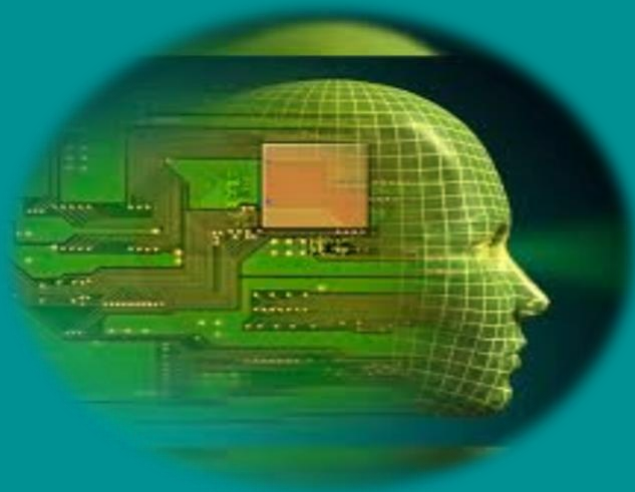


COORDINATING EDITORS

Tiina Pajuste

Heliona Bellani (Miço) Sejla Maslo Cerkić

**Legal Perspectives in the
Modern Era of Technological
Transformations**



ADJURIS 
International Academic Publisher

Legal Perspectives in the Modern Era of Technological Transformations

Editors:



Tiina PAJUSTE

Activity

Tiina Pajuste is Professor of International Law and Security at Tallinn University. Professor Pajuste has previously worked as a Research Fellow at the Lauterpacht Centre for International Law at the University of Cambridge, where she worked on the project *Legal Tools for Peace-Making*, researching the role international law plays in peace negotiations, and at the Erik Castrén Institute of International Law and Human

Rights (University of Helsinki), where she analysed human rights mainstreaming in the context of the European Security and Defence Policy. She completed her PhD at the University of Cambridge on “Accountability Mechanisms for International Organisations”. Her current research focuses on digital human rights, non-discrimination and different aspects of peace negotiations. She was the leader of the research focused working group of the Global Digital Human Rights Network (COST project; <https://gdhrnet.eu>). Link to CV: https://www.etis.ee/CV/Tiina_Pajuste/est?lang=ENG&tabId=CV_ENG.

Publications

Professor Pajuste’s research and publications focus on three main areas – the accountability of international organisations, the role of international law in peace processes and (digital) human rights – which are tied together with the overarching aim of researching the role of international institutions in international interