exist among member states in these factors. With the BEPS projects, we focus on how to eliminate the tax loopholes exploited by multinational corporations, and lay the foundations for a new international tax system in corporate taxation, dealing with the challenges of the digital economy. However, there is a growing debate that these initiatives do not address the tax avoidance practices of individuals at all (Beretta, 2019, pp. 68–69).

4. CONCLUSIONS

In conclusion, this research has illuminated the intricate dynamics of taxation within the digital economy, highlighting the urgent need for innovative tax measures and advanced tools to modernize tax administration and foster economic transparency. The study has underscored the significance of the OECD's BEPS 2.0 project as a cornerstone

in the development of a coordinated global response to the tax challenges presented by digitalization. As nations grapple with the implementation of these initiatives, the journey towards a more equitable and effective international tax system continues, with the hope of bridging the gaps that allow for tax evasion and ensuring that the digital economy contributes its fair share to public coffers. The findings of this research serve as a clarion call for ongoing collaboration and adaptation in the face of an ever-evolving economic landscape.

LIST OF REFERENCES

Adó.hu: Dióhéjban a globális minimumadóról 2024. Available at: https://ado.hu/ado/diohejban-a-globalis-minimumadorol/ (12. 4. 2024).

Alm, J. 2021. Tax evasion, technology, and inequality. *Economics of Governance*, 22, pp. 321-343. https://doi.org/10.1007/s10101-021-00247-w

Allingham, M. G. & Sandmo, A. 1972. Income tax evasion: A theoretical analysis. *Journal of Public Economics*, 1(3/4), pp. 323-338. https://doi.org/10.1016/0047-2727(72)90010-2

Alstadsæter, A., Johannesen, N. & Zucman, G. 2019. Tax evasion and inequality. *American Economic Review,* 9(6), pp. 2073-2103. https://doi.org/10.1257/aer.20172043

Alstadsæter, A., Johannesen, N. & Zucman, G. 2018. Who owns the wealth in tax havens? Macro evidence and implications for global inequality. *Journal of Public Economics*, 162, pp. 89-100. https://doi.org/10.1016/j.jpubeco.2018.01.008

Avi-Yonah, R. S. & Clausing, K. A. 2019. Toward a 21st-century international tax regime. *Tax Notes Int,* 26, pp. 839-849.

Beretta, G. 2019. 'Fixing' The Social Contract: A Blueprint for Individual Tax Reform. *Annals FLB. – Belgrade Law Review,* 4, pp. 68-115. https://doi.org/10.5937/AnaliPFB1904068B

Consilium.europa.eu. Policies: Digital Taxation. Available at: https://www.consilium.europa.eu/en/policies/digital-taxation/ (8. 7. 2024).

Erdős, É. 2020. A Digitális Gazdaság Adóztatásának Trendjei. *Iustum Aequum Salutare*, 16(4), pp. 7-18.

Gupta, S. *et al.* (eds.) 2017. *Digital revolutions in public finance.* Washington D.C: International Monetary Fund.

Khlif, H. & Achek, I. 2015. The determinants of tax evasion: A literature review. *International Journal of Law and Management,* 57(5), pp. 486-497. https://doi.org/10.1108/IJLMA-03-2014-0027

OECD. 2013. Addressing base erosion and profit shifting. Available at: https://www.oecd.org/en/publications/2013/02/addressing-base-erosion-and-profit-shifting_g1g2a9bc.html (14. 7. 2024).

OECD. 2024. Base erosion and profit shifting (BEPS). Available at: https://www.oecd.org/en/topics/base-erosion-and-profit-shifting-beps.html (14. 7. 2024).

Országgyűlés Hivatala. 2021. A Digitális Szektor Adóztatása. Available at: https://www.parlament.hu/documents/10181/39233854/Infojegyzet_2021_53_a_digitalis_szektor_adoztatasa.pdf/6ce30202-70cc-dc20aca8e0ff72fc587d?t=1623391933007 (1. 7. 2024).

Oxfam. 2022. Carbon Billionaires: The investment emissions of the world's richest people. Available at: https://policy-practice.oxfam.org/resources/carbon-billionaires-the-investment-emissions-of-the-worlds-richest-people-621446/ (9. 6. 2024).

Perez Lopez, C., Delgado Rodrıguez, M. J. & de Lucas Santos, S. 2019. Tax fraud detection through neural networks: An application using a sample of personal income taxpayers. *Future Internet,* 11(4), pp. 1-13. https://doi.org/10.3390/fi11040086

Saez, E. & Zucman, G. 2019. *The triumph of injustice: how the rich dodge taxes and how to make them pay.* New York: W.W. Norton & Company.

Stiglitz, J. E. 1969. The effects of income, wealth and capital gains taxation on risk-taking. *Quarterly Journal of Economics,* 83, pp. 263-283. https://doi.org/10.2307/1883083

Slemrod, J. 2006. Taxation and „big brother": information, personalization, and privacy in 21st century tax policy. *Fiscal Stud*, 27(1), pp. 1-15. https://doi.org/10.1111/j.1475-5890.2006.00025.x

Slemrod, J. 2019. Tax compliance and enforcement. *Journal Econ Lit*, 57(4), pp. 904-954. https://doi.org/10.1257/jel.20181437

Slemrod, J. & Weber, C. 2012. Evidence of the invisible: toward a credibility revolution in the empirical analysis of tax evasion and the informal economy. *Int Tax Public Finance*, 19(1), pp. 25-53. https://doi.org/10.1007/s10797-011-9181-0

Szilovics, Cs. 2003. *Csalás és jogkövetés az adójogban.* Budapest: Gondolat Kiadó.

Szilovics, Cs. 2024. Az adójog. In: Herich, Gy. (ed.), *Adó magyarázatok.* Budapest: Penta Unió Oktatási Centrum, pp. 5-20.

Taxobservatory.eu. 2021. The State of Tax Justice. Available at: https://www.taxobservatory.eu/repository/the-state-of-tax-justice-2021/#:~:text=TJN%20estimates%20that%20the%20world%20is%20losing%20over,responsible%20for%20facilitating%2099.4%25%20of%20corporate%20tax%20losses. (4. 7. 2024).

Unger, B. & van der Linde, D. (eds) 2015. *Research handbook on money laundering.* Cheltenham: Edward Elgar Publishing Inc.

Varga, E. 2020. A digitális vállalkozások adóztatásának kihívásai. Available at: 14_Varga_Erzsebet_A_digitalis_vallalkozasok_adoztatasanak_kihivasai.pdf (mtak.hu) (6. 7. 2024).

Yamen, A. & Coskun, A. & Mersni, H. 2023. Digitalization and tax evasion: the moderation effect of corruption. *Economic Research-Ekonomska Istrazivanja,* 36(2), pp. 1-24. https://doi.org/10.1080/1331677X.2022.2142634

Zucman, G. 2013. The missing wealth of nations: Are Europe and the US net debtors or net creditors? *The Quarterly Journal Economics*, 128(3), pp. 1321-1364. https://doi.org/10.1093/qje/qjt012

Zucman, G. 2015. *The hidden wealth of nations.* Chicago: University of Chicago Press. https://doi.org/10.7208/chicago/9780226245560.001.0001

UDC: 004.7:34 DOI: 10.56461/iup_rlrc.2024.5.ch17

Martin KÁLMÁN*
Faculty of Law, University of Pécs, Hungary

MOSAICS FROM THE LEGAL REGULATION OF BLOCKCHAIN TECHNOLOGY

The use of distributed ledger technology could bring breakthroughs in many sectors beyond the popular cryptocurrencies, such as Bitcoin, which remain the most exciting new developments in blockchain technology. As the decade-long euphoria surrounding the explosion of cryptocurrencies subsides, the underlying technology may gain prominence and find applications in various fields in the near future. Governments have recognised that the benefits of blockchain can be harnessed in the public sector, provided there is a suitable regulatory environment and safeguards. The growing number of governments using the technology to modernise their public services is clear evidence of this recognition. Blockchain technology can improve transaction efficiency, reduce costs, democratise data systems and increase trust. The use of blockchain technology can potentially reduce corruption and increase resilience to cyber-attacks. However, there are still many challenges to overcome in integrating distributed ledgers and fully realizing the transformative power of blockchain. The purpose of this research is to provide a snapshot of the legal issues and improvements of blockchain technology, identify legal opportunities, and draw some useful conclusions for both theory and practice by highlighting some of the main characteristics of the regulative landscape worldwide.

Keywords: innovation, cryptocurrency, blockchain, regulation, challenges.

1. INTRODUCTION

In recent years, the dazzling rise of cryptocurrencies like Bitcoin has captivated the world's attention, showcasing the potential of distributed ledger technology (DLT) to revolutionise financial transactions. However, as the initial fervour for digital currencies begins to stabilize, it is becoming increasingly clear that the true potential of blockchain technology extends far beyond the realm of cryptocurrency. This technology, characterized by its decentralized and immutable record-keeping capabilities, is poised to bring about

* LLM, ORCID: 009-0006-7459-1271, e-mail: *martin.kalmanka@gmail.com*

significant advancements across a multitude of sectors. The blockchain technology behind crypto-assets offers a wide range of untapped opportunities, from improving public administration, healthcare, simplifying and speeding up payment services, redefining public procurement (Glavanits, 2022) to the introduction of digital money (Bujtár, 2022). One of the most compelling advantages of blockchain is its potential to mitigate corruption and bolster cybersecurity, making public services more resilient and transparent. With the right regulatory frameworks and safeguards in place, blockchain stands to streamline processes, cut down on costs, democratize access to data, and bolster trust among stakeholders. Nevertheless, the journey towards integrating distributed ledgers into the fabric of public administration is fraught with challenges. It is imperative to navigate these obstacles carefully to unlock the transformative power of blockchain. At the same time, innovation also has adverse effects, as consumer protection, investor protection, the fight against money laundering (Gáspár, 2022) and tax fraud (Szívós, 2022), and data security are all issues that are under review in order to ensure that the legislator discourages illegal behaviour.

As governments worldwide begin to recognize the numerous advantages blockchain offers, there is an increasing trend toward adopting this technology to improve and modernize government functions, they begun to face different regulative challenges. Due to their different economic, social and cultural characteristics, some countries have a very advanced regulatory environment, such as Switzerland, Malta, and Estonia (Alper, 2023), but on the other side of the scale, there are countries such as China, India, Russia or Mexico where economic transactions involving crypto-assets are almost completely prohibited (Kecskés & Bujtár, 2019; Gupta, 2021). Some nations, including the United States of America, have not yet come to a decision in their public policy thinking, or even in their own domestic law, to vote for or against the technology. In Hungary, the legislator seemed oblivious to blockchain technology until the amendment of the personal income tax law in January 2022, but the new legal provisions lay the foundations for a crypto-friendly environment. Furthermore, the application of Markets in Crypto-Assets Regulation (MiCA) rules as an EU member state.

This study aims to present a snapshot of the legal regulation opportunities and challenges of blockchain technology. The objectives of this research are multifaceted: to present the most common issues regarding the adoption and legal acceptance of the technology, to mention some of the liberal and some of the conservative approaches, highlighting their effective way using the public and private sectors. Furthermore, to underline the European Union's role in driving the future of legal regulation and finally to unveil the Hungarian legal measures from a country-specific point of view. The structure of the paper follows the abovementioned objectives.

2. BARRIERS TO ADOPTION AND EMERGING ISSUES

Cryptocurrency regulation is a complex task, and there are many challenges associated with it. Different jurisdictions have different definitions and approaches to crypto regulation, which can make it difficult to create a unified framework. Barriers to cryptocurrency adoption include jurisdictional impacts because different countries have different laws and regulations regarding cryptocurrencies, decentralized finance, and

blockchain technology. This can create confusion and inconsistency for users and companies operating in multiple jurisdictions, taking cross-border economic activities. Furthermore, the regulatory landscape is constantly changing. This can create uncertainty and make it tough for companies and individuals to comply with the law. With regards to consumer protection, there is currently no uniform law. The lack of norms complicates the protection of consumers from scams and fraud, especially in the cyberspace (Gáspár, 2021). One of the biggest barriers is that there is currently no clear general definition of what qualifies as a cryptocurrency, decentralized asset, or security. It is worth mentioning that tax treatment of cryptocurrencies, decentralized finance and blockchain technology is still being debated in many jurisdictions. It is also difficult for users and companies to know how to properly report their income and calculate their taxes (Szívós, 2022). The poor level of understanding of crypto-assets causes many policymakers to have no or minimal technical knowledge to effectively regulate crypto assets, which puts a huge barrier before effective regulations.

In their study from 2018, Maria Demertzis and Guntram B. Wolff highlighted six key public policy issues posed by crypto-asset developments. What is the potential of crypto-assets in developed financial systems? How best to combat illegal activities such as money laundering and terrorist financing? How to protect consumers and investors? What about financial stability? How can crypto-assets be taxed? How can blockchain applications be integrated into the existing regulatory framework? (Demertzis, Merler & Wolff, 2018) These questions have not been answered yet, or have only been partially answered, in the few years since the study was written. This means that the regulation of crypto-assets has gone from full support to outright prohibition in some jurisdictions, such as China and India, but the development of a comprehensive legal environment has not yet been achieved in any jurisdiction (Kecskés & Bujtár, 2019), with the exception of Malta (Bujtár, 2018) and partially Estonia.

3. THE EFFECTIVE USE OF BLOCKCHAIN – EXAMPLES FROM THE PUBLIC AND PRIVATE SECTOR

The state and blockchain technology can intersect at numerous points. Public interest primarily focuses on the role of innovation within the financial sector, along with the consumer and investor protection challenges it presents. However, the application of blockchain has expanded to encompass a much broader scope and continues to grow (Shang & Price, 2019; Carvalho, 2019). One of the most prominent areas of sustainability efforts is the implementation of smart city projects. Smart cities utilize information technology and data to integrate and manage physical, social, and business infrastructures, streamlining services provided to residents while ensuring the efficient and optimal use of available resources. By combining innovative solutions such as artificial intelligence, cloud-based services, and blockchain technology—the subject of this discourse—municipalities can offer superior services to citizens and local communities. Blockchain can provide the mechanism for establishing a secure infrastructure that manages these functions. It can offer a secure, interoperable framework that allows all intelligent urban services and functions to operate beyond currently conceived levels. An

integral part of smart city projects is the blockchain-based storage of information related to taxation, registrations, and public services, all of which can be realized through blockchain and smart contract solutions (Henno, 2018; E-estonia, 2024). In the case of smart contracts, we refer to an electronically formed agreement where rights and obligations within the electronic contract automatically come into effect upon the proper sequence of predefined digital transactions—and under certain conditions, the fulfilment of additional terms. An agreement made entirely or partially in electronic form, which can be automated and executed via computer code, may require human input and oversight in some parts and can also be executed using conventional legal methods or a combination thereof (Sánchez, 2019; Thio-ac *et al.,* 2019).

4. COMPREHENSIVE APPROACHES – MARKETS IN CRYPTO-ASSETS DIRECTIVE

As in many other economic and financial areas, The Organisation for Economic Co-operation and Development (OECD) is calling for international action regarding blockchain technology and the crypto market. As a consequence, OECD recently approved the Crypto-Asset Reporting Framework (CARF) in August 2022 (see OECD, 2022). This new framework requires standardized reporting of tax information on crypto-asset transactions for automatic exchange of information. The CARF defines the relevant crypto-assets to be covered, as well as the intermediaries and service providers subject to reporting. The CARF also includes the latest developments in the Financial Action Task Force's Global Anti-Money Laundering Standards. Similar to the Common Reporting Standard (CRS), due diligence procedures require the identification of individual and legal entity clients and control persons. Additionally, the OECD approved amendments to the CRS in August 2022 to include electronic money products and central bank digital currencies (CBDCs) within its scope.

The Bank for International Settlements (BIS) has established an Innovation Hub as part of its global cooperation efforts, which involves collaboration with various financial institutions to explore new technological tools. The Innovation Hub is pioneering experiments on shared ledger technology platforms, exploring cross-border digital money and wholesale CBDC.

In response to most of the questions posed in the previous chapter, the European Union provided a complex and detailed answer. Back on 30 June 2022, the European Parliament and Council reached a temporary agreement on the Markets in Crypto-Assets (MiCA) regulation, which is a complex and comprehensive regulatory framework designed to regulate the entire crypto ecosystem. The formal adoption of the regulation happened on 16 May 2023 as the final step in the legislative process and entered into force 20 days after its publication in the Official Journal.

MiCA, along with the Digital Operational Resilience Act (DORA) and the DLT pilot regime, are part of the EU's comprehensive package of digital financial legislation aimed at supporting the digital transition and making Europe a global digital player. The aim of MiCA was to establish a regulatory framework for the crypto-asset market that supports

innovation and maximizes the opportunities offered by crypto-assets while preserving financial stability and protecting investors. With this agreement, the EU reaffirms that digital finance remains a top priority on its agenda and becomes the first significant jurisdiction to regulate crypto-assets.

MiCA covers all crypto assets that are currently not subject to existing financial services regulations. These range from utility tokens that provide access to services, to stablecoins that aim to maintain a stable value by referencing the value of multiple fiat currencies, commodity exchange products, or cryptocurrencies, and to general crypto-assets such as Bitcoin. MiCA categorizes crypto-assets into four broad categories: asset-referenced tokens that seek to maintain a stable value, e-money tokens that exclusively reference the value of a single fiat currency, utility tokens that provide access to the issuer's product or service, and general crypto-assets. User tokens that provide access to a specific product or service are generally exempt from the MiCA's whitepaper requirements (Fintechzone, 2023).

On the way to reach legal clarity, the European Securities and Markets Authority (ESMA) more precisely defined the conditions under which crypto-assets qualify as financial instruments, and therefore fall under the existing financial services regulation, or conversely, in this case, these other cryptos would fall under the scope of MiCA.

Crypto-asset issuers obliged to prepare and publish a crypto-asset information document that contains all relevant information regarding the specific crypto-asset. The members of the issuer's governing body must comply with the fairness requirements, and it will be prohibited for crypto-asset issuers to engage in misleading market communication.

To avoid undue administrative burdens, competent national authorities (NCAs) generally do not approve the whitepaper before its publication, although there are exceptions, such as for stablecoins. The issuer still needs to report the whitepaper to the national competent authority, providing an explanation as to why the crypto-asset does not qualify as a financial instrument under Annex I, Section C of Directive 2014/65/EU (MiFID II) or as another category outside the scope of MiCA, such as e-money or a deposit.

MiCA introduces several exemptions from the obligation to prepare and publish whitepapers, for example, in the case of crypto-assets that are offered for free, are automatically generated through mining activities, or are offered to a small number of investors or exclusively to qualified investors (Deloitte, 2022).

5. HUNGARIAN MEASURES

According to some estimates, the crypto sector operating in Hungary is worth several hundred billion forints, which means that without adequate regulation, the central budget can expect significant revenue losses from money laundering, fraud or tax evasion. However, until 1 January 2022, Hungarian lawmakers did not address the hype surrounding innovation, and as a result, they did not create any definition, categorization, or detailed guidelines in any of the most important areas, such as investor protection, consumer protection, taxation, and criminal law. Regarding the definition, the previous statement of the National Tax

and Customs Administration stated that bitcoin represents an unconditional payment promise without expiration or term, which can only be demonstrated as a claim, has no interest, but if it is converted to money or used, it will have a return, which can be a profit or loss. In practice, the tax authority's description has been generalized to other altcoins for several years (Szívós, 2021).

As part of the Digital Welfare Program, the FinTech strategy released in 2019 outlined important initiatives in terms of digitalizing the domestic financial system, and also highlighted the importance of blockchain technology. The document states that the aim is to provide regulatory protection for consumer interests and to reflect the needs of economic stakeholders, while also supporting legal harmonization with the European Union's norms. The authors also consider the use of blockchain technology for enabling smart city functions, as well as for potential use in public administration (Digitális Jólét Nonprofit Kft, 2019).

The amendment to the personal income tax law that came into effect on 1 January 2022, which placed cryptocurrencies into a separate category for tax purposes, is considered a major step forward. They are now treated similarly to income from regulated capital market transactions, which means that the previously high tax burden, which could reach almost 30%, has been significantly reduced by the legislature and private individuals' crypto earnings are subject to a favourable 15% tax rate. This move is likely to make Hungary a more attractive destination for digital nomad crypto investors, and it could also lead to greater economic transparency, as taxpayers are more likely to declare a higher percentage of their cryptocurrency income with this more favourable tax rate.

The author highlights that the personal income tax law has also specifically defined cryptocurrencies. According to the new definition, a "cryptocurrency" is the digital representation of value or rights that can be transferred and stored electronically using shared ledger technology or similar technology. Looking at the rule as a whole, it can be said that crypto assets now include cryptocurrencies or coins, various tokens, including NFTs. In addition, income from the transfer of rights related to other cryptocurrencies, such as an option right, is also considered cryptocurrency income, provided that this right is recorded using shared ledger technology. Practically any right or value recorded on a blockchain qualifies as a cryptocurrency, but it does not necessarily mean that every transaction in which a cryptocurrency changes hands will result in income from a cryptocurrency transaction.

It is important to note that regulatory efforts must continue, not just limited to taxation. The communication published by the National Bank of Hungary this year also projects this image, provided that the MiCA regulation on regulating crypto-assets progresses as planned, strict regulation will be expected in the Hungarian legal environment from mid-2024.

Similarly, the financial law bracket submitted in November 2022, also known as blockchain act, was adopted in December of that year and will come into effect in March of this year. The provisions create the possibility of tokenizing financial instruments, i.e., the appearance of financial instruments in shared ledgers. The National Bank of Hungary, which oversees financial supervision, has been designated to supervise and regulate blockchain applications (Magyarország Kormánya, 2022). The law was created to reflect on the normative handling of technology surrounding crypto-assets and to serve harmonization objectives in line with European Union legislation.

6. CONCLUSION

Ongoing debates about the merits and risks of cryptocurrencies are expected to intensify, particularly in corporate boardrooms where multi-billion-dollar decisions are made. Courts will play a crucial role in shaping blockchain's future, much like legislators. While a wave of compensation lawsuits could erode trust in cryptocurrencies, fair legal outcomes could reassure investors that they may be protected from significant losses. The current unregulated status of crypto-assets has led to numerous legal disputes, indicating a need for tighter and more comprehensive regulation (Morrison Cohen LLP, 2022).

Both the OECD and the European Union, along with the United States, are moving toward stringent regulations in response to the legal challenges posed by crypto-assets. This could signal a shift in the success story of cryptocurrencies as the state recognizes the potential risks to public order and the economy. The author suggests that the European Union and Hungary should foster a regulatory environment that protects consumers while promoting innovation in the cryptocurrency sector. Educating the public and businesses about digital assets is also crucial for building trust in this evolving market. A collaborative regulatory approach is essential for integrating cryptocurrencies into the financial system.

However, some believe that the growing interest of the state marks the end of the success story of cryptocurrencies, as lawmakers become aware of the negative impact and myriad risks on public order, the state budget, and the economy. It will then become clear what the real societal and economic goal and benefit of creating cryptocurrencies were, as it was an important and expensive experiment that transformed financial culture and paved the way for the introduction of digital state or central bank currencies (Szilovics, 2021).

LIST OF REFERENCES

Act CXVII of 1995 on Personal Income Tax with amendments.

Alper, T. 2023. Bis Claims CBDC Interoperability Victory While US Congressman Bids Block Digital USD. Cryptonews. Available at: https://cryptonews.com/news/bis-claims-cbdc-interoperability-victory-while-us-congressman-bids-block-digital-usd/ (6. 1. 2024).

Bujtár, Zs. 2022. Central bank-issued digital currencies and their characteristics in light of security. In: Kőhalmi L. *et al.* (eds.), *Biztonság és jog: Konferenciakötet. Magyarország.* PTE ÁJK Kriminológiai és Büntetés-végrehajtási Jogi Tanszék, pp. 49-61.

Bujtár, Zs. 2018. A kriptovaluták európai és máltai szabályozásának összehasonlítása: A máltai sólyom szárnyalása. *Európai Jog*, 18(5), pp. 6-16.

Carvalho, R. 2019. Blockchain and Public Procurement. *European Journal of Comparative Law and Governance*, 6(2), pp. 187-225. https://doi.org/10.1163/22134514-00602002

Deloitte. 2022. Regulatory News Alert: European legislators have agreed on a landmark law regulating crypto assets: Markets in Crypto-Assets (MiCA) Regulation July 2022. Available at: https://www2.deloitte.com/lu/en/pages/financial-services/articles/european-legislators-agreement-landmark-law-crypto-union-mica-regulation.html (12. 5. 2023).

Demertzis, M., Merler, S. & Wolff, G. 2018. Capital Markets Union and the Fintech Opportunity. *Journal of Financial Regulation*, 10, pp. 1-9. https://doi.org/10.1093/jfr/fjx012

E-Estonia.com. e-land-register. Available at: https://e-estoniax.com/solution/land-registry/ (8. 8. 2024).

Fintechzone. 2023. MNB: szigorú szabályozás vár a ktiptoeszközökre 2024-től. Available at: https://fintechzone.hu/mnb-szigoru-szabalyozas-var-a-kriptoeszkozokre-2024-tol/ (11. 11. 2023).

Digitális Jólét Nonprofit Kft. 2019. Magyarország Fintech Stratégiája - A hazai pénzügyi szektor digitalizációja 2019–2022. Available at: https://digitalisjoletprogram.hu/files/67/01/67018780db39d25c02d4b736abe8d1a1.pdf (13. 5. 2023).

Gáspár, Zs. 2021. Cryptocurrencies & Cybercrimes: The criminal aspects of crypto assets. In: Bujtár Zs. *et al.* (eds.), *Kriptoeszközök világa a jog és a gazdaság szemszögéből: konferenciakötet: 2021. március 19.* Pécs: Pécsi Tudományegyetem Állam- és Jogtudományi Kar, pp. 143-151.

Gáspár, Zs. 2022. Money Laundering and Cryptocurrencies in the Hungarian and EU Regulations. In: Bujtár Zs. *et al.* (eds.), *FINTECH – DEFI – Kripoeszközök Gazdasági és Jogi lehetőségei és kockázatai: Konferenciakötet – Válogatott Tanulmányok. Magyarország.* Pécs: Pécsi Tudományegyetem Állam- és Jogtudományi Kar, pp. 49-58.

Glavanits, J. 2022. Okosszerződések alkalmazási lehetőségei a közbeszerzési jogban. In: Auer Á. (eds.), *Közszerződési jogi koncepciók online kiadás*. Budapest: Akadémiai Kiadó. https://doi.org/10.1556/9789634548492.4

Gupta, R. 2021. *China's CBDC Cross Border Prospects and Challenges.* ICSIN. Available at: https://icsin.org/blogs/2021/08/23/chinas-cbdc-cross-border-prospects-and-challenges/ (3. 4. 2024).

Henno, J. 2018. *NJORD Estonia: Real estate transaction using blockchain technology.* NJORD Law. Available at: https://www.njordlaw.com/njord-estonia-real-estate-transaction-using-block-chain-technology/ (14. 5. 2024).

Kecskés, A. & Bujtár, Zs. 2019. Felvetések a kripto eszközök szabályozása terén. *Controller Info*, 7(2), pp. 49-53.

Magyarország Kormánya. 2022. Törvényjavaslat: A pénzügyi szektort érintő törvények módosításáról. Available at: https://www.parlament.hu/irom42/02029/02029.pdf (23. 7. 2024).

Morrison Cohen LLP. 2022. Morrison Cohen Cryptocurrency Litigation Tracker. Available at: https://www.morrisoncohen.com/news-page?itemid=471 (10. 2. 2023).

OECD. 2022. Crypto asset reporting framework and amendments to the common reporting standard. Available at: https://www.oecd.org/tax/exchange-of-tax-information/crypto-asset-reporting-framework-and-amendments-to-the-common-reporting-standard.htm (12. 7. 2024).

Sánchez, S. N. 2019. The Implementation of Decentralized Ledger Technologies for Public Procurement: Blockchain Based Smart Public Contracts. *European Procurement and Public Private Partnership Law Review*, 3, pp. 180-196. https://doi.org/10.21552/epppl/2019/3/7

Shang, Q. & Price, A. 2019. A blockchain-based land titling project in the Republic of Georgia. *Innovations,* 12(3-4), pp. 73-78. https://doi.org/10.1162/inov_a_00276

Szilovics, Cs. 2021. A kriptovaluták pénzfunkciójáról és gazdasági, társadalmi jelentőségéről. In: Bujtár, Zs. *et al.* (eds.). *Kriptoeszközök világa a jog és gazdaság szemszögéből: Konferenciakötet - Válogatott tanulmányok*. Pécs: Pécsi Tudományegyetem Állam- és Jogtudományi Kar, pp. 26-31.

Szívós, A. 2021. A kriptoeszközök és az adózás. In: Bujtár, Zs. *et al.* (eds.), *Kriptoeszközök világa a jog és gazdaság szemszögéből: Konferenciakötet - Válogatott tanulmányok*. Pécs: Pécsi Tudományegyetem Állam- és Jogtudományi Kar, pp. 12-23.

Szívós, A. 2022. Tax Treatment of Cryptocurrencies. In: Sergey, Y. Y. (ed.), *Proceedings of the 1st Blockchain and Cryptocurrency Conference.* Barcelona: International Frequency Sensor Association (IFSA) Publishing, S. L., pp. 11-14.

Thio-ac, A. *et al*. 2019. Blockchain-based System Evaluation: The Effectiveness of Blockchain on E-Procurement. *International Journal of Advanced Trends in Computer Science and Engineering*, 8(5), pp. 2673-2676. https://doi.org/10.30534/ijatcse/2019/122852019

UDC: 004.78:347.23
336.7:004

DOI: 10.56461/iup_rlrc.2024.5.ch18

Šime JOZIPOVIĆ*
Faculty of Economics, University of Split, Croatia
Marin KERŠIĆ**
Faculty of Law, University of Split, Croatia

SCHOLARLY SYSTEMATIZATION OF LEGAL NORMS: THE CASE OF DIGITAL PAYMENTS AND VIRTUAL ASSETS

Throughout history, legal theory has undergone continuous development. With the growing complexity of modern society, regulatory requirements have been increasing while contractual relationships have grown more sophisticated. Technological progress usually precedes regulation. This is only natural, as law serves to regulate the relationships between legal subjects concerning legal objects. However, this also means that regulation always lags one step behind innovation. Particularly in rapidly developing areas of technology, regulation can become complex, inconsistent and insufficiently balanced. The scholarly systematization of legal norms has become an important mechanism to mitigate such issues. Even more, scholarly systematization of legal norms in new technologies has sparked entire new areas of law. (At least) five reasons to approach legal norms regulating innovation from the perspective of the scholarly systematization of law are: first, the identification of valid legal norms is easier; second, it helps with legal interpretation, especially systematic interpretation; third, it serves to identify and resolve antinomies between norms; fourth, it is the basis for the formation of legal disciplines; and fifth, it impacts the jurisdictions of organs. The aim of this paper is to analyse the impact of the scholarly systematization of legal norms in the fin-tech space, based on recent key innovations including crypto-assets and central bank digital currencies.

Keywords: legal norms, systematization, digital payments, virtual assets.

* PhD, Associate professor, ORCID: 0000-0002-8050-5134, e-mail: *sjozipov@efst.hr*

** PhD, Assistant professor, ORCID: 0000-0002-0964-4625, e-mail: *marin.kersic@pravst.hr*

1. INTRODUCTION

With the growing complexity of modern society, regulatory requirements have been increasing while contractual relationships have grown more sophisticated (Bennett Moses, 2007). Technological progress usually precedes regulation (Visković, 2006, p. 235). Examples of this can be found in numerous cases of the industrial revolution that opened entirely new fields of regulation in areas like transportation, employee safety, social security etc. More recent examples include the rise of the internet and later the switch to smartphones which led to a fast-paced evolution in various segments of contract law and intellectual property law. Innovation preceding regulation is only natural. Law serves to regulate the relationships between legal subjects concerning legal objects. However, this relationship also means that regulation always lags one step behind innovation. Particularly in rapidly developing areas of technology, regulation can become complex, inconsistent and insufficiently balanced.

The so-called scholarly systematization of legal norms has become an important mechanism to mitigate such issues. Even more, scholarly systematization of legal norms in new technologies has sparked entire new areas of law. For example, the innovations in transportation technologies and the increasing importance of air transportation were the basis for the establishment of aerospace law as a separate field, while the increasing importance of mobile phones introduced services like mobile banking and mobile payment systems which are the foundation for digital payment law. In legal theory there can be identified (at least) five reasons to approach legal norms regulating innovation from the perspective of the scholarly systematization of law: first, the identification of valid legal norms is easier; second, it helps with legal interpretation, especially systematic interpretation; third, it serves to identify and resolve antinomies between norms; fourth, it is the basis for the formation of legal disciplines; and fifth, it impacts the jurisdictions of organs (Visković, 2006, pp. 268-269; see also: Aarnio, 2011, pp. 177-184). The notion of scholarly systematization of legal norms can be contrasted with the notion of hierarchical systematization of legal norms. While the first one is the product of the work of legal scholars (or legal scientists, so it can also be called scientific systematization of legal norms), the second one is the product of the legal system, i.e., the hierarchical relations between normative acts that contain respective norms (Visković, 2006, pp. 268-269). We opted for the term "scholarly" instead of "scientific" since it is a more faithful translation of the original term, even though scientific systematization of legal norms could also be used without any consequences for the idea of the paper.

This paper analyses the impact of the scholarly systematization of legal norms in the fin-tech space, based on recent key innovations including crypto-assets and central bank digital currencies. This space has been chosen due to its extremely rapid development and a strong focus on innovation. Especially innovative financial technology and crypto assets attract early adopters and tech-savvy individuals and thus form a functional ecosystem long before valid regulation can be established. The aim of this paper is to analyse two separate cases of innovation, namely the emergence of crypto-assets and the subsequent attempts to regulate it as well as the plans to introduce CBDCs – Central

Bank Digital Currencies. The comparison is chosen as in both cases innovative financial technology is compared, but with crypto assets, the creation of the technology preceded any regulation, while CBDCs are a public project and thus regulation goes hand in hand with the development of the technology. Based on this comparison, the five previously established benefits of scholarly systematization are analysed in order to determine their relevance in rapidly changing sectors, led by private or public initiatives.

In order to achieve the aim of the paper, this paper is divided into four parts. After this introductory section, Part 2 describes the development and evolution of crypto assets and the attempts to regulate them in the EU. Part 3 focuses on the introduction of CBDCs and the attempts to introduce them together with the respective regulations in the Eurozone. Part 4 focuses on the role of systematization and provides conclusions concerning the potential benefits of legal classification in rapidly developing areas of technology.

2. CRYPTO ASSETS

Crypto assets have increased in popularity in recent years, due to their numerous technological benefits including increased speed, efficiency and transparency (Çağlayan Aksoy, 2023, p. 185). The rise of crypto assets was sparked by the creation of Bitcoin, the first decentralized digital currency (Nakamoto, 2008). Bitcoin works on a decentralized ledger based on a proof of work authentication of transactions. This means that multiple participants (so-called crypto miners) attempt to solve a complex mathematical equation which requires significant processing power. Due to the fact that it is uncertain which miner will solve the equation, and the significant investment of resources, it is unlikely that the authenticator will provide incorrect feedback on a transaction. Thus, the system is built in a manner where transactions between various participants do not rely on the trust of any third party but are executed between pseudonymous participants through authenticators that are previously unknown (Jozipović, Perkušić & Ilievski, 2020, p. 3). As one can expect, this creates a fully decentralized system in which traditional legal concepts like rights and obligations, property, possession etc. are challenged (Mandjee, 2015, p. 165).

2.1. The Status of Crypto Assets from a Theoretical Point of View

Academia attempted very early to determine the legal status of crypto assets. The first category of crypto assets was so-called cryptocurrency like Bitcoin. Numerous academic papers attempted to classify cryptocurrencies in general as things, property, units of accounting, rights etc. However, it proved difficult to exactly identify their status, especially as data usually is not treated as property or right in general, but only under specific circumstances defined by law (Zilioli, 2020, p. 252). So, for example, for something to be considered a right, this right of one person must be related to the obligation of one or more other persons. In a fully decentralized system, however, it is difficult to identify who would bear these obligations. Furthermore, in cases of cyber-crime it has been difficult to categorize cryptocurrencies, as they do not have a physical form

in order to be considered a potential object of theft, but simultaneously also do not fulfil the requirements to be considered a specifically protected right like intellectual property (Zilioli, 2020, p. 253). The advantages of the scholarly systematization of law through the further development of the information, communication and technology (ICT) law can be seen here, since the object that is or that will be regulated by the law (in this case, crypto assets) does not clearly fall under the scope of the "traditional" branches of law.

2.2. The Role of Tax Law in Determining the Status of Crypto Assets

A breakthrough in the definition of cryptocurrencies was achieved at the moment, at which they were considered from a tax law perspective. Tax law is highly relevant for the functioning of any modern state. In order to levy taxes, it is not only a technical necessity but, in many cases, a constitutional requirement to exactly define all relevant requirements for taxation, especially what makes a taxable event. Thus, tax law will often be amongst the first fields of law that will be faced with novel concepts and issues. This comes as no surprise, since tax law is an exemplary case of public law and the coercive force of the state, placing the addressees of its norms in a subordinated position (Visković, 2006, p. 286).

However, tax law usually relies on other areas of law for the definition of key terms. Tax law-related issues thus in particular require the exact identification of the right area of law and applicable norms. This has once more been proven in the case of crypto assets-related taxation. Many governments like those of the USA (IRS notice) or the UK (UK-policy brief) had to address crypto assets from a tax standpoint. In addition to this, administrative authorities and courts were faced with cases involving crypto assets (Jozipović, Perkušić & Ilievski, 2021, p. 6; Mandjee, 2015). In an early decision of the European Court of Justice, it was made clear that cryptocurrencies cannot be considered tangible property (Skatteverket/Hedqvist). However, due to a lack of civil law harmonization in the EU in this area, there has not been one legal norm based on which a unified understanding of cryptocurrencies or crypto assets could be built. Thus, with the rise of the popularity of crypto assets, legislators had to create specific and adequate regulations for them (Wronka, 2024, p. 4). Further development of "information, communication and technology (ICT) law" as a new and emerging branch of law would help mitigate the issues regarding cryptocurrencies – in particular, the problem of identification of relevant legal norms, their interpretation and the resolution of antinomies between them. Antinomies between legal norms are more likely to arise in a more complex legal system, such as the EU one, because the rapid technological advancement pressures both national (member-state) and supranational legislative bodies to legally regulate social relations arising from new technological advancements.

It can be seen from the previous paragraph that the legal treatment of crypto assets was primarily determined by tax law. Here, the scholarly systematization of law is not only relevant first of the aspects mentioned (identification of legal norms) but even more: in the case of crypto assets, it *established* fundamental legal norms which legally defined a new technological advancement.

2.3. Crypto Asset Regulation

An important step in crypto asset regulation came with the implementation of new anti-money laundering (AML) standards when the term "virtual currency" was defined for AML purposes and the scope of financial service providers was widened significantly. Due to insufficient regulation in the crypto-asset space and the decentralized nature of crypto-assets, they were increasingly used as vehicles for illegal activities like fraud or money laundering (Jozipović, Perkušić & Ilievski, 2020, pp. 11, 16; Trautman, 2018, p. 467). Thus, the EU implemented new standards in order to mandate service providers in this space to ensure conformance with reporting and controlling standards (AMLD 5). Other legal sources like MiFID II, which regulates financial instruments only partially cover crypto assets to the extent that they overlap with existing financial instruments (Jozipović, Perkušić & Gadžo, 2022). The Anti-Money laundering efforts of the EU show that even very urgent matters like the prevention of certain criminal activities will take time to be regulated. Even if this regulation is introduced faster than more general regulation on an issue, it will still lag significantly behind the introduction of the technology.

Only after a long period of time in which existing national and European regulations were not harmonized in this field, did the EU introduce the Markets in Cryptoassets Regulation (MiCAR). The MiCAR is a key segment in the broader block-chain strategy of the EU which includes multiple aspects from increasing the interoperability of technologies and creating an open innovation environment (Perkušić, Jozipović & Piplica, 2020, p. 371). MiCAR was aimed at increasing legal certainty and finally giving clarity over numerous open issues concerning the categorization and treatment of crypto assets (van der Linden & Shirazi, 2023, p. 21). It defined key categories of crypto-assets like stablecoins, cryptocurrencies and crypto-tokens, and established a partial framework for crypto assets. However, again the legislative process to establish MiCAR has shown the inefficiencies in legislation in rapidly developing environments. So-called non-fungible tokens (NFT) emerged as a new category of crypto assets. These tokens were different from existing crypto assets as each singular token was uniquely identifiable and thus able to serve as proof of ownership of certain rights or privileges (Takahashi, 2022, p. 340). The legislative procedure has not taken this category into account and during the legislative process, it was questioned if the MiCAR should be postponed in order to include this category of crypto asset as well. In the end, it was decided to not include NFTs into MiCAR, due to the additional delay this would cause. The first bitcoin was mined in 2008. MiCAR entered into force in 2023, about 15 years later, and it still covers only certain aspects of the crypto-asset space (MiCAR). This example shows, how difficult it is for legislators to keep up with innovation. It can be argued that the lack of development in information, communication and technology (ICT) law, resulting from the complexity of crypto assets, contributed to legislation falling behind and not catching up with technological development. The need for interdisciplinary research can be seen here since ICT law is arguably among the areas of law which require the most non-legal input and knowledge.

3. CBDCs

As has been shown above, crypto assets are an example of rapid innovation within the private sector that required regulators and legislators to act in order to regulate an entirely new space. Due to the fact that the technology preceded any attempts of regulation, regulators were significantly lagging behind, and it took a long time to start regulating crypto assets on an EU level. Within this timeframe, the legal status of crypto assets was mostly derived from case law and legal theory which used analogies and attempts to identify the relevant legal norms.

Central Bank Digital Currencies (CBDC) are similar to crypto assets in that they are based on innovative financial technology and have the potential to strongly influence consumer behaviour and the market for financial services. However, in contrast to crypto assets which are advanced through private and often decentralized initiatives, CBDCs are centralized public projects spearheaded by national or supranational central banks. For example, one of the most advanced CBDC projects - the digital yuan project is entirely controlled by the People's Bank of China (Yuan – progress report). In the Eurozone, the ECB is currently working on the possible implementation of a digital euro. In both cases, the CBDC involves numerous innovations and various cutting-edge financial technologies. However, CBDCs are created in order to become legal tender and thus require upfront regulation, in contrast to private projects like crypto assets which, as has been shown above have to be regulated ex-post. In the following text, we present how the processes of innovation and regulation of CBDC-related technologies diverge from those related to crypto-assets. Based on this analysis, we will then in the next chapter analyse how the different benefits of systematization affected regulation, legal certainty and efficiency of the legal system.

3.1. CBDCs and Regulation

In order to understand CBDCs, first it is essential to understand the difference between a means of payment and legal tender. The modern view of legal tender is that this term describes a means of payment that under (supra)national law must be accepted as a settlement for a debt (Selgin, 2003, p. 116; Goldberg, 2009, p. 147). Cryptocurrencies are usually used for payment on a voluntary basis, except in cases where national legislators explicitly grant them the status of a mandatory means of payment (Jozipović, Perkušić & Mladinić, 2024, p. 79), while the acceptance of CBDCs is planned to be mandatory and thus impacts the rights of creditors. Namely, when creditors have to accept a specific means of payment, such payment should be safe and cost-efficient, as all associated costs with the transaction represent an additional burden, which for another legal tender like cash might not exist. For this reason, it was essential to determine the status of CDBCs beforehand and define clear criteria for its use.

While different central banks focused on different key aspects of CBDC development, one important concept for the digital euro was, that it should become an important substitute to cash and thus offer the majority of the advantages that cash provides, without having some of the downsides.

Within the EU, consumer protection and individual privacy are considered high priorities. Thus, end-users of the digital euro should be able to use it in a safe manner that protects their privacy. However, privacy has to be defined differently from anonymity, as in contrast to cash, digital euro transactions are planned to be traceable (ECB-1). In order to limit access to private data, the Proposal for a Regulation on the Digital Euro defines rules for the separation and limitation of access to information. So, the ECB and national central banks will have the role of processing data in order to complete transactions and other related purposes. However, the Proposal states that personal data processing should build on the use of state-of-the-art security and privacy-preserving measures, such as pseudonymization or encryption, to ensure that data is not directly attributed to an identified digital euro user by the ECB and national central banks. (Proposal, art. 35). These rules show that legislation is defining the direction that the technology in this field will have to take.

Cost and efficiency of transactions are essential in order for the digital euro project to be successful. Especially small businesses could have challenges covering installation costs for the required technology as well as additional fees. Therefore, the Digital Euro proposal highlights the following „For microenterprises and non-profit legal entities, the acquisition of the required infrastructure and the acceptance costs would be disproportionate. They should therefore be exempted from the obligation to accept payments in digital euro. In such cases, other means for the settlement of monetary debts should remain available" (Proposal, nr. 18). The Proposal thus determines various exempt groups, like NGOs, natural persons acting for their private purposes or businesses that employ fewer than 10 persons or whose annual turnover or annual balance sheet total does not exceed EUR 2 million (Proposal, art. 9). This exemption is further combined with strict rules on the maximum transaction fees in the legislative part of the proposal. Here the maximum merchant service charge or inter-PSP fee is regulated to ensure that they do not exceed the lowest of the following two amounts (Proposal, art. 17):
(i) incurred services provider cost increased by a reasonable margin of profit and
(ii) fees or charges requested for comparable means of payment.

In the case of CBDCs, (some) positive impacts of the scholarly systematization of law are preceded by and achieved by the regulation. The reason for this is that CBDCs, compared to crypto assets, are public and not private projects and that significant research into new means of payment has already been completed in the crypto-asset and fin-tech space.

3.2. New Technologies and CBDCs

In order to ensure that CBDCs can successfully be implemented, it is necessary to adapt existing financial infrastructure and develop new cyber-security solutions, as well as innovative payment mechanisms. One of the most innovative technologies that is planned to be developed for the digital euro, is the offline payment option. The digital euro is planned to be fully accessible for offline payments similar to cash. This would allow its use even for the unbanked population in the Eurozone, as well as in remote locations without reliable internet access, for example on planes, boats or remote islands. Such a technology, which would be secure, ensure privacy and which could work off-line while being economically viable, currently does not exist, and thus will have to be developed first.

3.3. Regulatory Efforts and Innovation

The regulatory process for the digital euro started early on in the digital euro project. Even in the very early phase, where the potential of the digital euro was assessed, significant efforts were put into determining how the legal design of the digital euro should look. This was important as through the digital euro project, private money would be transformed into public money (ECB-2) Even more, it took for the process to get into an advanced stage before it was decided that innovative and technologically challenging features like offline payment would be implemented early on. The digital euro first had to be defined as a clear concept with its key features. In parallel with this process, the required regulation of the digital euro was already being discussed, and only after this, the process for solving complex technological challenges was initiated (ECB-3). This is in stark contrast to the development of crypto-asset technologies where the legal characteristics of crypto assets were determined *ex-post*. With the digital euro, technological innovation is set for the later stages of the project, basically as a custom solution to the legal and economic characteristics that were already predetermined by the legislator.

4. BENEFITS AND EFFECTS OF LEGAL SYSTEMATIZATION

Having presented digital payments and virtual assets, we can turn to the benefits of scholarly systematization of legal norms in the given context. In this context, it makes sense to first analyze the benefits relating to crypto-asset regulation.

4.1. Benefits of the Systematization of Crypto-Asset Regulation

The first and obvious advantage is the easier identification of relevant legal norms. The development of the "information, communication and technology (ICT)" law is of particular relevance here since digital payments and virtual assets represent a new possibility of transactions, typically used by tech companies which advance technological development. Achieving a high level of legal certainty by identifying and systematizing legal norms in this area of law is necessary in order to foster (or at least not slow down) further technological development. In the early phase of crypto assets, it was essential to classify them not just as data, but in the context of rights and obligations of their holder and third parties. For the 15 years before MiCAR entered into force, classification helped to guide the decision of tax authorities and judicial bodies in the right direction and determine that crypto assets while not considered things, still represent a type of property due to their market value.

Secondly, the more developed the scholarly systematization of law is in this area, the interpretation of relevant legal norms (and in particular, the systematic interpretation) will be easier. For example, the classification of crypto assets into various categories allowed us to classify crypto service providers and determine to which extent other legal norms like AML regulation will be applicable. This made it easier for participants in this space to comply with regulation thus increasing legal certainty.

Third, the more developed the scholarly systematization of law is, the easier the antinomies between norms can be determined. This is especially the case when there is a possibility of regulation from two legislators – the national one, and the (supra)national, EU one. However, we have shown that the initiative from the (supra)national legislator is more relevant here, as the EU is taking the lead in crypto-asset regulation due to the complexity and relevance of the matter.

Fourth, the scholarly systematization of law constitutes new areas of law. The development of new areas of law, such as the mentioned information, communication and technology (ICT) law resolves some of the issues we are facing by establishing itself between public and private law. Furthermore, digital finance law is continuing to emerge as a separate area of law and is undergoing an increasingly dynamic evolution.

Finally, the work on scholarly systematization of law also influences the determination of the competence of various bodies, for example, tax authorities, AML authorities, banking authorities etc.

It is important to note two things. First, we do not propose a particular systematization of crypto-asset regulation here. It would be beyond the scope of any (one) paper. Instead, we use a particular general theoretical framework to present the benefits of the scholarly systematization of legal norms in the area of crypto-asset regulation by providing some examples. In a similar manner, the same general theoretical framework could be used (and in our opinion, fruitfully) in other areas of law. Second, it has to be emphasized that there is a lack of scholarly systematization of legal norms in the area of crypto-asset regulation which creates problems. It comes as a result of regulation lagging behind technological developments. The problems are those that have been mentioned before and which are mitigated by the scholarly systematization of norms. First, the identification of relevant (valid and applicable) legal norms. Second, more difficult interpretation of legal norms and the (im)possibility of applying the systematic interpretation. Third, unclear situations in the cases of conflicts between norms and the question of which norm should take precedence. Fourth, scholarly systematization of law constitutes new areas of law. Fifth and final, the competencies of different bodies can remain unclear and overlap, which can lead to so-called negative conflicts of jurisdiction.

4.2. The Impact of Crypto-Asset Regulation on the Development of New Technologies

Crypto-asset regulation significantly benefited from legal systematization, which helped bridge the 15-year gap between the initial creation of the technology and the first comprehensive regulation in the EU. However, as has been seen above, CBDC regulation took another route. It partially preceded technological development. However, this was only possible due to the fact that CBDC represents a reaction to the increasing popularity of alternative means of payment and the decreasing importance of cash. Thus, the innovations in the field of digital payments, especially crypto assets, paved the route for CBDCs.

When considering this relationship between these innovations, it becomes even clearer how legal systematization impacts innovation. Namely, the legal systematization

conducted concerning crypto assets significantly contributed to the identification of issues with existing payment regulation and allowed legislators to consider public law solutions. CBDCs are in essence a public law regulation-driven innovation that builds on the broader space of financial technology law.

5. CONCLUSIONS

In this paper, we conducted a comparison of crypto-asset regulation and proposed digital euro (CBDC) regulation in the EU and their relation to innovation. By comparing the two very different regulatory processes, we were able to show how systematization impacts innovation and adaptation processes. First, CBDCs heavily relied on the systematization of crypto-asset-related issues, as legal norms from various fields had to be used in order to determine the nature of crypto-assets and the rights and obligations of participants in the crypto-asset space. Later, systematization served an important role in the design of a broader crypto-asset framework. Finally, regulatory competencies have heavily been based on the overlap of ICT law and other fields like tax law, law concerning the prevention of criminal activities, contract law etc. However, the impact of legal systematization did not stop there.

When CBDCs are closely examined, it becomes clear that they do not necessarily represent an anomaly of regulation preceding innovation, but rather a reaction of the public sector to innovation in the private sector. Legal systematization made it possible to identify issues and challenges with payment services and thus allowed regulators to start researching a public answer to private innovation in the payment space both from a regulatory as well as from a technological perspective. While regulation precedes some aspects of the technology that will have to be used for the digital euro, the majority of the processes related to the technology have already been tested by private solutions like crypto assets. Thus, the combination of innovation in the private sector, in combination with regulation concerning that innovation, and significant systematization efforts, created the basis for a "regulation first" approach of CBDCs in the EU.

LIST OF REFERENCES

Books, Monographs and Textbooks

Aarnio, A. 2011. *Essays on the Doctrinal Study of Law*. Dordrecht: Springer. https://doi.org/10.1007/978-94-007-1655-1

Visković, N. 2006. *Teorija države i prava*. 2nd ed. Zagreb: Birotehnika CDO.

Scholarly articles

Bennett Moses, L. 2007. Why have a Theory of Law and Technological Change? *Minnesota Journal of Law, Science and Technology*, 8(2), pp. 589-606.

Çağlayan Aksoy, P. 2023. The applicability of property law rules for crypto assets: considerations from civil law and common law perspectives. *Law, Innovation and Technology*, 15(1), pp. 185-221. https://doi.org/10.1080/17579961.2023.2184140

Goldberg, D. 2009. Legal tender. *Working Paper No. 2009-04*, *2*, Bar-Ilan University, Department of Economics, Ramat-Gan. Available at: https://www2.biu.ac.il/soc/ec/wp/2009-04.pdf (3. 8. 2023).

Jozipović, Š., Perkušić, M. & Gadžo, S. 2022. Tax Compliance in the Era of Cryptocurrencies and CBDCs: The End of the Right to Privacy or No Reason for Concern? *EC Tax Review*, 31(1), pp. 16-29. https://doi.org/10.54648/ECTA2022003

Jozipović, Š., Perkušić, M. & Ilievski, A. 2020. Cryptocurrencies as (i)legal Tender in North Macedonia and the EU. *Iustinianus Primus Law Review*, 11(2), pp. 1-22.

Jozipović, Š., Perkušić, M. & Ilievski, A. 2021. From Taxation to Comprehensive Regulation of Cryptoassets. *Iustinianus Primus Law Review*, 12(1), pp. 1-14.

Jozipović, Š., Perkušić, M. & Mladinić, N. 2024. A comparative review of the legal status of national cryptocurrencies and CBDCs: a legal tender or just another means of payment. *Pravni vjesnik: časopis za pravne i društvene znanosti Pravnog fakulteta Sveučilišta J. J. Strossmayera u Osijeku*, 40(1), pp. 77-95. https://doi.org/10.25234/pv/27044

Mandjee, T. 2015. Bitcoin, its Legal Classification and its Regulatory Framework. *Journal of Business and Securities Law*, 15, pp. 157-211.

Perkušić, M., Jozipović, Š. & Piplica, D. 2020. The need for legal regulation of blockchain and smart contracts in the shipping industry. *Transactions on Maritime Science*, 9(2), pp. 365-373. https://doi.org/10.7225/toms.v09.n02.019

Selgin, G. 2003. Adaptive Learning and the Transition to Fiat Money. *The Economic Journal,* 113, pp. 147–165. https://doi.org/10.1111/1468-0297.00094

Takahashi, K. 2022. The law is applicable to proprietary issues of crypto-assets. *Journal of Private International Law*, 18(3), pp. 339–362. https://doi.org/10.1080/17441048.2022.2138102

Trautman, L. J. 2018. Bitcoin, Virtual Currencies, and the Struggle of Law and Regulation to Keep Pace. *Marquette Law Review*, 102(2), pp. 448–537. https://doi.org/10.2139/ssrn.3182867

van der Linden, T. & Shirazi, T. 2023. Markets in crypto-assets regulation: Does it provide legal certainty and increase adoption of crypto-assets? *Financial Innovation*, 9:22, pp. 1–30. https://doi.org/10.1186/s40854-022-00432-8

Wronka, C. 2024. Crypto-asset regulatory landscape: a comparative analysis of the crypto-asset regulation in the UK and Germany. *Journal of Asset Management*, pp. 1-10. https://doi.org/10.1057/s41260-024-00358-z

Zilioli, C. 2020. Crypto-Assets: Legal Characterisation and Challenges under Private Law. *European Law Review*, 45(2), pp. 251-266. https://doi.org/10.2139/ssrn.3532316

Articles, Press Releases and Reports

ECB-1 – A stocktake on the digital euro – Summary report on the investigation phase and outlook on the next phase, ECB 2023. Available at: https://www.ecb.europa.eu/paym/digital_euro/investigation/profuse/shared/files/dedocs/ecb.dedocs231018.en.pdf (1. 10. 2024).

ECB-2 Panetta, F. & Dombrovskis, V. Why Europe needs a digital euro. 2023. Available at: https://www.ecb.europa.eu/press/blog/date/2023/html/ecb.blog230628~140c43d2f3.en.html (1. 10. 2023).

ECB-3 – press release ECB. 2022. Available at: https://www.ecb.europa.eu/press/key/date/2022/html/ecb.sp221107~dcc0cd8ed9.en.html (1. 10. 2024).

IRS notice - Internal Revenue Service, Notice 2014–21, 2014–16 I.R.B. 938. Available at: http://www.irs.gov/pub/irs-drop/n-14-21.pdf (1. 10. 2024).

Nakamoto, S. 2008. Bitcoin: A Peer-to-Peer Electronic Cash System. White paper.

UK-policy brief - Policy paper, Revenue and Customs Brief 9 (2014), Bitcoin and other cryptocurrencies. Available at: https://bitcoin.org/bitcoin.pdf (1. 10. 2024).

Yuan progress report - Progress of Research & Development of E-CNY in China, Working Group on E-CNY Research and Development of the People's Bank of China 3, 8 (July 2021).

Legal sources and case law

AMLD 5 – Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU.

MiCAR - Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937, PE/54/2022/REV/1.

MiFID II - Council Directive 2014/65/EC of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU [2014] OJ L173/349.

Proposal for a Regulation of the European Parliament and of the Council on the establishment of the digital euro, COM/2023/369 final.

Skatteverket/Hedqvist (C-264/14) EU:C:2015:718.

UDC: 004.738.5:364.636-057.1 DOI: 10.56461/iup_rlrc.2024.5.ch19

*Helga ŠPADINA**
Faculty of Law, "Josip Juraj Strossmayer" University of Osijek, Croatia
*Marijana LJUBIĆ***
Faculty of Law, University of Mostar, Bosnia and Herzegovina

CYBERBULLYING AND DIGITAL EXCLUSION AS NEW FORMS OF WORKPLACE MOBBING

Technological innovations in labour law are allowing us to accelerate the pace of labour and to achieve more in a shorter time. Innovations led to the digitalization of all spheres of life, including our work, which then significantly increased the possibility of virtual and digital violence. Virtual violence has several well-known forms, such as digital abuse, cyberbullying, cyberstalking, online sexual harassment, cross-platform harassment, non-consensual intimate image sharing (or revenge porn), sextortion, unsolicited pornography, unwanted sexualization, impersonation, hate online speech, hacking, doxing, trolling, digital voyeurism, Zoom bombing and other forms of digital abuses. Among those, cyberbullying is moving from online social networks to the world of labour relations. There, it takes several forms from the apparent one to the almost invisible form which is the digital exclusion of access to work-related information in digitalized work environments.

Cyberbullying through digital exclusion is very peculiar because it is difficult to establish facts and prove that a worker was intentionally digitally excluded from important work information. Secondly, it is difficult to prove the intention of the abuser. Thirdly, it is difficult to establish a link that would amount to cyberbullying.

Digital exclusion as one of the forms of harassment at work, can be used to isolate and ignore workers and deliberately exclude them from other employees and superiors. Victims of digital exclusion at work can also be managerial employees of individual organizational units within the institution, whose supervisor prevents them from implementing digitalization and business improvement through computerization and connecting common services within a single organizational unit.

The paper has two research questions: the first question is whether we can qualify digital exclusion as a form of cyberbullying in labour relations. The second research question is

* PhD, Associate Professor, ORCID: 0000-0002-5826-176X, e-mail: *hspadina@pravos.hr*

** M.sc. iur, Doctoral Candidate, ORCID: 0009-0005-7609-1193, e-mail: *marijana.ljubic@gmail.com*

how labour law could regulate the prevention of cyberbullying and digital exclusion. The aim of the paper is to contribute to academic discussions on the timely regulation of novel issues in labour law.

Keywords: digital violence, digital exclusion, cyberbullying.

1. VIOLENCE AND HARASSMENT IN THE WORKPLACE

> „Recognizing the right of everyone to a world of work free from violence and harassment...
> ...violence and harassment in the world of work can constitute a human rights violation or abuse...
> ...a threat to equal opportunities... and unacceptable and incompatible with decent work"
>
> ILO, C190, 2019

Digital transformation of a workplace is a key step in modernizing work and maintaining competitiveness. Digitalization is a prerequisite for modern, efficient, competitive, secure business, and more efficient use of human resources leads to better work results, and easier and faster communication and cooperation. However, despite today's digital age, digitality offers ample space for abuse in the workplace. Digital violence or cyber violence including cyberbullying and all other sub-forms like digital exclusion is becoming one of the prevailing forms of harassment at work, which can be used to isolate and ignore workers and deliberately exclude them from active participation in work processes and decision-making.

Violence and harassment at work jeopardize the health of a victim, dignity, right to livelihood and decent work. It breaks the emotional and psychological well-being of a worker, reduces productivity and it turns a workplace into a place of anxiety and fear for a worker who is a harassment victim. Harassment has huge financial costs for employers who instead of investing in research and development, have to cover the high costs of litigation, investigation and sick leaves, all with huge loss in productivity and turnover of workers. ILO pointed out that harassment impacts negatively on the organization of work, workplace relations, worker engagement, enterprise reputation, and productivity.[1]

Prior to the digitalization of work, workplace violence was broadly identified as physical and psychological, with numerous sub-categories dependent on the severity of the offence. Violence at work in person was slightly different than today, sometimes more visible because in many cases incidents would have witnesses. In recent years, with the rapid development of digitalization, violence has digitalized with some remarkable features because of very sophisticated methods, extremely fast sharing time or on the opposite side, very easy cover (it takes few seconds to delete online abuse) and its availability to basically unlimited or insufficiently limited online audience. All of these can cause devastating health consequences and can be even fatal (as we witnessed in recent

[1] ILO C190, 2019.

suicides of youth who were cyberbullied) if a victim does not develop an appropriate coping mechanism or reach out for professional help.

When considering the elements of the definition of digital violence in the workplace, the starting point should be a standard definition of violence transformed into the digital space. International Labor Organization in the C190 - Violence and Harassment Convention, 2019 (No. 190) defined "violence and harassment in the world of work as to refer to a range of unacceptable behaviours and practices, or threats thereof, whether a single occurrence or repeated, that aim at, result in, or are likely to result in physical, psychological, sexual or economic harm, and includes gender-based violence and harassment."[2] Awareness of the digital vulnerability of workers to online abuse was reflected in the 2019 ILO Violence and Harassment Convention as the first international legal instrument which regulated cyberbullying through inclusion of the ICT communication in the scope of the Convention in the art. 3 *(*"This Convention applies to violence and harassment in the world of work occurring in the course of, linked with or arising out of work: (d) through work-related communications, including those enabled by information and communication technologies…").[3]

Considering possible forms of digital violence, it can take the form of digital abuse, sending inappropriate (usually offensive or sexualized) text messages, chats or comments, cyberbullying, cyberstalking, online sexual harassment, cross-platform harassment, nonconsensual intimate image sharing (or revenge porn), sextortion, unsolicited pornography, unwanted sexualization, impersonation, hate online speech, hacking, doxing, trolling, digital voyeurism, Zoom bombing and other forms of digital abuses. In this paper, we will focus on digital exclusion as one form of cyberbullying which is moving from online social networks to the world of labour relations and can lead to negative work status outcomes, usually demotion or termination of employment.

2. DEFINING DIGITAL EXCLUSION

Exclusion at work refers to the situation in which individuals or groups of employees are intentionally or unintentionally left out, marginalized, or treated unfairly within the workplace environment. Exclusion can manifest in both overt and subtle ways, creating a hostile or unwelcoming atmosphere that can have negative consequences for individuals and the organization as a whole.[4]

Formerly obvious exclusion from work and withholding of important documents and/or information became more blurred and hidden behind the vast size of electronic correspondence.

Victims of electronic violence through digital exclusion at work can be all categories of workers within the employer's organizational structure, including employees who perform managerial tasks within the institution, i.e. heads of individual organizational units.

[2] ILO, C190, 2019.

[3] Ibid.

[4] Fermin, J. 2023. How to identify exclusion in the workplace. Available at: https://www.allvoices.co/blog/how-to-identify-exclusion-in-the-workplace (1. 7. 2024).

The basic form of digital exclusion as a form of harassment at work is complete disconnection from digital communication by intentionally disabling access to communication technologies and tools, i.e. refusing digital communication with the employee. In this way, the employee is excluded from teamwork, intentionally not invited to work meetings, social events and activities related to the employer. This exclusion, lack of support in work and ignoring the employee's contribution to work results in a lack of information due to intentional withholding of data or insufficient information of the employee about the data necessary to perform the tasks of his workplace, as well as the social exclusion of the employee from the rest of the business team in the performance of his work tasks, which leads to a decline in motivation for work and efficiency in performing tasks.[5] Furthermore, a form of digital exclusion is the intentional denial, restriction or difficulty of access to information that is essential for the performance of the employer and the duties of the employee's workplace. This restriction can intentionally hinder the use of communication channels and make it difficult to access information through the use of digital documents, thus depriving the employee of important information and instructions for performing the work tasks of his workplace (for example, obstructing or disabling the receipt of e-mails, restricting access to certain content on the employer's website or content located in the so-called shared folders used by more than one person, intentionally excluding an employee from webinars and online meetings, and many other forms), disabling access to information occurs by restricting access to the employer's official documentation and certain documents stored in digital form, as well as access and use of IT programs necessary for the performance of the duties and tasks of the employee's workplace.[6]

All of the above forms of digital exclusion can result in harassment of employees at work and have serious negative consequences on productivity, efficiency, professional development and health of the worker who is a victim of cyberbullying.[7]

3. IN-PERSON BULLYING IN THE WORKPLACE V. CYBERBULLYING

Workplace bullying is usually repeated and unreasonable behaviour directed towards a worker or a group of workers that creates a risk to health and safety. Examples of behaviour, intentional or unintentional, that may be workplace bullying if they are repeated, unreasonable and create a risk to health and safety include, but are not limited to abusive, insulting or offensive language or comments, aggressive and intimidating conduct, belittling or humiliating comments and victimization.[8]

For the International Labor Organization (ILO), workplace bullying is "offensive behaviour through vindictive, cruel, malicious or humiliating attempts to undermine an individual or groups of employees. It involves ganging up on or "mobbing" a targeted employee and subjecting that person to psychological harassment. Mobbing includes

5 *Ibid.*

6 *Ibid.*

7 *Ibid.*

8 Safe Work Australia, Guide for Preventing and Responding to Workplace Bullying, 2016.

constant negative remarks or criticisms, isolating a person from social contacts, and gossiping or spreading false information."[9]

This definition is applicable to cyberbullying which includes the same elements as the ILO outlined, with some distinctive elements such as lack of isolation of a victim from social contacts.

Heinz Leymann who is considered a creator of the term "mobbing" defined key elements of mobbing at the workplace as: "psychological terror or mobbing in working life involves hostile and unethical communication which is directed systematically by one or more individuals, mainly toward one individual who, due to mobbing, is pushed into a helpless and defenceless position and held there by means of continuing mobbing activities. These actions occur on a very frequent basis (at least once a week) and over a long period of time (at least six months' duration). Because of the high frequency and long duration of hostile behaviour, this maltreatment results in considerable mental, psychosomatic and social misery."[10]

OECD pointed out key differences between in-person bullying and cyberbullying[11]

Table 1.1. Core features of traditional bullying and cyberbullying

Features	Traditional bullying	Cyberbullying
Aggressive acts	Verbal, physical, relational	Verbal, relational
Repetition	The actions occur repeatedly	Easy sharing and forwarding, and permanence of the digital environment mean that one act of cyberbullying can be viewed and experienced many times without repetition of the act or bullying behaviours by the perpetrator
Power imbalance	Key factors could be physical strength, age, social status, intelligence	More difficult to define in the digital environment; key factors could be popularity, social status, digital skills, anonymity
Intentionality	Present	Present
Space	Relegated to school or other in-person environments	Omnipresence of digital environment means cyberbullying has no fixed boundaries
Bystanders	Physically present; tends to be a small group	Bystanders could simply be witnesses to the acts in real time or at a later time; they could be physically present with the bully or the victim when the act occurs; the audience can be large or small

(Source: OECD, 2022)

4. IS DIGITAL EXCLUSION A SUBFORM OF CYBERBULLYING IN THE WORKPLACE?

In testing whether digital exclusion can be considered a form of cyberbullying in the workplace, we need to look into the crucial elements of (cyberbullying and analyse whether these elements are applicable to digital exclusion. In doing so, we will take elements of workplace mobbing or bullying as defined by Leymann[12] and key elements of cyberbullying as defined by the OECD.

[9] ILO, 1998, p. 2.

[10] Leymann, 1996.

[11] Gottschalk, 2022.

[12] Leymann, 1996.

4.1. Comparison Between Crucial Elements of Bullying Definition (Leymann) and Digital Exclusion

4.1.1. Psychological Terror

Omission to do something in the workplace which jeopardizes job security – like exclusion from work communication and information sharing – can be considered a form of psychological terror because the victim is constantly under stress and is unable to perform the job due to exclusion. Psychological terror in the workplace is difficult to establish post-festum and it is subject to individual perception. One person can consider digital exclusion a terror and harassment because of his/her work ethic and interest in the job, while the other person can be satisfied that the workload decreased, while the salary is still being paid. Therefore, in order to establish properly whether digital exclusion led to psychological terror, we need to employ the usual and widely accepted standard of a reasonable person that is used to establish harassment in the workplace.[13]

4.1.2. Hostile and Unethical Communication

Lack of necessary work-related communication in the workplace signals a high likelihood of visible or invisible harassment. If an employer or peers exclude someone from usual communication, although there is no direct hostile or unethical communication, silence in communication creates hostility because the victim of such communication is unaware of the reasons, next steps (if the perpetrator is a supervisor), possibility to get promoted and participate in the professional development and overall future prospects of that job. A subtle message linked to digital excommunication is always that the victim is not needed anymore, so his involvement in work-related communication is unnecessary, leading to the possibility of demotion or termination of an employment contract. Hostility in this case is performed by the omission of including workers. The unethical component is the manner in which this is done. Instead of clearly and transparently communicating to the worker that his performance is lower than expected, that his position will be laid off in the near future or that there are issues in his/her performance, by digitally excluding a worker, the employer is choosing the most unethical venue because it creates hostile work environment.

---

[13] First explicitly espoused and adopted by the Ninth Circuit court of Appeals in Ellison v Brady, 924 F2d 872 (9th Cir 1991). The reasonable woman standard was first espoused in the Rabidue dissent by Judge Keith. Rabidue v Osceola Refining Co., 805 F2d 611, 623-28(6th Cir 1986). In his dissent, Judge Keith criticized the majority's finding that the lewd comments and posters of nude and semi-clad women did not create a hostile working environment since "the overall circumstances of the plaintiff's workplace evince[d] an anti-female environment". Rabidue, 805 F2d at 623. In criticizing the majority's conclusion, he disagreed with the court's holding that, in considering hostile environment claims, the courts should adopt the perspective of the reasonable person's reaction to a similar environment. The judge opined, "the reasonable person perspective fails to account for the wide divergence between most women's views of appropriate sexual conduct and those of men." Id at 626. The judge concluded, unless a reasonable woman standard is adopted, "the defendants as well as the courts [will be] permitted to sustain ingrained notions of reasonable behavior fashioned by the offenders, in this case, men," in Gettle, 1983. Available at: https://dsc.duq.edu/dlr/vol31/iss4/9 (5. 7. 2024). Cf. Winterbauer, 1991, pp. 811-821.

4.1.3. Systematic Manner

Digital exclusion is mostly systematic in its course. In order to establish a harassment pattern of digital exclusion, there must be systematic behaviour, meaning that one incident of digital exclusion would not suffice to be considered cyberbullying through digital exclusion. The systematic manner of digital exclusion could be established only through a detailed electronic analysis of the digital correspondence of the perpetrator and the applicability of the relevance test of correspondence to the victim of digital exclusion. If the systematic manner of digital exclusion is firmly established, then digital exclusion evidently forms one sub-group of mobbing or bullying in the workplace.

4.1.4. Conducted by One or More Individuals

Digital exclusion can be conducted by anyone in the workplace. Most frequently, it will be conducted by the supervisor for the mere fact that such exclusion would be reported and acted upon due to its labour status implications for the victim. Digital exclusion can be conducted by several individuals and this situation is frequent when the management of an employer company systematically harasses one worker through work-related isolation and exclusion from work-related correspondence. Also, we can have digital exclusion by individual peers (colleague) or a group of colleagues who intentionally excluded their colleague.

4.1.5. Directed Toward One Individual

Digital exclusion can be directed either toward one worker or a group of workers. If one worker is excluded from work-related communication, it is more difficult to prove exclusion, while group exclusion might be rare, but definitely easier to establish in possible informal and formal proceedings to demonstrate digital exclusion.

4.1.6. Helpless and Defenseless Position

A worker who has been digitally excluded is in a helpless and defenceless position because he/she might not be aware that important work decisions have been made without him/her. Victims of such abuse might not be aware he/she is left out of training opportunities, promotions, webinars and other professional development opportunities. The position of digitally excluded worker is defenceless because the person is unaware of ongoing cyber mobbing and cannot properly prepare his/her defence. Due to the ease of deleting digital trail of work correspondence, a worker might not be able to prove that he/she was indeed a victim of digital exclusion unless his/her peers were copied to the correspondence.

4.1.7. High Frequency (At Least Once a Week)

Due to the high rate of digital exchange in today's workplaces, it would not be an issue to have a high frequency of digital exclusion. In addition to the exclusion from email correspondence, worker can be excluded from social networks which are being used to communicate such as Telegram, Microsoft Teams, Viber, Instagram and other platforms for communication.

4.1.8. Long Duration of Hostile Behaviour (At Least Six Months)

This element of in-person mobbing[14] Is not applicable to the digital exclusion because of the speed of digital communication and the amount of electronic messages exchanged during working hours and after working hours, all related to work. In such a speed of digital communication, one can easily receive hundreds of electronic messages per day, so this element of having hostile behaviour lasting at least six months is more applicable to real life, rather than in cyber work where throughout just one week, a worker can be excluded from several hundreds or even thousands relevant messages.

4.1.9. Maltreatment Results in Considerable Mental, Psychosomatic and Social Misery

Digital exclusion does lead to the misery of a victim the same way as in-person forms of harassment lead to negative health outcomes and can cause mental, psychosomatic and social misery. The direct link between digital exclusion as any other form of workplace mobbing and the health of a victim has been well established and documented in comprehensive research on the topic of health consequences of workplace abuse.[15]

4.2. Comparison Between Cyberbullying (OECD) and Digital Exclusion

4.2.1. Aggressive Acts

Digital exclusion at work is an act of aggression because it jeopardizes equal opportunities, discriminates against an employee who becomes a victim of unfair treatment and it jeopardizes the right to work. It is not relevant whether the aggression is done at the micro or macro level, as long as it creates information isolation and a work environment in which an employee cannot perform his/her work due to a lack of relevant digital correspondence and work-related information. Aggressive acts can also take the form of exclusion from online meetings and webinars. All of these lead to a situation in which an employee cannot participate in the work-related discussion and will bear labour status-related consequences of such abuse.

4.2.2. Repetition

Digital exclusion can easily be frequently repeated in digital space. A worker who is a victim of digital exclusion can notice it if he/she maintains contact with colleagues. If a victim works remotely, there is a limited possibility of noticing digital exclusion and digital isolation. In assessing the relevance of repletion, we would need to apply the same reasoning as courts when assessing whether harassment was persistent.[16]

---

[14] Cf. Nielsen & Einarsen, 2018. pp. 71-83.

[15] Study links workplace harassment to serious health issues. Atamba *et al.,* 2023; Abdulla, Lin & Rospenda, 2023, pp. 899-904; Rospenda *et al.*, 2005 pp. 95-110; Rospenda, Richman & McGinley, 2023.

[16] Cf. High Court in DPP (O' Dowd) v Lynch, 2008, IEHC 183.

4.2.3. Power Imbalance

Digital exclusion in the workplace has more serious consequences if it is done by superiors and targets subordinate employees. In this case, the employee can easily lose a job because he/she is unable to perform well without access to all important information. If peers digitally exclude a colleague from work-related correspondence, consequences can also be detrimental, but they might not result in job loss. If a subordinate employee intentionally digitally excludes his/her supervisor(s), consequences would likely be rather detrimental for a perpetrator.

4.2.4. Intentionality

In today's digitalized work, it will be challenging, but not impossible, to establish intentional digital exclusion of an employee because usually emails address large groups of employees and it is very easy to blame the speed of communication and unintentional omission. Therefore, it is crucial to include a factor of repetition of such behaviour over the course of a certain time to establish properly that a specific employee was intentionally excluded from work-related correspondence. Another issue is the necessity to examine professional email accounts to establish which correspondence was withheld from certain employees, as emails can easily be deleted and supervisors can easily say that simply forgot to share certain information with an employee.

4.2.5. Space

Digital exclusion happens in digital space which is a very vast term to encompasses not only email correspondence, but also work-related information exchanged through various social networks such as WhatsApp, Viber, Instagram, Facebook, Telegram, SMS messages, internal work platforms, clouds, shared maps, and many other forms of digital communication. In such a diversity of communication channels, and with unlimited options to delete sensitive communication for criminal or labour dispute litigation purposes, a victim of digital exclusion should not be in a position to prove the discriminatory behaviour of the perpetrator and the burden of proof should shift to the respondent to prove that he/she did not commit the unlawful act.

4.2.6. Creation of a Hostile Work Environment

Digital exclusion at the workplace creates a hostile work environment in both situations – if the employee is aware of it and if an employee is unaware of it and assumes he/she might be a victim of digital exclusion. An employee who has been excluded from important information and discussions with the purpose of sending a subtle message that the employer does not need him/her anymore and his/her contract will soon be terminated, experiences a hostile work environment in which employee feels insecure, stressed and under pressure. If exclusion goes unnoticed and unaddressed by the supervisor for a certain period of time, the level of stress for an employee is even higher due to a lack of information about why exclusion happened and a lack of feedback on performance, so in this case, the hostile

work environment can yield more serious health wellbeing consequences for a worker. US Supreme Court even further extended the scope of hostile work environment in DPP v Doherty to include communications which are not directly addressed or sent to the subject of those communications but to persons close to the victim.[17] Along the same line of thought, there is a theoretical distinction between direct and indirect cyberbullying.[18]

In conclusion of this chapter and taking into consideration of above-mentioned test for all key elements of cyberbullying and workplace mobbing, digital exclusion fulfils all main criteria of both definitions and therefore, it can be considered as a sub-form of cyberbullying at work.

5. LEGAL REGULATION OF DIGITAL EXCLUSION IN THE WORKPLACE

Legal regulation of prohibition of all forms of cyberbullying, including, but not limited to digital exclusion, is crucial in the prevention of such abuse of labour relations. International and national labour law – through primary and secondary legislation - laws, regulations, collective agreements and internal employment policies - could minimize the risk of all forms of cyberbullying, including digital exclusion. In that sense, ILO has stipulated obligations of Member States in art. 42. of C 190 Violence and Harassment Convention from 2019.[19] Therefore, when regulating the prohibition of digital exclusion, we need to be aware that the starting point should be a clear legal commitment grounded on a strict and explicit prohibition of all forms of digital violence, including digital exclusion or intentional omission to facilitate digital work tools as a method of mobbing of workers. Further, policy needs to provide a definition of a problem, establish confidential reporting procedures, disciplinary procedures and investigation and regulate proper informal and formal settlement procedures, prior to court litigation and post-festum counselling services for victims.

---

[17] DPP v Doherty, 2019, IECA 350.

[18] Langos, 2012, pp. 285-289; De Stefano *et al*., 2020.

[19] ILO C190, 2019 "Each Member shall adopt, in accordance with national law and circumstances and in consultation with representative employers' and workers' organizations, an inclusive, integrated and gender-responsive approach for the prevention and elimination of violence and harassment in the world of work. Such an approach should take into account violence and harassment involving third parties, where applicable, and includes:
(a) prohibiting in law violence and harassment;
(b) ensuring that relevant policies address violence and harassment;
(c) adopting a comprehensive strategy in order to implement measures to prevent and combat violence and harassment;
(d) establishing or strengthening enforcement and monitoring mechanisms;
(e) ensuring access to remedies and support for victims;
(f) providing for sanctions;
(g) developing tools, guidance, education and training, and raising awareness, in accessible formats as appropriate; and
(h) ensuring effective means of inspection and investigation of cases of violence and harassment, including through labor inspectorates or other competent bodies."

The next step is to regulate properly the rights and obligations of all workers regarding cyber communication, including basic rules on decent digital communication, prohibition of online harassment and digital exclusion. All of these need to be sanctioned adequately through disciplinary sanctions. Each employee and all managers should get familiar with all the rules, organize induction and refresher training and sign a form outlining that the employee has understood the main features of the policy.

Victims of digital exclusion should not be in a position to prove digital exclusion and discriminatory behaviour of the perpetrator and the burden of proof should shift to the respondent to prove that he/she did not intentionally digitally exclude the worker and that exclusion was reasonable and justified for the benefit of work.

6. CONCLUDING REMARKS

Due to the rapid pace of digitalization of work, cyberbullying at work replaces in-person workplace bullying and mobbing. As such, it required immediate attention of legal practitioners and academics because if it is ignored, the basic labour rights of workers will be jeopardized while employers will have to bear the loss in other, previously mentioned workplace harassment-related costs - primarily, the cost of productivity.

Subsequently, within cyberbullying at work, we can distinguish several sub-categories of abusive behaviour, among which is digital exclusion leading to negative work status outcomes, usually demotion or termination of employment.

Digital exclusion at work is a serious breach of labour law and this paper tested the main elements of cyberbullying and workplace mobbing against their applicability to digital exclusion. The result of such a test is that digital exclusion fulfils all the crucial criteria of bullying definition (psychological terror, hostile and unethical communication, systematic manner, conducted by one or more individuals, directed toward one individual, helpless and defenceless position, high frequency, and maltreatment results in considerable mental, psychosomatic and social misery) while it partially meets criteria of long duration (of at least six month) due to high frequency of such abuse linked to the amount of electronic correspondence. In the second test, we compared the OECD definition of cyberbullying to digital exclusion and established that all elements exist in digital exclusion (aggressive acts, repetition, power imbalance, intentionality, space and creation of a hostile work environment). Therefore, the conclusion is that digital exclusion can be qualified as a sub-form of both - cyberbullying and workplace mobbing.

The second research question was related to possible legal regulation of the prevention of cyberbullying and digital exclusion in labour law. The paper sets out the key elements of such regulation, following the lines of ILO which guided the best avenue to take for regulation of prevention of workplace harassment in its Violence and Harassment Convention from 2019.

The way forward should be to take into consideration sometimes overly dynamic changes in labour relations, such as the digitalization of work communication, and predict and legally sanction possible abusive behaviours in digital space to prevent them from actually harming workers.

LIST OF REFERENCES

Abdulla, A. M., Lin, T. W. & Rospenda, K. M. 2023.Workplace Harassment and Health: A Long Term Follow up. *Journal of Occupational and Environmental Medicine,* 65(11), pp. 899-904. Available at: https://acoem.org/Publications/Press-Releases/Workplace-Harassment-and-Health-%E2%80%93-A-Long-Term-Follow-Up (17. 6. 2024). https://doi.org/10.1097/JOM.0000000000002915

Atamba, C., Mosonik, J. K., Stuckler, D., Sungu, L. J., Santoso, C. M. A. & Mohamed, H. H. 2023. Impact of Workplace Mistreatment on Employees' Health and Well-Being in Chinese Firms: A Systematic Review. *Sage Open*, 13(4). https://doi.org/10.1177/21582440231211417

De Stefano, V., Stylogiannis C., Wouters, M. & Durri I. 2020. "System needs update": Upgrading protection against cyberbullying and ICT-enabled violence and harassment in the world of work. *ILO Working Papers*, 1. Available at: https://webapps.ilo.org/static/english/intserv/working-papers/wp001/index.html (20. 6. 2024).

DPP v Doherty [2019] IECA 350. Available at: https://ie.vlex.com/vid/dpp-v-doherty-840637726 (20. 6. 2024).

Fermin, J. 2023. How to identify exclusion in the workplace. Available at: https://www.allvoices.co/blog/how-to-identify-exclusion-in-the-workplace (1. 7. 2024).

Gettle, J. A. 1983. Sexual Harassment and the Reasonable Woman Standard: Is It a Viable Solution? *Duquesne Law Review*, 31(4), pp. 841-858.

Gottschalk F. 2022. Cyberbullying: An overview of research and policy in OECD countries, *OECD Education Working Paper* No. 270. Available at: https://www.oecd-ilibrary.org/education/cyberbullying_f60b492b-en (20. 6. 2024).

High Court in DPP (O' Dowd) v Lynch. 2008. IEHC 183.

ILO, C190. 2019. Violence and Harassment Convention. Available at: https://normlex.ilo.org/dyn/normlex/en/f?p=NORMLEXPUB:12100:0::NO::P12100_ILO_CODE:C190 (20. 6. 2024).

International Labor Organization (ILO). 1998. When working becomes hazardous, Available at: http://www.ilo.org/public/english/bureau/inf/magazine/26/violence.htm) (20. 6. 2024).

Langos, C. 2012. Cyberbullying: The Challenge to Define. *Cyberpsychology, Behavior, and Social Networking,* 15(6), pp. 285-289. https://doi.org/10.1089/cyber.2011.0588

Leymann, H. 1996. The Mobbing Encyclopaedia. Available at: http://www.leymann.se/English/12100E.HTM (20. 6. 2024).

Long-Term Effects of Harassment on Mental Health. 2024. Available at: https://workshield.com/long-term-effects-of-harassment-on-mental-health/ (20. 6. 2024).

Nielsen, M. B. & Einarsen, S. 2018. What we know, what we do not know, and what we should and could have known about workplace bullying: An overview of the literature and agenda for future research. *Aggression and Violent Behavior,* 42, pp. 71-83. https://doi.org/10.1016/j.avb.2018.06.007

Rospenda, K. M., Richman, J. A., Ehmke, J. & Zlatoper, K. W. 2005. Is Workplace Harassment Hazardous to Your Health? *Journal of Business and Psychology*, 20(1), pp. 95-110. https://doi.org/10.1007/s10869-005-6992-y

Rospenda, K. M., Richman, J.A., McGinley, M. 2023. Effects of chronic workplace harassment on mental health and alcohol misuse: a long-term follow-up. BMC Public Health, 23, pp. 1-12. https://doi.org/10.1186/s12889-023-16219-0

Safe Work Australia. 2016. Guide for Preventing and Responding to Workplace Bullying. Available at: https://www.safeworkaustralia.gov.au/system/files/documents/1702/guide-preventing-responding-workplace-bullying.pdf (25. 6. 2024).

Study links workplace harassment to serious health issues. 2024. Available at: https://www.safetyandhealthmagazine.com/articles/25192-study-links-workplace-harassment-to-serious-health-issues (25. 6. 2024).

Winterbauer, H. 1991. Sexual Harassment—The Reasonable Woman Standard. *The Labor Lawyer, American Bar Association*, 7(4), pp. 811-821.

UDC: 004.42: 331.5.024.5 DOI: 10.56461/iup_rlrc.2024.5.ch20

Mina KUZMINAC*
Faculty of Law, University of Belgrade, Serbia
Mario RELJANOVIĆ**
Institute of Comparative Law, Belgrade, Serbia

NEW ACTORS OR NEW TOOLS – ALGORITHMS IN EMPLOYMENT AND LABOUR RELATIONS

It can be said that, for more than a decade, algorithms seriously affected the work processes around the world. Despite this, in most countries, there are only pioneering attempts to analyze their impact on the quality of the enjoyment of workers' rights and to prevent or sanction the possible abuses of algorithmic decision-making. The research follows some basic recorded bad practices, both during the hiring process and in the work process itself. The goal is to point out the fact that algorithms in themselves represent a significant technological achievement that makes labour relations more efficient and easier, but that precise normative limits of their usage have to be set. Algorithms are therefore neither good nor bad themselves, as good or bad are more of parameters by which their functioning has been defined. Guided by this idea, authors try to point out basic principles of prior and subsequent control of algorithmic decision-making, in order to preserve or improve the quality of the achieved rights of workers without, at the same time, diminishing the importance of automation of data processing in the work process. Available current literature on this topic, as well as normative sources and the most significant judicial practice, were used in the research.

Keywords: algorithms in labour law, algorithmic management, labour rights, employment discrimination, human-in-command approach.

* LL.M, Teaching Assistant, ORCID: 0000-0003-3209-231X, e-mail: *mina.kuzminac@ius.bg.ac.rs*

** PhD, Research Fellow, ORCID: 0000-0001-6379-7545, e-mail: *m.reljanovic@iup.rs*

1. INTRODUCTION AND CONCEPTUAL BACKGROUND

The labour market and the world of work which exists today, from a macro perspective, is, in some aspects, very similar to the world of work that existed decades ago, with the constantly present struggle to truly implement the fundamental labour law principles. In that sense, "human work in organizations has been influenced and shaped by digital technologies ever since their advent in the mid-twentieth century. In the earlier stages of development, digital systems were mainly used for calculation tasks that were cumbersome or time-intense for humans to perform" (Oppl & Stary, 2019, p. 1). The categories established in labour law are designed to assign legal status, from which certain associated rights and obligations flow (Koscher, 2022, p. 17). These categories are being blurred by some factors emerging in the labour markets worldwide. A closer look allows us to see changes and particularities influenced by "new" factors and trends such as the neoliberal concept of economy and society, demographic change, climate change, globalization and global crises and certainly, digitalization.[1] Having in mind the mentioned, in this part, we shall focus on the one issue which belongs, so to speak, to the trend of a "new normative basis for future paradigms regulating the digital world" – work processes algorithms.[2]

We shall address this issue from the wider perspective, in terms of referring to possible advantages, as well as disadvantages of algorithms "participating" in the labour market, at the employer's side of the employment process and organization of the work duties. However, we shall also try to incorporate the micro perspective i.e. the worker's perspective facing the algorithm, into the research.[3]

Algorithmic management is a process of automated decision-making by the computer based on preset software (data) parameters. An explanatory memorandum for the Directive on improving working conditions in platform work sums up its role in the work process: "Digital labour platforms use automated systems to match supply and demand for work. Albeit in different ways, digital platforms use them to assign tasks, monitor, evaluate and make decisions for the people working through them. Such practices are often referred to as 'algorithmic management'" (Proposal for a Directive of the European Parliament and of the Council on improving working conditions in platform work).[4] However, algorithms

[1] When it comes to digitalization and the world of work, it is certain that digitalization makes a lot of things possible, easier and more efficient. At the same time, it bears many risks, with the obvious one being putting the equality sign between digitalization and precarization. Reljanović & Misailović, 2021, pp. 407–410. The said is true not "only" when it comes to the world of work –"history shows that technological advances make work easier, safer, and more productive, but at the same time open opportunities for abuse". Bagari & Franca, 2023, p. 138.

[2] In this "new reality", new discourses are being formed and becoming more present. As stated, "one example of this is the discourse that casts social problems as technological problems, capable of being solved through proper algorithms or further technological innovation in the 'new spirit of digital capitalism'". Kocher, 2022, p. 22.

[3] Certainly, algorithms are becoming increasingly "popular" not only in employment but in different spheres of life and concerning different issues, from education to police investigations. Morondo Taramundi, 2022, p. 74.

[4] As the Directive was adopted on April 24, 2024, currently, the only available text is the proposal of the Directive: Proposal for a Directive of the European Parliament and the Council on improving working

can be used in employment procedures as well, for profiling candidates, headhunting on the labour market, and similar activities.[5]

In that sense, as it is pointed out in literature: "the evidence shows that the more aware employees are of the impending introduction of smart technology, artificial intelligence, robotics and algorithms in their workplaces, the lower their organisational commitment and career satisfaction, and the higher their turnover intentions, the tendency to depression and cynicism about the job. This does not make for the happy, harmonious, productive workplaces of the future that some envisage – and it has a lot to do with the underlying political-economic foundations not only of capitalism in its contemporary guise but capitalism as a historically specific mode of production more broadly" (Dinerstein & Pits, 2021, p. 41).

If we take the stance that the thread connecting different spheres and aspects of society is knowledge, then we should also take into account that "algorithms have risen to become one of the – if not the – central technology for creating, circulating, and evaluating knowledge in multiple societal arenas" (Jarke *et al.*, 2024, p. 7).

Bearing in mind everything said, the research is directed towards identifying the potential positive and negative aspects of the use of algorithmic management in the process of employment and labour relations. The basic hypothesis is that algorithms introduce significant innovations into the work process, which does not necessarily have to be negative in terms of the quality of working conditions and workers' rights. In order to use the potential of algorithms primarily for positive outcomes, it is necessary to look at the use of algorithms both through the lenses of traditional labour law guarantees, as well as through the holistic and integrative approach aimed at effectively preventing abuses that have been observed in practice so far.

The analysis that follows is based on the modest normative foundations of controlling algorithms in the world of labour, but also on the well-established basic principles of labour law and guarantees of decent work, including the right to equality and prohibition of discrimination. Concerning the mentioned, the key methods that shall be used are the conceptual analysis, normative method, as well as the case study of case law relevant to the use of algorithms in employment and especially the human-in-command approach.

2. (DIS)ADVANTAGES OF ALGORITHMS "EMPLOYING PEOPLE"

In order to assess the changes, both positive and negative, that introducing an algorithm can have in the employment process, we should, in the first place, briefly address the general principles and guarantees which labour law, at the international level, provides in this regard. Namely, when it comes to the hiring process, the goal of the labour law guarantees is to find a balance between the right and the freedom of the employer to choose the person it would consider best for the job in question and the goal to protect

conditions in platform work (Text with EEA relevance) {SEC(2021) 581 final} - {SWD(2021) 395 final} - {SWD(2021) 396 final} - {SWD(2021) 397 final}.

[5] See for detailed profiling analysis: Anrig, Browne & Gasson, 2008, pp. 65-87.

workers in the employment process. In that sense, it is considered that the employer, in the recruitment process, has the right to determine necessary prerequisites for the job and the conditions that the jobseeker must fulfil in order to be employed. Therefore, we could say that the employer first decides upon the conditions necessary for the job and then on the best candidate, from the ones who have applied for the job in question. However, such freedom is not without limitations, the crucial one being the principle of equality and prohibition of discrimination. Namely, the general rule is that it is prohibited to, in any way, make an (unjustified) distinction between job seekers on the basis of one or multiple personal grounds. In other words, it is allowed for the employer to make a distinction based on professional qualifications, such as qualifications, work experience, knowledge and skills while making a difference is forbidden based on personal grounds. An exception to this rule can be found in cases where a certain personal ground or grounds are considered a real and decisive condition for performing a certain job, i.e., are a business necessity.[6]

So, the process of hiring is a process shaped by vertical inequality which bears many risks, perhaps the most emphasized being the risk of discrimination, but also other risks in terms of violations and abuse of rights (and power). That is also the context in which many novelties, including digitalization and specifically algorithms, as a new form of automation, are being introduced. Analysis of advantages and disadvantages in this regard also helps us in further understanding the issue of protecting the workers, which is the goal of labour law, in the context where algorithms are introduced.

In that sense, we would like to address the advantages that introducing algorithms in the recruitment process can have.[7] Namely, the use of algorithms is present even in, as we decide to call them, professional social networks or hiring platforms, out of which perhaps the most popular is LinkedIn, which implements algorithmic decision-making in terms of creating predictive analytics. Even networks of not primarily professional character, such as Facebook, can also include job advertisements, and often such algorithms exclude certain groups, such as older potential jobseekers (Kim & Scott, 2018). Furthermore, the algorithmic tools that organisations use often include "CV and resume screening, telephone, or video interviews, providing an algorithmic evaluation", all of which are used before the "face-to-face interview" (Köchling & Wehner, 2020, pp. 832-834). In other words, as the International Labour Organization points out, algorithms conduct the so-called "workers' profiling" by certain parameters, which may manifest the bias introduced when constructing such parameters (ILO, 2022, p. 21).

The two key positive points we see, when it comes to using algorithms in the recruitment process, refer to efficiency and impartiality. When it comes to efficiency, it is important to also put this issue in a certain context. Namely, it is true that, especially in the last couple of years, particular attention has been devoted to the recruitment process, and human resources management is gaining more and more attention in workplaces,

[6] For more in this regard, see: Kovačević, 2021, pp. 564–669.

[7] In that sense, we use the term recruitment as a wider term that includes recruitment in terms of advertising the jobs and taking the first step in finding the best candidate, while it also includes the candidate selection.

as well as legal theory.[8] With the flexibilization of work in different senses, with remote work becoming the "new reality", especially after the COVID-19 pandemic, jobs are becoming more accessible to a greater number of job seekers, which leads to creating a highly competitive hiring process.[9] When it comes to highly valued and more complex and responsible jobs, the number of the jobseekers that apply can be quite large, while testing them, from the moment of reading the CV-s, through numerous "stages" of testing, by written tests, interviews and so on, can require a lot of time and effort being dedicated to each and every candidate. In that sense, algorithms can be a great *tool* which leads to greater efficiency, so it is considered that "the major driving forces for algorithmic decision-making are savings in both costs and time, minimizing risks, enhancing productivity, and increasing certainty in decision-making" (Köchling & Wehner, 2020, p. 796)[10]. What is more, "software algorithms can help interpret data or draw conclusions about a particular problem that can be of great use in implementing ideas as part of innovation work behaviour" (Bogilović, 2023, p. 51).

To this we add the discussion on the risk of discrimination in the recruitment process – "given the growing awareness of algorithmic discrimination, the politics of digital technologies are also increasingly being acknowledged as a serious societal challenge" (Jarke *et al.*, 2024, p. 21). It is often emphasized that perhaps the greatest step forward in introducing algorithms in the recruitment process refers to, if not eliminating, then at least reducing bias, stereotypes and prejudices based on such stereotypes, which are the root causes of discrimination in employment (Díaz-Rodríguez *et al*., 2023, p. 2). There is an understanding that algorithms cannot be biased as they are "only mathematics" that collect and process data. Therefore, introducing a digital system, the algorithm is praised as a way to move past the "human imperfections", as human minds think subjectively and are often coloured by learned patterns of thinking and acting that include bias towards anyone who is "different".[11] However, as it turns out, the mentioned cannot be looked at from a one-sided perspective, as algorithms also bear many risks.[12] The situation in practice has shown us that the use of algorithms does not necessarily mean

[8] Namely, algorithms bring not only more efficiency but also the sense and "promise" of efficiency. See: Heine, 2023, pp. 50–63.

[9] In relation to that, it is considered that three major developments in the world of work, which are closely connected are: automation, flexibilization and intensification of work. Kremer, Went & Engbersen, 2021, pp. 1–9.

[10] With the new technological developments, balancing the different interests while not putting question the principle of equality and non-discrimination, i.e., balancing the goals of fairness and "professional personalization" becomes extremely challenging.

[11] In that sense, we would like to emphasize, that, in order for discrimination to exist, it is not for the discriminatory intent to exist. When it comes to human bias, we can argue that such bias is a result of a reality that is necessarily distorted in a subjective perception of each human, often reflecting on the process of choosing the most suitable job seeker. Wimmer, 2022, pp. 30–75.

[12] In light of the developments "typical" of the 21st century, we can speak of the "renewed interest in a utopia that was also present in the period following the deep economic crisis of the 1970s: the dream that the dynamics of automation released by capitalist crisis create the potential to progressively liberate society from capitalist work". Dinerstein & Pits, 2021, p. 48.

that the recruitment process shall be impartial and objective. Sometimes, the use of algorithms can have quite the opposite effect, which the Amazon case, as perhaps one of the most media-covered cases in this regard, confirms.

Amazon has used an AI tool, an algorithm, as a recruitment tool with the goal of spotting potential jobseekers, whose CVs are to be graded from one to five stars. However, it turned out that this tool was not gender-neutral as it has put women who have applied for "typically male jobs", such as software engineer, in a worse position, i.e., has downgraded their CVs (Lavanchy, 2018).[13] So, the Amazon case has shown us that algorithms do not (always) find the "perfect match for the job", at least not without discriminating (Fritsch, 2021).

What is more, "algorithmic discrimination might create refined and highly intersectional categories which make the identification of a disadvantaged group linked to a protected category much more difficult" (MacKinnon, 2013, pp. 1029-1030). In order to understand the bias that an algorithm can have, we must look deeper into the way that the algorithms operate. A simplified procedure in this regard includes three steps: the input, or collecting data, then defining "parameters and metrics, machine learning functions, optimisation loops, analysis loops", and finally making a decision (Baiocco *et al.*, 2022, pp. 29-30). When discussing what are, metaphorically said, algorithms fed with, we are in fact asking ourselves what is the input data because algorithms learn from historical data as an example. Such was the case with Amazon, where the algorithm was also "fed" with some data, and as it turned out, it was data that showed male dominance and has, therefore, introduced the factor of being male as a factor of success. So, actually, Amazon used an algorithm with the purpose of screening the CVs of the jobseekers, while this algorithm only "repeated" the story which was the "story of hiring" in the company Amazon, and that is the story of giving preferences to male

[13] Regarding a, to the same extent different topic, as it is not a case regarding the employment sphere, it seems that Amazon is once again in the spotlight as there is currently a lawsuit by the Federal Trade Commission (FTC) and 17 state attorneys against Amazon. In short, the ones who filed a lawsuit stated that "Amazon violates the law not because it is big, but because it engages in a course of exclusionary conduct that prevents current competitors from growing and new competitors from emerging. By stifling competition on price, product selection, and quality, and by preventing its current or future rivals from attracting a critical mass of shoppers and sellers, Amazon ensures that no current or future rival can threaten its dominance. Amazon's far-reaching schemes impact hundreds of billions of dollars in retail sales every year, touch hundreds of thousands of products sold by businesses big and small and affect over a hundred million shoppers". As part of its strategy, it is stated that Amazon has used algorithms to influence the market in ways that are the subject of the lawsuit. As part of its strategy, it is stated that Amazon has used algorithms to influence the market in ways that are the subject of the lawsuit. Federal Trade Commission, FTC Sues Amazon for Illegally Maintaining Monopoly Power -2023. Available at: https://www.ftc.gov/news-events/news/press-releases/2023/09/ftc-sues-amazon-illegally-maintaining-monopoly-power (1. 10. 2024).

In this context, a new study by researchers at Carnegie Mellon University sheds light on the effectiveness of automated pricing strategies used in e-commerce and their interactions in competitive markets, finding that pricing algorithms with seemingly benign aims can lead to higher prices in the market – specifically when others use more sophisticated pricing algorithms. For more interesting perspectives on this case, see: Algorithmic Pricing: Understanding the FTC's Case Against Amazon – 2023. Available at: https://www.cmu.edu/news/stories/archives/2023/october/algorithmic-pricing-understanding-the-ftcs-case-against-amazon (1. 10. 2024).

candidates in comparison to female.[14] Having that in mind, we should ask ourselves do algorithms, at first glance so neutral and, in fact, contribute to the growth of risk of discrimination (Todolí-Signes, 2021, pp. 433-451). And even if we consider it to be so, we must further ask ourselves whether algorithms are "the ones to blame", or should we, in fact, blame humans, which create and "feed" algorithms with information,

Having in mind the mentioned, i.e., the ups and downsides of including algorithms in the recruitment process, we shall take a glance at the legal sources that are relevant in this regard.

In 2022, the European Commission took the stance that there is "insufficient transparency regarding such automated monitoring and decision-making systems and people lack efficient access to remedies in the face of decisions taken or supported by such systems" (European Foundation for the Improvement of Living and Working Conditions, 2022). In that sense, we shall just mention the Platform Work Directive, which will be addressed in more detail in the second part of the paper. Namely, from the recruitment perspective, it is important to state that this directive "may represent a first attempt to regulate algorithmic management in a consistent framework, although it only covers workers mediated by digital labour platforms" (Baiocco *et al.*, 2022, pp. 29-30). As stated in the preamble of the Directive: "Algorithmic management is a relatively new and – apart from EU data protection rules – a largely unregulated phenomenon in the platform economy that poses challenges to both workers and the self-employed working through digital labour platforms". Also, article 6 of the Directive is dedicated to the issue of algorithmic management, and even though this precise article is primarily dedicated to platform workers, it is also relevant from the perspective of the recruitment process. Namely, it emphasizes the importance of using algorithms only for data relevant to the work performed, and by no means any personal data, such as the data on private conversations, health, psychological or emotional state.[15]

[14] Concerning the Amazon case, the following is stated in the literature: "The information that the algorithm 'sees' about individuals is a set of features, which may be less informative or not as representative for individuals belonging to minority groups (...) For instance, in the example above of Amazon's recruiting tool, most of the resumes belonged to males (majority group), while female applicants (minority group) were not representative. As a consequence, a prediction algorithm solely trained to maximize expected accuracy (or to minimize expected loss) of the training data, will lead to higher prediction errors for the minority group, as the prediction error decreases as more data is collected". Valera, 2021, p. 17.

[15] In that sense, we feel obliged to emphasize the many risks that introducing algorithms carries when it comes to personal data. Certainly, the issue of personal data is important as such, but also in terms of risks it carries when it comes to job seekers and employees. Requesting personal data from employees is often a "prerequisite" and sort of a "first step" when it comes to discrimination. Therefore, adopting the GDPR (Consolidated text: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), *Official Journal of the European Union* L 119, 04.05.2016) is of great importance when it comes to the world of work in general and especially when it comes to algorithms in the world of work. Namely, this regulation introduces the principles of equality, transparency and fairness when it comes to processing personal data (Article 5 of the GDPR). In that sense, ILO also recognizes the importance of Regulation when it comes to employees' personal data. See: Hendricks, 2022. Protection of workers' personal data: General principles, International Labour Organization Working Papers.

What could we conclude when it comes to the use of algorithms in the recruitment process? It is certain that digitalisation introduces disruption in the world of work and in that sense, in the recruitment process (Kocher, 2022, p. 4). That being said, whether we find this to be primarily positive or negative, the reality is that algorithms are "making their way" into the labour market.[16] In other words, no matter how optimistic or pessimistic the view we have of the future, we cannot deny that algorithms are the future, as well as our present. It is also certain that taking any step in further development of positive aspects that algorithms bring to the recruitment process is not possible without seeing the negative sides as well. So, in order for algorithms not to be considered "black boxes" as they are, at times, referred to in theory, it is considered crucial to pay attention to the following three elements in algorithm management: *transparency, interpretability, and explainability* and start from that (Köchling & Wehner, 2020, p. 799).[17]

3. ALGORITHMIC MANAGEMENT – TRANSFORMING WORK RELATIONSHIPS AND REMOTE WORK

3.1 Algorithms in a Transforming Work Environment

If algorithmic management is considered about certain "classic" work tasks, one can certainly notice an evolution in their performance. In the past, work automation meant higher productivity, lower production costs, as well as the possibility of achieving better working conditions. Algorithmic management certainly provides all of these benefits. However, at the same time, new risks arise regarding workers' rights, since the pre-programmed work process depends on the data inputs of humans and can be used for purposes that are exclusively aimed at increasing profits and greater exploitation of workers, rather than improving the conditions in which work is performed. In the last decade, several problems have arisen related to the deterioration of the working conditions of workers who work using new technologies, although they perform tasks in the domain of "classic" jobs, such as providing services for the transportation of people and goods, courier services etc. Furthermore, certain aspects of the new technologies enable erasing the line between private and professional life, work and free time, practically in every occupation. Some of these problems could be directly related to algorithmic management.

Available at: https://www.ilo.org/legacy/english/intserv/working-papers/wp062/index.html (1. 10. 2024). However, even though years have passed since this regulation was adopted, the situation in practice shows us that employers are still "struggling" to implement the principles provided by the Regulation. European Commission, Can my Employer Require me to give my Consent to Use my Personal Data? n. d. Available at: https://commission.europa.eu/law/law-topic/data-protection/reform/rights-citizens/how-my-personal-data-protected/can-my-employer-require-me-give-my-consent-use-my-personal-data_en (1. 10. 2024).

[16] Even though digital platforms also existed before the COVID-19 pandemic, it seems that the pandemic period has changed so much in the world of work, including the increase in the number of digital platforms and in the development of the role they play in the world of work. Together with the digital platforms, algorithms started to gain more "popularity". Rani, Pesole & González Vázquez, 2024, pp. 5, 12.

[17] Precisely because of hiding many risks that are primarily related to privacy and data, but also other risks that are closely related to this issue, including the risk of discrimination, algorithms are referred to as "black boxes". For more in this regard, see: Wischmeyer, 2020, pp. 75–103.

Working time is one of the issues most threatened by the digitization of the work process. The possibility of constant electronic communication between the employer and the employee effectively reduced the free time of the employee and led to a continuous state of stand-by time (Reljanović & Misailović, 2021, pp. 414-416). It is not surprising that, as one of the consequences of this development of events, there is also the standardization of the "right to disconnect" in national labour laws (Reljanović & Misailović, 2021, pp. 414-416). Although Directive 2003/88/EC concerning certain aspects of the organisation of working time leaves no room for the existence of "inter-categories" and clearly distinguishes between what is meant by working time and what is free time (Maiso Fontecha, 2022, pp. 1-6), in practice this distinction is not always the clearest when it comes to specific jobs. In recent cases C-344/19 (D.J. vs. Radiotelevizija Slovenija, Judgment of the Court (Grand Chamber) of 9 March 2021) and C-580/19 (RJ v Stadt Offenbach am Main, Request for a preliminary ruling from the Verwaltungsgericht Darmstadt, Germany), Court of Justice of the European Union (CJEU) declared that "stand-by time must be regarded as working time in its entirety when the constraints imposed on the person during stand-by time significantly affect that person's ability to freely manage his time during which his professional services are not required" (Hadžić, 2021; CJEU C-344/19, para. 36-38). Furthermore, "a period of stand-by time must be classified as working time automatically when a person is obliged to remain at his/her workplace and the disposal of his/her employer" (Hadžić, 2021). This raises a few important questions regarding algorithmic management and working duties. Namely, if the working time of the delivery person is managed by the algorithm in the usual way – the algorithm "decides" in which order it will assign existing requests for delivery to currently free couriers (on stand-by), the question arises whether the time that passes between two deliveries must be included in the working time. If the answer is positive, and based on the analysis of the CJEU's decisions it will be so, we come to the conclusion that algorithmic decision-making can significantly affect working time restrictions and workers' free time. This is because the worker is sometimes on stand-by time for several hours. The worker can certainly be excluded from the platform, if the platform itself allows it. This issue was resolved by adopting a special Directive regulating the work of platform workers. In countries outside the EU, especially those that ignore the existence of platform work in their legislation, this question is still open. In such a case, the worker can choose to significantly extend working hours, but without being paid for it, because payment is made according to the number of deliveries, and not according to the total time spent available for making deliveries. If the worker goes offline, there is a risk of discriminatory treatment due to insufficient hours spent on the platform, while he/she/they also cannot earn in pay-for-performance modes of engagement. In this way, the predictability of working hours, the limitation of the number of working hours, as well as the payment in accordance with the work performed, are deeply explored and extended beyond legislative limits. The business risk, i.e. the number of deliveries that will be available through the platform, in this way is completely transferred to the worker – the platform practically regulates workers' working hours, but does not respect any of the legal restrictions, because it claims that the worker is in a business relationship and not in an employment relationship.

Automated algorithmic decision-making can lead to discrimination against a certain group of workers. This happens both in cases where the algorithm is based on discriminatory assumptions and in cases where indirect discrimination occurs, i.e. there is an unjustified treatment of workers using seemingly neutral criteria. One of the examples of such illegal behaviour was created by the application of selective rules for assigning work tasks in a company that deals with the delivery of goods in Serbia.[18] Namely, this company, using shortcomings in labour legislation, hires couriers in two modalities. The first is through "false self-employment", and the second is through the contracts on business cooperation with certain companies (not registered as temporary work agencies) that hire couriers who work exclusively for the platform. The first group of workers is paid according to performance (per delivery), while the second has a fixed salary regardless of the number of deliveries. While in the first category, there are mostly workers from Serbia, in the second, as a rule, there are workers who came from abroad. According to domestic couriers, the company's algorithm is set to favour workers coming from "partner companies" because they are economically more profitable – they are paid the same regardless of the number of deliveries they make. The protesting workers, however, perceived this problem as a problem of discrimination based on nationality – which is a consequence of the connection between the modality of work engagement and citizenship, that is, the country of origin of the worker. Thus, algorithmic management is used to increase profits (which, of course, is also illegal), but it also results in direct discrimination of workers according to labour law status, i.e. indirect discrimination according to the country of origin. However, this case should be viewed from another angle – foreign workers who are "favoured" in the described way do not benefit from it. On the contrary, they are also discriminated against because their work is worth significantly less (calculated according to individual deliveries, i.e. delivered kilometres) than the work of workers who are "falsely self-employed". In this way, multiple intertwined layers of discrimination of all workers were created, due to the fact that the algorithm for assigning jobs was written in a way that violates the equal treatment of delivery workers. There are, of course, other ways to discriminate through algorithms – for example, the algorithms that calculate salary can be set to deny certain types of bonuses to workers who have used their legal rights to leave work – for sick leave, childcare, annual leave, etc. It can be said that in fact, any automated "inference" and "decision making" that produces a certain type of inequality for which there is no and cannot be a rational and objective justification is discriminatory, regardless of the fact that it is supposedly "objective". Machine decision-making does not affect the existence of discrimination, as well as the employer's objective responsibility for it. In situations where decision-making software was intentionally fed with data that led to discrimination, the scope of employers' responsibility only expands – but it exists in any case.

Excessive supervision of workers in the work process is primarily reflected in their location monitoring. This mode is typical for courier services, as well as all workers who

[18] See: Popović, P. V. 2024. Domaći „protiv" stranih radnika dostave: Šta muči koga, a šta kaže Wolt Available at: https://n1info.rs/biznis/domaci-protiv-stranih-radnika-dostave-sta-muci-koga-a-sta-kaze-wolt/ (1. 10. 2024); Kompanija Wolt uvela diskriminatorna pravila za strane radnike – 2024. Available at: https://www.masina.rs/kompanija-wolt-uvela-diskriminatorna-pravila-za-strane-radnike/ (1. 10. 2024).

perform work tasks in the field and outside the employer's premises. Workers are subjected to a regime in which the software calculates the shortest/fastest route the worker must travel through the GPS, monitors his effective movement during the entire working time, and measures work efficiency and labour costs based on the distance travelled.[19] The main problem with this way of monitoring the work process is the lack of complete information for the software to process the current working conditions. For example, if there is a traffic jam or a car breakdown, there is no way, without the involvement of the human factor, to correct the work efficiency of a certain worker based on circumstances beyond his/her/their control. If there is no such correction, and most often it does not exist, the specific work performance of the worker will appear significantly worse than it really is.

The efficiency of the work process determined by the software is not characteristic only of courier services. On the contrary, its use in the production and service sector is common and happening every day. So it happens that the software, using the data it is being "fed" with, calculates the speed of the production line in the factory, the number of manufactured units of goods per worker (or group of workers) that represents the working norm, as well as the number of contacts that online service providers can make during working hours. The problem with this type of management has the same roots as in the previous cases – the software does not consider factors that are the result of objective problems that may arise in the work process. The algorithm has only one task, which is devoid of judgment – to make the work process as efficient and cheap, as possible. In order to perform that task, it uses exclusively the data provided by the employer, i.e., the goals that the employer wants to achieve, without the possibility of reasoning whether these goals are realistically achievable. This can lead to a significant increase in the work pace that cannot be objectively achieved. Even more significant is the absence of subjective factors when arranging the work process. Algorithmic management does not recognize the fact that, for example, not all workers are present on the production line on a certain working day (for example, one is absent due to illness) – the algorithm will not adapt to new circumstances until a human adjusts it. If this does not happen, and as a rule it does not happen, it may happen that an impossible work norm is demanded of workers, as well as that the work process is organized according to ideal conditions that do not exist at that moment, and therefore cannot be performed in the way that the software has arranged it.

Algorithmic collection of data about workers may constitute a violation of the GDPR, especially its article 22, which refers to automated individual decision-making, including profiling. The existence of such practice is clear from the judgment of the Italian court in the "Foodinho" case when the platform was punished for violating Article 22 with a severe fine (Agosti *et al.*, 2023).

[19] Even GPS monitoring carried out for those purposes will be considered illegal from the point of view of violation of the right to protection of personal data and violation of the right to privacy of workers, if the worker has not been introduced to the details of monitoring and the way data is being processed, or if it is carried out with the actual aim of monitoring the activities and behavior of workers. See: Reljanović, 2020, p. 79.

Based on the previous problems, it is clear that in situations where the decision on the rights of workers is left exclusively to the program management, there will be a significant chance for potential violation of regulations. The main problem will be that the software decision-making method is automated and devoid of human supervision, which leads to the interpretation of circumstances in a way that does not respect parameters which are not part of the basic computer program that makes decisions. Thus, the algorithm can calculate that the worker is insufficiently efficient based on poor work results that are not in accordance with the set work norm and optimized work process, although in specific circumstances there were no pre-conditions set for the worker to perform work tasks in such a manner. This can lead to workers being sanctioned and even fired (Baiocco *et al*., 2022, pp. 16-17).

3.2. Algorithms in a Transformed Work Environment

Unlike "traditional" jobs, new digital jobs are exclusively tied to the latest technological advances. These are jobs that did not exist before and that developed only recently. They can be characterized by exceptional flexibility in the choice of employer, specific work tasks and work schedule ("freelance" type of work), but they can also be performed in "classic" forms of work (programming jobs that are performed based on an employment relationship in the employers' premises).

The supervision of workers in these jobs can be even more intensive than in traditional occupations. For example, there have been cases in which employees are constantly recorded by cameras on their computers, when recorded which websites they visited during working hours when the employer has access to their mobile phone listings, and even when special software records what the employee has typed on the keyboard while working. It goes without saying that these actions of the employer are prohibited in the vast majority of countries, primarily because the worker is seen as someone (or even something), who, during working hours (and even after regular working hours) is obliged to completely ignore any aspect of his/her/their private life. However, the boundaries between the right to monitor the work process and the right to privacy, which is one of the respective human rights and which the worker certainly retains at the workplace, are very clearly defined (Reljanović, 2020). Therefore, any automatic processing of data that can be considered personal data and/or part of the employee's private life is prohibited by the employer. Software that deals with the collection of such data must be limited to information that is relevant to the work tasks being performed at that moment – any overstepping of these limits can lead to a violation of the law, and even finding the person to be criminally responsible, in more serious cases. However, despite the obvious inherent limitations in monitoring the work process in this way, the over-surveillance of workers by algorithms persists in several employers.

Digital workers are also subject to the same rights violations as "traditional workers" described in the text above. This refers to cases of discrimination, excessive working hours and deciding on employment rights through algorithms, including breach of the right to privacy and collection of workers' personal data.

Another consequence of algorithmic management, which may not be as direct as previous ones, but indirectly affects the realization of workers' rights, is the separation, i.e., individualization of digital workers. Regardless of whether the work is done remotely or from the employer's premises, algorithmic management effectively affects the micro-division of jobs in ways that have not been recorded before. Workers do not have to be aware of the existence, number, or any other characteristics of other workers – this will usually happen with remote work. But even when working in the same space, algorithmic management aimed at micro-businesses (and micro-management) provides individualization that is (still) not possible in some "classic" professions. The direct consequence of this is not only the lack of awareness of the existence (and aspirations, positions, and working conditions) of other workers but also the lack of the possibility of joining together to achieve collective goals, in the traditional sense of the struggle for labour rights. Unionisation, as well as collective bargaining, seem mission impossible in such a highly individualized environment (Kim, 2023, pp. 18–20). Some authors also refer to the misuse of algorithms, when location data (cross-locations of multiple workers) is collected in order to create a profile which shows how much time these workers spend together (for example, delivery workers between tasks) in order to assess whether there is a danger of them unionising (De Stefano, 2018, p. 7).

4. "HUMAN TOUCH" IN ALGORITHMS ACTING IN THE WORLD OF WORK

Algorithms have made a lot of changes in the world of work – from the work organization to the perception of industrial relations (European Commission, n. d., Algorithmic management and digital monitoring of work). Having in mind the mentioned, both in terms of the recruitment process, but also work environments that are transforming and the ones that have already been transformed, we may draw some conclusions. The key conclusion in this regard is that the question that imposes itself is not whether or not we should introduce algorithms in employment, but in what way should algorithms be introduced, so that their positive sides become emphasized, and the negative sides, as much as possible, downsized.

Therefore, we must look at algorithms not as (completely) autonomous and not as a governing system, but as a tool, like any other tool that is used by individuals in recruitment.[20] Such opinion is confirmed in a judgement of the Supreme Court of Spain dealing with courier workers, from 2020, that sets the ground for further use of algorithms in the world of work. The labour dispute concerned a worker who started working in 2015, based on a service contract, as a self-employed person, for the company Glovo in Spain.[21]

[20] Certainly, "the use of algorithms to make decisions does pose some questions about the extent to which accounting professionals versus the algorithms can be held accountable for ultimate outcomes in business or on audits". Murphy & Feeney, 2023, p. 43.

[21] Decision of the Supreme Court of Spain: Tribunal Supremo, Sala de lo Social, 25. 9. 2020, STS 2924/2020 - ECLI:ES:TS:2020:2924. This company was founded in 2014 with the goal to provide delivery services with the help of computers and in the digital context, widely speaking. In other words, Glovo acts as a sort of commission agent, i.e., an intermediary between customers and the places and employers from where

In the further development of events, the plaintiff signed a contract with Glovo by which he was considered an economically dependent self-employed worker. Working for Glovo meant, i.e., that tasks were distributed either in an automated mode of distributing tasks (that could be rejected by the worker) or in a manual mode. Anyhow, the tasks are *distributed by an algorithm which has the goal to make the most cost-efficient combination in terms of performing the tasks*. The tasks could be rejected by the worker once already accepted and in such a case, the task would be reassigned to another worker. What is important to emphasize in this regard, when it comes to the worker in question, is that the remuneration which a worker receives is consisted of precise rates which were regulated in Annex 1 of the contract the worker had, as well as the added sum based on miles crossed and the waiting time.

On the other hand, it is also important to have in mind within that, in the system Glovo applied, there were categories of beginner, junior and senior worker, and that not accepting a single order for more than three months could result in downgrade of the person in question. Having in mind the mentioned, the score for each worker was based on the following: the customers' score, the demonstrated efficiency in fulfilling tasks and the performing the tasks in the so-called "diamond hours", i.e., hours of the highest demand.[22] The said has put workers, so to say, in the state of constant competition in terms of performing the most demanding requests, i.e., working in the most demanding hours. In relation to the "working hours", or more precisely, the previously already accepted tasks, the grading system in the case at hand, "reduces" 0,3 points (out of the maximum five) to a worker that turned out not to be operational in the time slot that he/she/they previously reserved. However, the exception to this rule were the cases in which there was a justified reason for not performing the task and, in such cases, there was a procedure to communicate the mentioned.

Understanding the said context is of key relevance when it comes to dealing what specifically happened in the case at hand and how it has shed a (new) light on the use of algorithms in the world of work. On October 19, 2017 the plaintiff has sent a message to defendant about staying at home due to a fever, while in the next couple of days, the plaintiff has again texted about health problems which prevented him from performing work tasks, and each time has received a reply from the defendant that everything is all right. Then, on October 24 and 25, the plaintiff has returned to work, but has again, on October 27, written that he is not feeling well and is not capable to perform work. The response he has received from the defendant was delayed, and after that he was not regularly assigned tasks, his scores were degraded, and he was ultimately left without work.

The worker has filed a complaint stating that, due to the nature of work he performed, he was in a *de facto* employment relationship and that he was discriminated, and in that sense, subject to a discriminatory dismissal, based on health reasons. Glovo, as the defendant, referred to the freedom to provide services based on Treaty on the

---

the customers would like their delivery to be from. In order to perform such activities, Glovo uses a website and a mobile application.

[22] In that regard, the workers are free to use the route they consider best but are constantly located by a GPS located on their mobile phones.

Functioning of the EU (Articles 49 and 56 of the Consolidated versions of the Treaty on the Functioning of the European Union, 26. 10. 2012, Official Journal of the European Union, L 326/47-326/390), but also the right to freely chose a profession based on the Charter of Fundamental Rights of the EU (Articles 15 and 16 of the Charter of Fundamental Rights of the European Union, 18. 12. 2000, Official Journal of the European Union, C 364/1– 364/22), and asked the case to be referred to the CJEU for a preliminary ruling. However, the Spanish court refused such a request by the plaintiff.[23] So, the Spanish court took upon itself to determine whether this case actually encompassed the existence of an employment relationship, and in relation to that, the prohibition of the discriminatory dismissal. In other words, the opened question related to the existence and the degree of subordination based on which an employment relationship can be distinguished from self-employment. In that sense, the criteria that the Spanish court has taken into account refer to working under a certain brand name (and reputation), then the question of whether the digital platform in fact represents a means of production rather than just an intermediary (which Glovo does), while digital rating, i.e., the surveillance the employees is also a relevant factor that should be considered when addressing this issue. Having in mind all the facts on the case, the Court concluded that the plaintiff was in fact in an employment relationship with Glovo. In that regard, the Court stated that Glovo is a delivery and not only and intermediary company and has explained this stance by relying on various facts, including: the fact that the company makes all the commercial decisions[24], the fact that the workers were not, in any way, included and relevant in the agreements between Glovo and the business that the goods are delivered from, as well as the fact that the workers were not paid directly by the customers, but by the platform (Glovo). By taking the stance that in this case there is an employment relation, the Court has put an end, at least to some extent, to dilemmas and disputes which were opened in previous years and cases and has also widened the scope the understanding the concept of employee and employment relationship in a "new" context.

From the algorithmic perspective, this case is greatly relevant as it has addressed the risks that "participation" of algorithms in employment bears, by recognizing the failure of the algorithm to take into account the justified (health) reason for not performing the working tasks. Therefore, this case is considered a landmark case when it comes to the so-called *human-in-command approach*, which emphasizes the need to have a human who would look into more detail into the decisions made by an algorithm and would

[23] The Court took the stance that "it is debatable whether the defining notes of the contract of employment between a Glovo delivery rider and this company are fulfilled" and that in this context "there is no reasonable doubt as to the application of the law". Furthermore, the Court recalled the Reasoned Order of the CJEU of 22 April 2020, Case C 692/19, which dealt with the application of the Directive 2003/88/EC, and where the CJEU concluded that the national court should determine whether a relationship that exists with the service provider is in fact of subordination nature. Finally, by recalling this decision of the CJEU, the Court addressed the stance of the CJEU in the said case, which was such that no preliminary ruling was needed.

[24] In that sense, we would like to reiterate that the particularity of the employment relationship is manifested precisely in the fact that the employer bears the economic risk of business, which creates balance with the subordination, i.e., the fact that the employer has normative, controlling and disciplinary prerogatives.

present sort of the "higher instance" of control. In this sense, the terms we would like to draw your attention to are human-on-the-loop and human-in-command. While the first refers to human intervention in all aspects of creating and functioning of the system, the human-in-command approach refers more to the overseeing of the process and making a decision in the final instance. In other words, the final assessment would be the one made by a human, while the algorithm is a tool.[25] In relation to the mentioned, we would also like to underline that European Trade Union Confederation (ETUC) has taken the stance that that AI innovations are not "*per se* good and do not *per se* deliver positive outcomes for society", while the human-in-command approach is of crucial importance in this sense (ETUC, 2020).

Here, when dealing with the human-in-command approach, we encounter something that could be addressed as "innovation paradox", where we have a constant development from a technological point of view, and still, it is only in this development, where we see the need for a "human touch". In other words, it turns out that the more knowledge technology has, the more we recognize the need to have "faith" in human knowledge in terms of commanding the technology, i.e., algorithms (Adams-Prassl, 2019, p. 2). In relation to human-in-command approach, i.e., "controlling the algorithms" we would like to emphasize the importance of labour legislation or recognizing algorithms in labour legislation, as a first step in addressing the risks they bear in the world of work. The second step refers to introducing this, human-in-command approach in legislation, and recognizing the risks that can be prevented or at least reduced with the application of this approach. Application of this approach is relevant in relation to different labour law rights and guarantees, starting from the recruitment procedure, up until dismissals, individual and collective. When it comes to the recruitment process, without introducing the human-in-command approach, we run the risk of discrimination. Therefore, "subsequently, employers can disqualify high-quality candidates over minor and unimportant features that are detected by machine algorithms" (Špadina, 2023, p. 177). Furthermore, it can be stated that "human evaluation of shortlisted candidates during the interview phase is crucial to ensure a human review of machine-based decisions on the initial vetting of job applications" (Špadina, 2023, p. 177).

It is interesting that the Directive in the preamble deals with the issue of algorithmic management, focusing on the importance of transparency and accountability. Certainly, achieving such goals is not possible without a human-in-command approach. Special attention to this issue is dedicated to Articles 7 and 8 of the Directive, which deal with human monitoring of automated systems, and stipulate the need for a human review of decisions made by an algorithm. Certainly, the person "in charge of the algorithm" must have the adequate competence to assess the decision made by an algorithm", and, in our understanding, the knowledge of the person must be such that it entails the legal, as well as the technological aspects. Also, the Directive stipulates the right of the platform

[25] In a strict sense of a word, in a scenario in which the decision is made by a human, we cannot speak of the algorithm decision-making, but rather of algorithms as tools helping humans to make decisions. What is more, it is especially important that such a decision was made in an employment law context, and the case which included multiple layers of complexity.

worker to request information which would clarify the facts and circumstances that have influenced the decision that affects the working conditions of a (platform) worker. Furthermore, "where the explanation obtained is not satisfactory or where platform workers consider their rights infringed, they also have the right to request the digital labour platform to review the decision and to obtain a substantiated reply within a week" (Article 8 Paragraph 3 of the Directive). In relation to this, when it comes to the human-in-command approach, of relevance is also Article 9 of the Directive which stipulates the necessity of the digital platforms to inform and consult workers' representatives, and if there are no representatives, the platform workers themselves. The goal is to introduce social dialogue (also) in the sphere of platform work and by that reduce the risks that algorithms and algorithmic management bear.[26]

Besides the mentioned, as we argued, the use of algorithms "includes the collection and processing of a huge amount of data, which raises questions regarding the protection of personal data and privacy" (Bagari & Franca, 2023, p. 142). While the right not to be subject to automated decision making, without the "human touch" is also regulated by Article 9 of the revised Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, as well as the Article 88 of the GDPR, the fear of abusing data by algorithms in the world of work remains. Therefore, the human-in-command approach can be also beneficial in this regard, i.e., in the aspect of reducing the risks of personal data breaches. "Negotiating the algorithm, should, therefore, become a central objective of social dialogue and action for employers' and workers' organisation" (De Stefano & Taes, 2023, pp. 21-36).

5. CONCLUSIONS

Algorithms are very much present in the world of work and we can no longer consider whether they can be avoided or their impact should be somehow limited. These questions could be more hypothetical and relate to historical context, i.e., the moments when the answer could be different. The introduction of algorithms into various spheres and aspects of life, including the world of work, brings a new kind of "enthusiasm" that is largely justified when we take into account all the positive innovations that the use of algorithms enabled or could provide in the future. On the other hand, the fear of algorithms is well-founded and justified, bearing in mind certain negative experiences in the last ten years. So, algorithms are neither good nor bad in themselves – the way they are used is good or bad.

[26] This article is without prejudice to existing information and consultation requirements under Directive 2002/14/EC. Article 10 – Persons performing platform work who do not have an employment relationship This provision ensures that the provisions on transparency, human monitoring and review of Articles 6, 7 and 8 – which relate to the processing of personal data by automated systems – also apply to persons performing platform work who do not have an employment contract or employment relationship, i.e. the genuine self-employed. This does not include the provisions on health and safety at work, which are specific to workers. This is without prejudice to the provisions of the Platforms-to-Business Regulation (2019/1150).

When used for the purposes of increasing efficiency, they can save a lot of time and energy for the employer, that is, result in the optimization of work processes in every segment where there is a need for automatic processing of large amounts of data. However, this processing must be based on lawful parameters and cannot lead to a violation of workers' rights or any other violation of regulations. As we have shown with practical examples, the usage of algorithms based on insufficiently precise data that the algorithm is being "fed" with, that is, the creation of a base for automatic decision-making that is not aligned with the basic principles of enjoying the labour rights and the human right to dignity, can lead to the appearance or the extension of illegal practices, both of those which are already present in the classic way of decision-making of the employer, as well as many new ones that are specifically related to decision-making by automatic information processing. Using algorithms to hide the direct link between the employer's actions and the violation of workers' rights is a naive construct that will not bring any advantage to unscrupulous employers. On the contrary, when algorithms are used incorrectly, the employer is objectively responsible for the damage that occurs, as well as for any other behavior at work and in connection with work that leads to the creation of damage to the employee. The objective responsibility of the employer in this case is not reduced due to the fact that the decision is made by some intangible electronic entity, because that entity is under the complete control of the employer, thus making it the only one responsible for the entity's performance and outcomes.

In order to prevent abuses of algorithmic decision-making, one should take into account bad practices from the past and objective and subjective difficulties that occurred in its application. In this sense, appropriate definitions of algorithms and algorithmic decision-making should be introduced into the labour law, and the concepts defined in this way should be determined in relation to the responsibilities of employers and the rights of the employees. As already emphasized, even without special normative interventions, the employers' responsibility is unquestionable. But if the employer can show that it did everything in its objective power to prevent some negative consequences from occurring, this will certainly be taken into account when determining responsibility for certain types of harmful actions towards workers (such as the case of indirect discrimination that was a result of the employer's unconscious actions without the intention to produce discriminatory results). That is why it is necessary to accept these modern concepts in the labour legislation as reality, and to clearly limit the domain of what is permitted from the domain of what is prohibited.

Also, the presence of the human (preventive and corrective) factor in decision-making and the transparency of the algorithms' application are two basic assumptions to ensure their lawful usage. Namely, everyone who is evaluated by the algorithm must have access to the parameters of their evaluation, as well as the possibility to influence final decisions regarding their work-related rights, through the appeal procedure. Human control over algorithms must therefore be expressed twice: as a predictive correction of the database on the basis of which the algorithm decides, and as a subsequent correction mechanism of the decision made by the algorithm when it is clear that it does not correspond to the letter of the law, i.e. that it is a consequence of the inability of the algorithm to take into account all relevant circumstances during the decision-making process. We see the advantages and disadvantages of algorithms, as well as the persons who manage algorithms through all of the

above. Which flaws or virtues will grow or decrease in the future, remains to be seen. At this moment, we need a human-in-command approach. However, the speed of changes in the world of work requires constant re-examination of every standpoint, including this one.

LIST OF REFERENCES

Monographs and Scholarly Articles

Adams-Prassl, J. 2019. What if Your Boss Was an Algorithm? The Rise of Artificial Intelligence at Work. *Comparative Labor Law & Policy Journal*, 41(1), pp. 123-146.

Agosti, C., Bronowicka, J., Polidoro, A. & Priori, G. 2023. *Exercising workers' rights in algorithmic management systems: Lessons learned from the Glovo-Foodinho digital labour platform case*. Brussels: European Trade Union Institute. https://doi.org/10.2139/ssrn.4606803

Anrig, B., Browne, W. & Gasson, M. 2008. The Role of Algorithms in Profiling. In: Hildebrandt, M. & Gutwirth, S. (eds.), *Profiling the European Citizen – Cross-Disciplinary Perspectives*. Berlin: Springer, pp. 65–87. https://doi.org/10.1007/978-1-4020-6914-7_4

Bagari, S. & Franca, V. 2023. EU Approach to the Use of Artificial Intelligence in Employment Relationships. In: Sarıipek, D. B. & Franca, V. (eds.), *Digital and Green Transitions: New Perspectives on Work Organization*. Bursa: DORA Basım-Yayın Dağıtım Ltd, pp. 137-160.

Baiocco, S., Macias, E., Rani, U. & Pesole, A. 2022. The Algorithmic Management of Work and its Implications in Different Contexts, *JRC Technical Report, JRC Working Papers Series on Labour, Education and Technology*, 2022/02, pp. 1-39.

Bogilović, S., 2023, "Innovative Work Behaviour in the Digital Age of Business", in: Sarıipek, D. B. & Franca, V. (eds.), *Digital and Green Transitions: New Perspectives on Work Organization*. Bursa: DORA Basım-Yayın Dağıtım Ltd.

De Stefano, V. & Taes, S. 2023. Algorithmic management and collective bargaining. *Transfer: European Review of Labour and Research*, 29(1), pp. 21-36. https://doi.org/10.1177/10242589221141055

De Stefano, V. 2018. Negotiating the algorithm: Automation, artificial intelligence and labour protection. *Employment Working Paper,* 246, Geneva: ILO. https://doi.org/10.2139/ssrn.3178233

Díaz-Rodríguez, N., Del Ser, J., Coeckelbergh, M., de Prado, M. L., Herrera-Viedma, E. & Herrera, F. 2023. Connecting the dots in trustworthy Artificial Intelligence: From AI principles, ethics, and key requirements to responsible AI systems and regulation. *Information Fusion*, 99, pp. 1-24. https://doi.org/10.1016/j.inffus.2023.101896

Dinerstein, A. C. & Pits, F. H. 2021. *Futures Past and Present: On Automation, A World Beyond Work? (Society Now).* Leeds: Emerald Publishing Limited. https://doi.org/10.1108/978-1-78769-143-820201002

Heine, M. 2023. *Der Vorbehalt menschlicher Entscheidungen im Arbeitsverhältnis: Zum Einsatz «Künstlicher Intelligenz» in arbeitsrechtlichen Entscheidungsprozessen*. Berlin: Duncker & Humblot. https://doi.org/10.3790/978-3-428-58817-6

Jarke, J., Prietl, B., Egbert, S., Boeva, Y. & Heuer, H. 2024. Knowing in Algorithmic Regimes: An Introduction. In: Jarke, J., Prietl, B., Egbert, S., Boeva, Y., Heuer, H. & Arnold, M. (eds.),

Algorithmic Regimes: Methods, Interactions, and Politics. Amsterdam: Amsterdam University Press, pp. 7-34. https://doi.org/10.2307/jj.11895528.3

Kim, P. T. & Scott, S. 2018. Discrimination in Online Employment Recruiting. *Saint Louis University Law Journal*, 1(1), pp. 93–118.

Kim, P. 2023. Artificial Intelligence, Big Data, Algorithmic Management, and Labor Law. *Washington University in St. Louis Legal Studies Research Paper Series*, No. 23-06-01, pp. 1-23.

Köchling, A. & Wehner, M. C. 2020. Discriminated by an algorithm: a systematic review of discrimination and fairness by algorithmic decision-making in the context of HR recruitment and HR development. *Business Research*, 13(3), pp. 795-848. https://doi.org/10.1007/s40685-020-00134-w

Kocher, E. 2022. *Digital Work Platforms at the Interface of Labour Law – Regulating Market Organisers*. Oxford: Hart Publishing. https://doi.org/10.5040/9781509949885

Kovačević, Lj. 2021. *Zasnivanje radnog odnosa*. Beograd: Pravni fakultet Univerziteta u Beogradu.

Kremer, M., Went, R. & Engbersen, G. 2021. *Better Work: The Impact of Automation, Flexibilization and Intensification of Work*. Cham: Springer. https://doi.org/10.1007/978-3-030-78682-3

MacKinnon, C. A. 2013. Intersectionality as Method: A Note. *Intersectionality: Theorizing Power, Empowering Theory*, *Signs*, 38(4), pp. 1019-1030. https://doi.org/10.1086/669570

Maiso Fontecha, L. 2022. Working time: recent case law of the Court of Justice of the European Union. *ERA Forum*, 23, pp. 1–6. https://doi.org/10.1007/s12027-022-00708-7

Morondo Taramundi, D. 2022. Discrimination by machine-based decisions: inputs and limits of anti-discrimination law. In: Custers B. & Fosch-Villaronga, E. (eds.), *Law and Artificial Intelligence: Regulating AI and Applying AI in Legal Practice*. Cham: Springer, pp. 73-85. https://doi.org/10.1007/978-94-6265-523-2_4

Murphy, B. & Feeney, O. 2023. AI, Data Analytics and the Professions. In: Lynn T., Conway, P. R. E. & van der Werff, L. (eds.), *The Future of Work: Challenges and Prospects for Organisations, Jobs and Workers*. Dublin: Palgrave Macmillan, pp. 35-51. https://doi.org/10.1007/978-3-031-31494-0_3

Oppl, S. & Stary, C. 2019. *Designing Digital Work: Concepts and Methods for Human-centered Digitization*. Cham: Palgrave Macmillan. https://doi.org/10.1007/978-3-030-12259-1

Reljanović, M. & Misailović, J. 2021. Radnopravni položaj digitalnih radnika – iskustva evropskih zemalja, *Strani pravni život*, 65(3), pp. 407-432. https://doi.org/10.5937/spz65-33727

Reljanović, M. 2020 Zaštita podataka o ličnosti u radnom odnosu. In: Prlja, D. & Andonović, S. (eds.), *Zaštita podataka o ličnosti u Srbiji*. Beograd: Institut za uporedno pravo, pp. 61-92.

Špadina, H. 2023. Legal aspects of artificial intelligence in the employment process. *Stanovištvo*, 61(2), pp. 167-181. https://doi.org/10.59954/stnv.546

Todolí-Signes, A. 2021. Making algorithms safe for workers: occupational risks associated with work managed by artificial intelligence. *Transfer: European Review of Labour and Research*, 27 (4), pp. 433–451. https://doi.org/10.1177/10242589211035040

Valera, I. 2021. Discrimination in Algorithmic Decision Making. In: Weber, U. (ed.), *Fundamental Questions*. Baden-Baden: Nomos Verlagsgesellschaft GmbH & Co. KG, pp. 15-26. https://doi.org/10.5771/9783748924869-15

Wimmer, M. 2022. *Algorithmusbasierte Entscheidungsfindung als Methode des diskriminierungsfreien Recruitings*. Baden-Baden : Nomos Verlagsgesellschaft. https://doi.org/10.5771/9783748932055

Wischmeyer, T. 2020. Artificial Intelligence and Transparency: Opening the Black Box. In: Wischmeyer, T. & Rademacher, T. (eds.), *Regulating Artificial Intelligence*. Cham: Springer, pp. 75–103. https://doi.org/10.1007/978-3-030-32361-5_4

Legal Sources

Charter of Fundamental Rights of the European Union, 18.12.2000, *Official Journal of the European Union*, C 364/1– 364/22.

CJEU, C-344/19, *D.J. vs. Radiotelevizija Slovenija*, Judgment of the Court (Grand Chamber) of 9 March 2021.

CJEU, C-580/19, *RJ v Stadt Offenbach am Main,* Request for a preliminary ruling from the Verwaltungsgericht Darmstadt (Germany).

Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, *European Treaty Series - No. 108,* Strasbourg, 28. 1. 1981.

Directive 2003/88/EC of the European Parliament and of the Council of 4 November 2003 concerning certain aspects of the organisation of working time, *Official Journal of the European Union L 299/9* of November 18, 2003.

Proposal for a Directive of the European Parliament and the Council on improving working conditions in platform work (Text with EEA relevance) *{SEC(2021) 581 final} - {SWD(2021) 395 final} - {SWD(2021) 396 final} - {SWD(2021) 397 final}*.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), *Official Journal of the European Union L 119*, 04.05.2016.

Treaty on the Functioning of the European Union, 26.10.2012, *Official Journal of the European Union, L 326/47-326/390*.

Supreme Court of Spain, Tribunal Supremo, Sala de lo Social, 25.09.2020, STS 2924/2020 - ECLI:ES:TS:2020:2924.

Internet and Other Sources

Algorithmic Pricing: Understanding the FTC's Case Against Amazon. 2023. Available at: https://www.cmu.edu/news/stories/archives/2023/october/algorithmic-pricing-understanding-the-ftcs-case-against-amazon (1. 10. 2024).

European Commission. n. d. Algorithmic management and digital monitoring of work . Available at: https://joint-research-centre.ec.europa.eu/scientific-activities-z/employment/algorithmic-management-and-digital-monitoring-work_en (1. 10. 2024).

European Commission. n. d. Can my Employer Require me to give my Consent to Use my Personal Data? Available at: https://commission.europa.eu/law/law-topic/

data-protection/reform/rights-citizens/how-my-personal-data-protected/can-my-employer-require-me-give-my-consent-use-my-personal-data_en (1. 10. 2024).
European Foundation for the Improvement of Living and Working Conditions - Algorithmic Management. 2022. Available at: https://www.eurofound.europa.eu/en/european-industrial-relations-dictionary/algorithmic-management (1. 10. 2024).
European Trade Union Confederation (ETUC). 2020. AI – Humans must be in command. Available at: https://www.etuc.org/en/document/ai-humans-must-be-command (1. 10. 2024).
Federal Trade Commission. 2023. FTC Sues Amazon for Illegally Maintaining Monopoly Power. Available at: https://www.ftc.gov/news-events/news/press-releases/2023/09/ftc-sues-amazon-illegally-maintaining-monopoly-power (1. 10. 2024).
Fritsch, C. 2021. *Algorithmen am Arbeitsplatz*. Available at: https://arbeitundtechnik.gpa.at/2021/05/26/algorithmen-am-arbeitsplatz/ (1. 10. 2024).
Hadžić, D. 2021. European Union – When Is Stand-by Time Working Time? Available at: https://kpmg.com/xx/en/home/insights/2021/03/flash-alert-2021-085.html (1. 10. 2024).
Hendricks, F. 2022. Protection of workers' personal data: General principles, I*nternational Labour Organization Working Papers*. Available at: https://www.ilo.org/legacy/english/intserv/working-papers/wp062/index.html (1. 10. 2024).
International Labour Organization. 2022. The Algorithmic Management of work and its implications in different contexts. *Background paper*, 9/2022. Available at: https://www.ilo.org/media/372856/download (1. 10. 2024).
Kompanija Wolt uvela diskriminatorna pravila za strane radnike. 2024. Available at: https://www.masina.rs/kompanija-wolt-uvela-diskriminatorna-pravila-za-strane-radnike/ (1. 10. 2024).
Lavanchy, M. 2018. Amazon's sexist hiring algorithm could still be better than a human: Expecting algorithms to perform perfectly might be asking too much of ourselves. Available at: https://www.imd.org/research-knowledge/digital/articles/amazons-sexist-hiring-algorithm-could-still-be-better-than-a-human/ (1. 10. 2024).
Popović, P. V. 2024. Domaći „protiv" stranih radnika dostave: Šta muči koga, a šta kaže Wolt. Available at: https://n1info.rs/biznis/domaci-protiv-stranih-radnika-dostave-sta-muci-koga-a-sta-kaze-wolt/ (1. 10. 2024).
Rani, U., Pesole, A. & González Vázquez, I. 2024. Algorithmic Management practices in regular workplaces: case studies in logistics and healthcare. Available at: https://www.ilo.org/publications/algorithmic-management-practices-regular-workplaces-case-studies-logistics (1. 10. 2024).

UDC: 347.235:347.136 DOI: 10.56461/iup_rlrc.2024.5.ch21

Marijan ŠAKOTA*
Municipal Court in Osijek, Croatia

LIMITATIVE EFFECT OF ELECTRONIC COMMUNICATION IN THE LAND REGISTRY PROCEDURE

Before the Act on Amendments to the Land Registration Act entered into force, parties could submit proposal for entry of a registrable right to the land register court in several ways. The proposal for entry could be submitted electronically, either by email or the e-Citizens digital platform, by submitting it directly to the court registry or sending it by postal service. After the Act entered into force, such a proposal can be submitted only in electronic form through the information system, that is, through the Joint Information System of the Land Registry and Cadastre. In this case, the parties' communication with the court is conditioned by the submission of a proposal for entry to a notary public or a lawyer, who are mandatory users of electronic communication with the court. Before the Act entered into force, the parties could directly submit a proposal for entry to the court and request the registration of their right, which was the most common way of the proposal submission. The proposal used to be submitted in writing and its content was not significantly limited.

Keywords: land registry, proposal for entry, information system, electronic communication.

1. INTRODUCTION

The topic of this paper is the submission of a proposal for registration in the land register in electronic form as determined by the Act on Amendments to the Land Registration Act (AALRA/22).[1] The Act introduced significant changes to the Croatian legal system, its provisions exclude any other form of proposal submission, which was previously possible and allowed. As a consequence, this has a certain limitative effect for the applicants of registration in the land register because it is mandatory to submit a proposal in electronic form, with certain requirements related to signing it with a qualified electronic signature. Their right to submit proposals in any other form is no longer permitted. Imposed restrictions are being analysed in the scope of Article 6 of The European Convention on Human

* Senior Court Advisor – Specialist, ORCID: 0009-0007-7872-4139, e-mail: *marijansakota@gmail.com*

1 Act on Amendments to the Land Registration Act, *Legal Gazette*, no. 128/2022– AALRA/22.

Rights (the Convention) and case law of The European Court for Human Rights (ECtHR). An overview of the legal frame and subordinate legislation in the Croatian legal system that served as the basis for the implementation of electronic communication in the land registry procedure is given. The importance of the order of priority for registration is emphasized and the consequences that could occur in the case of a delay in the submission of the proposal, i.e., its connection to the principle of trust or public faith in the land register. The positive effect of electronic communication aims to modernize and accelerate the procedure itself and to abandon the current written form of interaction with the court. Since the new legislative solution excludes any other form of proposal submission, which was previously possible, the new legal frame brought up restrictions which can be connected to excessive formalism and even the individual's right to access the tribunal. Restrictions which collide with principal rights may be considered deficiencies in, almost, every legal system.

2. ELECTRONIC PROPOSAL IN THE SCOPE OF THE RIGHT OF ACCESS TO A COURT AND EXCESSIVE FORMALISM

With the entry into force of AALRA/22 applicants, who submit proposals for registration in the land register, have limitative right of submission regarding the prescribed form. The proposal for registration in the land registry now can only be submitted in electronic form through a notary public or a lawyer. Before the act came into force, applicants could submit a proposal for registration in several ways. The proposal could also be submitted electronically, either through an e-mail or the e-Citizens platform or by handing it directly to the court registry, even through a postal service provider. The submission itself, in this sense, is conditioned and limited by the amendments. It is conditional because the proposal must be submitted only through an intermediary and it is limited because the applicants can no longer directly submit the proposal to the court or using the e-Citizens platform. Notaries and lawyers are mandatory users of electronic communication with the court and it takes place through the Joint Information System of the Land Registry and Cadastre.[2] Considering that, the right of participants in the legal transaction of real estate to directly address the court is limited, due to the imposed indirect communication via intermediaries. The intermediaries in communication with the court are notaries public and lawyers, as the only authorized users of electronic communication.

In the scope of Article 6 of The Convention,[3] i.e. in the broader sense of the right of access to a court, it can be argued whether the right of access to a court is restricted by the new legislative form. The fact is that applicants are not allowed to submit their proposals directly to the court and the fact is that an intermediary is being introduced in communication between applicants and the court. On the other hand, this is the only legal possibility to execute the registrable rights. If the proposal is submitted directly to the land registry court it will be rejected due to the lack of procedural requirements.

[2] Republika Hrvatska – Ministarstvo pravosuđa, uprave i digitalne transformacije. Podnošenje e-prijedloga za upis u zemljišnu knjigu. Available at: https://mpudt.gov.hr/podnosenje-e-prijedloga-za-upis-u-zemljisnu-knjigu/14341 (10. 10. 2024).

[3] European Convention on Human Rights.

When it comes to the lack of procedural requirements it is well known that the ECtHR, and its case laws, underline the importance of the right of access to a court and this right can't be subordinate to any procedural requirements.[4] In Article 6, the word court is used in the term tribunal. The notaries public and lawyers can't be considered as a tribunal according to the case law of the ECtHR. They don't have the power to issue a binding decision[5] and they don't have full jurisdiction over the case[6] in the electronic communication with the land registry court, when they receive a proposal in a written form. They also don't have the ability to determine matters within their competence on the basis of rules of law, following proceedings conducted in the prescribed manner.[7]

Apart from restricting direct communication with the court, the formality of the proposal's content is also imposed. Before the act came into force the applicants could submit a proposal directly to the court, requesting the registration of their right. The proposal was submitted in a written form and its content was not significantly limited. The form as a presumption of the proposal's validity was not a requisite condition because it was stipulated that, due to the fact that the proposal was not submitted on the prescribed form, the proposal will not be rejected if it can be acted upon.[8] When formality is introduced into out-of-court proceedings and indirect communication is imposed, this can represent additional obstacles for the applicants in exercising their rights, and in some cases, additional costs.

The changes can be justified by efforts to modernize and accelerate the procedure itself and to abandon the current written form of interaction between the parties and the court, which is replaced by electronic communication. The question arises whether problems will occur when the parties' approach to the court is restricted by introducing an intermediator. This primarily refers to the content of the proposal, which will be drawn up by a notary public or a lawyer. In that case, can it be considered that the amendments lead to excessive formalism since the applicants can no longer directly submit a registration proposal whose content was not a requirement for its acceptance? The formalism can be, also, discussed due to the fact that before the amendments entered into force, the proposal could not be rejected only because it was not submitted in the prescribed form.

When it comes to the proposal submission, if the proposal is submitted directly to the court in a written form or using e-Citizens digital platform, even an e-mail, it will be rejected because it has to be submitted in electronic form by an intermediary. According to the ECtHR the right of access to a court is an inherent aspect of the safeguards enshrined in the European Convention on Human Rights, referring to the principles of the rule of law and the avoidance of arbitrary power which underlie much of the Convention.[9] In this sense, the fact is that electronic form is a procedural rule or requirement

[4] Council of Europe. 2023a. Excessive Formalism by Courts. Available at: https://rm.coe.int/thematic-factsheet-excessive-formalism-courts-eng-docx/1680aae7f4 (10. 10. 2024).

[5] ECtHR, Benthem v. the Netherlands, No. 8848/80, 23 October 1985, paras. 40 and 43.

[6] ECtHR, Galina Kostova v. Bulgaria, No. 36181/05, 12 November 2013, para. 59.

[7] ECtHR, Sramek v. Austria, No. 8790/79, 22 October 1984, para. 36.

[8] Art. 105 and 109 of the Land Registration Act, *Legal Gazette*, no. 63/2019.

[9] Council of Europe. 2023b. Implementation of ECHR judgments: new thematic factsheet on excessive formalism by courts. Available at: https://www.coe.int/en/web/human-rights-rule-of-law/-/

and it has to be submitted to an intermediary, who is not considered a tribunal. When a court rejects a proposal on the basis of procedural rules or requirements, the applicant's right to address the court can be considered restricted.

3. ELECTRONIC COMMUNICATION IN THE LAND REGISTRY PROCEDURE

Notaries public and lawyers in the legal transaction of real estate, as authorized persons in land registry procedure, were introduced back in 2013, when the Act on Amendments to the Land Registration Act (AALRA/13)[10] entered into force. That legislation introduced significant changes when it comes to electronic communication. The changes also related to the submission of entry proposals in electronic form (see Articles 9 and 33), which was previously not possible. They also referred to the implementation of registration based on an electronic document, delivery in electronic form, as well as the issuance of an electronic land register extract (see Articles 4, 15 and 31), and it is stipulated that land registers are kept in electronic form. It is prescribed that submission of a proposal for entry, electronic delivery of a decision, and issuance of an electronic land registry extract are tasks which could be performed by notaries public and lawyers as authorized users, through the information system. This legislation is also important because its provisions served as the basis for the introduction and establishment of an information system, through which electronic communication between the court and the parties takes place. This system is called the Joint Information System of Land Registers and Cadastre (JIS).[11] According to Art. 25 Paragraph 1 AALRA/13 it is an information system in which land register and cadastre data are stored, maintained and preserved, and it consists of data stored in the Land Registry Database, land register data and land cadastre data (LRDB).[12]

Based on Art. 34 AALRA/13, the Ordinance on technical and other conditions of electronic data processing in land registers was adopted (Ordinance/15),[13] and it entered into force on 2 November 2015. The mentioned regulation was applied only in procedures of electronic issuing of the verified land registry extracts at the request of a party through an authorized user.[14] Authorized users, in addition to notaries and lawyers, could also be legal entities with public authorities, which was later changed. Although the mentioned regulations introduced significant changes regarding electronic communication in land registry data processing, Ordinance/15 only prescribes the possibility of issuing a land registry extract in electronic form.

implementation-of-echr-judgments-new-thematic-factsheet-on-excessive-formalism-by-courts (10. 10. 2024).

[10] Act on Amendments to the Land Registration Act, *Legal Gazette*, no. 55/2013 – AALRA/13.

[11] Republika Hrvatska – Ministarstvo pravosuđa, uprave i digitalne transformacije. Uređena zemlja – katastar. Available at: https://oss.uredjenazemlja.hr/ (10. 10. 2024).

[12] Art. 25 Paragraph 1 of the AALRA/13.

[13] Ordinance on technical and other conditions of electronic data processing in land registers, *Legal Gazette*, no. 119/2015 – Ordinance/15.

[14] Art. 3 of Ordinance/15.

Submission of electronic proposal for entry was regulated by the subordinate legislation only in 2017, with the amendment of Ordinance/15, although the legislation act entered into force much earlier. The Ordinance on amendments to the Ordinance on technical and other conditions for electronic data processing in land registers (Ordinance on amendments/17),[15] prescribes the procedure, method and conditions for submission of electronic proposals to the land registry. Before that, notaries and lawyers were only authorized to issue electronic land registry extracts, as already stated.

For comparison, the Austrian legal system introduced electronic communication in 1990 as a means of communication with the parties and their counsel that would be equivalent to submissions in hard copy. In introducing this system, Austria was the first country in the world to establish Electronic Legal Communication.[16] The communication is taking place via the Austrian e-Justice digital platform and the platform allows online communication between the courts and the public prosecutors' offices on the one hand and the parties on the other, in the same way as in paper form. It can be used for all types of proceedings. There are no proceedings which must always be initiated online.[17] According to the § 83 of the Federal Law of 2 February 1955 on Land Registers (General Land Register Act 1955 – GBG. 1955),[18] it is allowed to submit a proposal in written form and even in the form of a court record. It can be seen that electronic communication doesn't have to exclude written nor other forms, such as the case with e-Citizens digital platform in Croatian legal system. Especially if that kind of a restriction can be seen as limiting principal rights guaranteed by the Convention. There's no explicit provision, like the one of Article 105 AALRA/22, demanding that a proposal must be submitted in electronic form via intermediary, although the communication is taking place via e-Justice. If a proposal is submitted in written form directly to the court, it should not be rejected due to the lack of procedural requirements.

3.1. Electronic Communication Through the Joint Information System

Electronic communication takes place through the JIS subsystem and personal user account. Proposals for entry must be signed by a qualified electronic signature[19] which is considered equal to a handwritten signature and a stamp, relating its legal effect. It was important to assimilate the effects of a handwritten signature and stamp with a qualified electronic signature as notaries public and lawyers, outside electronic communication,

[15] Ordinance on Amendments to the Ordinance on Technical and Other Conditions for Electronic Data Processing in Land Registers, *Legal Gazette*, no. 23/2017.

[16] Federal Ministry of Justice. Available at: https://www.bmj.gv.at/public.html (10. 10. 2024). See more: Austrian Federal Ministry of Justice. 2023. IT Applications in the Austrian Justice System. Available at: https://www.justiz.gv.at/file/2c94848b6ff7074f017493349cf54406.de.0/IT%20Applications%20in%20the%20Austrian%20Justice%20System%20Stand%2007.09.2023.pdf?forcedownload=true (10. 10. 2024).

[17] E-justice Europa. Online processing of cases and e-communication with courts. Available at https://e-justice.europa.eu/content_automatic_processing-280-at-en.do?member=1 (10. 10. 2024).

[18] Federal Law Consolidated: Complete Legal Provision for the General Land Register Act 1955, Version of 30.10.2024 (Bundesrecht konsolidiert: Gesamte Rechtsvorschrift für Allgemeines Grundbuchsgesetz 1955, Fassung vom 30.10.2024). Available at: https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10001941 (10. 10. 2024).

[19] Art. 12 Paragraph 1 of the Ordinance.

use a handwritten signature and stamp. This is their legal obligation since their signature and seal are evidence of the document's authenticity and the authenticity of the statements they draw up or the duty they carry out.[20] The signing of documents and statements by electronic signature in the notary public service, still, represents an exception because this method of signature can be used only when pursuant to a separate law.[21] Considering the lawyer's practice, such restriction is not regulated.[22] The reason for this lies in the specific elements of the public service they carry out, which gives them different authorities when it comes to drawing up documents.

Communication takes place through a personal user account assigned by the administrator. In this case, the administrator is the competent ministry and the request for creating a personal user account is submitted through the Chamber of Notaries or the Chamber of Advocates.

The Ordinance on electronic data processing of users and authorized users of the land registers (Ordinance)[23] is currently in force. Its provisions stipulate that land registry extracts, which used to be issued exclusively by the land registry court, can be issued by notaries public and lawyers. In that matter, a part of the data-related affairs in the land registry was transmitted to extrajudicial services. Likewise, the possibility of submitting proposals in electronic form is prescribed (see Article 27 and Article 105 of the LRA).

The submission of the proposal in electronic form was introduced into the legal system on 15 March 2017, when the Ordinance on Amendments/17 entered into force. The proposals submission form and the procedure conducted by notaries public and lawyers, when they receive a proposal, have not changed significantly. The applicants shall submit their proposals and the documents based on which registration is requested to a notary public or to a lawyer in written form. They shall convert them in electronic form by scanning, verify all important facts relevant to the registration, draw up the proposal for registration, sign the proposal and all the attached documents with a qualified electronic signature and deliver them to the Land Registry Court. The time of the proposal's receipt shall be considered to be the time when it is received in the recipient's information system, i.e., when it is recorded on the recipient's server.

4. PROPOSAL SUBMISSION AND DELIVERY

The proposal and all attachments based on which the registration is requested must be converted into electronic form by scanning and signed with a qualified electronic signature, even those documents that have already been prepared in electronic form.[24] A

[20] Art. 12 The Attorneys Act, *Legal Gazette*, no. 9/1994, 117/2008, 50/2009, 75/2009, 18/2011, 126/2021 – AA and Art. 44 of the Notaries Public Act, Legal Gazette, no. 78/1993, 29/1994, 162/1998, 16/2007, 75/2009, 120/2016, 57/2022 – NPA.

[21] Art. 18 Paragraph 11 of the NPA.

[22] Art. 12 Paragraph 1 of the AA.

[23] Ordinance on Electronic Data Processing of Users and Authorized Users of the Land Registers, Legal Gazette, no. 108/2019 – Ordinance.

[24] Art. 12 of the Ordinance.

qualified electronic signature means an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures.[25] A qualified signature creation device represents the appropriate computer equipment and supporting programs used to create an electronic signature, while a qualified certificate is related to the issuer of such a signature, which must meet certain requirements.

Entry proposals must be signed, as well as all documents based on which the registration is requested, whether they are official or private documents. The legal effects of an electronic signature are equal to a handwritten signature, and a document signed with an electronic signature has the same provable value as a private document signed by hand.[26]

It is considered that the proposal is received at the land registry court when it is registered on the recipient's server, which records the day, month, year, hour and minute of the proposal's arrival.[27] The mentioned indications are important because of the order of priority that determines the order in which the entry in the land register will be carried out. Those indications are, also, rendered visible (by lead seal) in the land registry file and they show the date and time when the proposal was received by the land registry court, and the number of the diary of land registry submissions under which it was received (diary number).[28] In this way, the publicity function of land registers is realized because it immediately makes visible and publicly available the fact that a proposal for the entry of certain content has been received.

Actions that precede sending the proposal and recording it on the land registry court's server greatly affect the time that can be considered proposal's reception. A server is a computer that serves as a data source for other terminals or computers or an organization or institution that provides a server on which a network site is set up.[29] This central computer provides files to terminals directly connected to it or is a network server accessed by client devices.[30] In this case, the server would be the competent ministry, that is JIS through which the proposal is submitted. The relevant moment that is considered the receipt of a proposal is the registration of the proposal on the server of the Land Registry Court. The procedure takes place through the JIS, as already mentioned, which notaries and lawyers access through their user accounts.

The proposal submission process itself consists of several time-separated actions that, in addition to human action, are also exposed to the action of information technology. Before the entry into force of AALRA/22, when parties were able to submit

[25] Art. 3 Paragraph 12 of the Regulation (EU) no. 910/2014 of the European Parliament and the Council of 23 July 2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market and repealing Directive 1999/93/EC, *Official Journal*, no. L 257/73 – Regulation (EU) no. 910/2014.

[26] Art. 25 of the Regulation (EU) no. 910/2014.

[27] Art. 13 of the Ordinance and Art. 108, paragraph 2 LRA/19.

[28] Art. 108 of the LRA/19.

[29] Struna – Hrvatsko strukovno nazivlje. Poslužitelj. Available at: http://struna.ihjj.hr/naziv/posluzitelj/48899/ (10. 10. 2024).

[30] Struna – Hrvatsko strukovno nazivlje.

motions directly to the court, there was less danger of errors in the receipt of proposals, which led to errors in determining priority order and execution of registration. Each proposal for registration would be received immediately, with an indication of the date and exact time of receipt, and a seal would be immediately entered in the land register. Such errors could lead to a violation of the principles of completeness and truthfulness of land registers. The state is directly responsible for the damage caused by the violation of these principles.

5. ORDER OF PRIORITY AND PRINCIPLE OF PUBLIC FAITH – PUBLIC TRUST

As already stated, the order of priority in the land registry procedure plays a very important role because it is an institute without which the land registry system would lose its purpose and meaning in the legal transaction of real estate. In all regular and special land registry procedures, the decisions that are made take into consideration the priority order of received proposals and executed entries, in order to determine all decisive facts and circumstances related to the proposal's admissibility and registrable rights, which is especially important for legal effects which occur after the registration. The impact of legal effects is determined according to the date and time when the proposal is received, and the order of priority is also determined according to the date and time of receipt. The priority order implies a strict chronological order of submitted proposals. The proposal which has been received first, according to the lead seal, will be registered first.

The order of priority, that is, its role, is directly linked to the principle of trust or public faith in land registers. This principle is two-sided and its constituent parts are: the principle of truthfulness and the principle of completeness of the land register. Both principles are included in the principle of protection of trust or public faith in land registers. The basis for the application of the principle is the provisions of the Act on Ownership and Other Real Properties (AO).[31] The direct application of the principle of trust is made possible by the provision of Article 7 of the LRA/96, which stipulates that the land register is public.[32] This implies that everyone can view the data of the land registry, regardless of whether or not there is a legal interest, that is, that the entered data is not secret, nor that there is a restriction or protection of this data when it comes to their use in legal transactions.

As it can be concluded, the principle of truthfulness is related to the correctness of the owner's information that has been registered, and it contains a rebuttable presumption that all the information is true. The principle of completeness implies that all registerable rights and all facts relating to real estate are entered in the land register, that is, that there is no right or fact if they are not registered. This principle also contains a

[31] Art. 122, 123 and 124 of the Act on Ownership and Other Real Properties, *Legal Gazette*, no. 91/1996, 68/1998, 137/1999, 22/2000, 73/2000, 129/2000, 114/2001, 79/2006, 141/2006, 146/2008, 38/2009, 153/2009, 143/2012, 152/2014, 81/2015, 94/2017– AO.

[32] Art. 7 Paragraph 1 LRA/96, idem Art. 7 Paragraph 1 LRA/19.

rebuttable presumption that what is not registered does not exist, that is, that the actual condition of the real estate is equal to what is registered in the land register. Considering that the order of priority directly affects the order in which the registrations will be carried out, it also directly affects the legal effects that will occur after the registrations are executed. For this reason, the time of receipt of the electronic proposal for registration is extremely important, and the introduction of an intermediary in the proposal submission process can affect not only the order in which the registration will be carried out but also the legal effects that will occur.

Under the provision of Article 122 AO, it can be understood that *bona fides* is prerequisites when the legal action of acquisition of real estate is being made. Such action represents a real contract and it can be concluded that protection is limited to cases of derivative acquisition *inter vivos*.[33] As some author says,[34] the scope of protection is limited to the cases of derivate acquisition and this circumstance is particularly strongly articulated under the *Grundbuch* model, where the protection prerequisite is the acquisition of a right based on a legal action.

6. CONCLUSION

Electronic communication in the land registry procedure has brought up certain restrictions in Croatian legal system. Excluding any other form of proposal submission and introducing an intermediary in non-litigation procedure have certain impact on the principle right of an individual to directly addresses the court. In the scope of Article 6 of the Convention, it can be argued whether the right of access to tribunal was being violated. Applicants can no longer submit the proposal directly to the court and if they do so, their proposal will be rejected due to the lack of procedural requirements, i.e., prescribed method and form. According to the previous legal solution, proposals submission in electronic form was also possible through the e-Citizens digital platform, which is no longer the case. *De lege ferenda*, it would be useful to expand the method of proposals submission, in order to enable the parties to directly address the court. In that sense the right of access to tribunal would be respected and excessive formalism would be avoided, if we also take into consideration other legal systems, e.g., Austrian. *De lege lata*, the submission is limited and conditioned by the participation of intermediaries who perform public service. This method of submission can lead to a delay, which directly affects the visibility of the lead seal in the land registry file. The visibility of the lead seal affects the priority order of registration and the legal effects of the registration. The process of submitting a proposal to the mediator and delivering it to the court consists of several actions separated in time, and they are subject to human action, as well as the action of information technology. Such actions may cause a delay in the submission and recording of the receipt on the court server, which ultimately leads to a delay in the registration and legal effects.

[33] Blajer, P. A. 2023. On the principle of public faith of land registers in a comparative context. *European Property Law Journal*, 12(2-3), 2023, pp. 79-125.

[34] Blajer, pp. 89 *et seq*.

LIST OF REFERENCES

Act on Amendments to the Land Registration Act, *Legal Gazette*, no. 128/2022.

Act on Amendments to the Land Registration Act, *Legal Gazette*, no. 55/2013.

Act on Ownership and Other Real Properties, *Legal Gazette*, no. 91/1996, 68/1998, 137/1999, 22/2000, 73/2000, 129/2000, 114/2001, 79/2006, 141/2006, 146/2008, 38/2009, 153/2009, 143/2012, 152/2014, 81/2015, 94/2017.

Act on Non-litigation Procedures, *Legal Gazette*, no. 59/2023.

Austrian Federal Ministry of Justice. 2023. IT Applications in the Austrian Justice System. Available at: https://www.justiz.gv.at/file/2c94848b6ff7074f017493349cf54406.de.0/IT%20Applications%20in%20the%20Austrian%20Justice%20System%20Stand%2007.09.2023.pdf?forcedownload=true (10. 10. 2024).

Blajer, P. A. 2023. On the principle of public faith of land registers in a comparative context. *European Property Law Journal*, 12(2-3), 2023, pp. 79-125. https://doi.org/10.1515/eplj-2023-0005

Council of Europe. 2023a. Excessive Formalism by Courts. Available at: https://rm.coe.int/thematic-factsheet-excessive-formalism-courts-eng-docx/1680aae7f4 (10. 10. 2024).

Council of Europe. 2023b. Implementation of ECHR judgments: new thematic factsheet on excessive formalism by courts. Available at: https://www.coe.int/en/web/human-rights-rule-of-law/-/implementation-of-echr-judgments-new-thematic-factsheet-on-excessive-formalism-by-courts (10. 10. 2024).

Dika, M. 2009. "Izvanparnična" i koncilijacijska funkcija javnih bilježnika – *de lege lata* i *de lege ferenda*. *Zbornik Pravnog fakulteta u Zagrebu*, 59(6), pp. 1153-1177.

ECtHR, Benthem v. the Netherlands, No. 8848/80, 23th of October 1985.

ECtHR, Galina Kostova v. Bulgaria, No. 36181/05, 12th of November 2013.

ECtHR, Sramek v. Austria, No. 8790/79, 22th of October 1984

E-justice Europa. Online processing of cases and e-communication with courts. Available at https://e-justice.europa.eu/content_automatic_processing-280-at-en.do?member=1 (10. 10. 2024).

European Convention of Human Rights.

Federal Law Consolidated: Complete Legal Provision for the General Land Register Act 1955, Version of 30.10.2024 (*Bundesrecht konsolidiert: Gesamte Rechtsvorschrift für Allgemeines Grundbuchsgesetz 1955, Fassung vom 30.10.2024*). Available at: https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10001941 (10. 10. 2024).

Hrvatska enciklopedija. Građansko pravo. Available at: https://enciklopedija.hr/clanak/gradjansko-pravo (10. 10. 2024).

Law on the Legal Profession, *Legal Gazette*, no 9/1994, 117/2008, 50/2009, 75/2009, 18/2011, 126/2021.

Land Registration Act, *Legal Gazette*, no. 91/1996, 68/1998, 137/1999, 114/2001, 100/2004, 107/2007, 152/2008, 126/2010, 55/2013, 60/2013, 108/2017.

Land Registration Act, *Legal Gazette*, no. 63/2019.

Notary Public Act, *Legal Gazette*, no. 78/1993, 29/1994, 162/1998, 16/2007, 75/2009, 120/2016, 57/2022.
Ordinance on amendments to the Ordinance on technical and other conditions for electronic data processing in land registers, *Legal Gazette*, no. 23/2017.
Ordinance on Amendments to the Ordinance on technical and other conditions of electronic data processing in land registers, *Legal Gazette*, no 106/2018.
Ordinance on technical and other conditions of electronic data processing in land registers was adopted, *Legal Gazette*, no. 119/2015.
Ordinance on electronic data processing of users and authorized users of the land registers, Legal Gazette, no 108/2019
Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, *Official Journal,* no L 257/73.
Republika Hrvatska – Ministarstvo pravosuđa, uprave i digitalne transformacije. Uređena zemlja – katastar. Available at: https://oss.uredjenazemlja.hr/ (10. 10. 2024).
Republika Hrvatska – Ministarstvo pravosuđa, uprave i digitalne transformacije. Podnošenje e-prijedloga za upis u zemljišnu knjigu. Available at: https://mpudt.gov.hr/podnosenje-e-prijedloga-za-upis-u-zemljisnu-knjigu/14341 (10. 10. 2024).
Struna – Hrvatsko strukovno nazivlje. Poslužitelj. Available at: http://struna.ihjj.hr/naziv/posluzitelj/48899/ (10. 10. 2024).
Šago, D. 2021. Neki aspekti uloge javnog bilježnika kao povjerenika suda u sudskim postupcima. *Aktualnosti građanskog i trgovačkog zakonodavstva i pravne prakse*, 18, pp. 173-192. https://doi.org/10.47960/2744-2918.18.21.173

CIP - Каталогизација у публикацији
Народна библиотека Србије, Београд

34(082)
343(082)
349::007(082)

INTERNATIONAL Conference Regional Law Review (5 ; 2024 ; Beograd)

[Fifth International Conference] Regional Law Review, Belgrade, 2024 : annual edition / [editors Jelena Kostić, Anita Rodina, Teresa Russo]. - Belgrade [etc.] : Institute of Comparative Law [etc.], 2024 (Beograd : Birograf comp). - [X], 283 str. ; 24 cm. - (Collection Regional law review, ISSN 2812-698X)

"In front of you is the fifth volume of RLR collection of papers..." --> foreword. - Tiraž 150. - Str. VII: Foreword / editors. - Napomene i bibliografske reference uz tekst. - Bibliografija uz svaki rad.

ISBN 978-86-82582-25-0

1. Kostić, Jelena, 1981- [уредник] [аутор додатног текста]

а) Право -- Зборници б) Кривично право -- Зборници в) Информациона технологија -- Право -- Зборници

COBISS.SR-ID 156233737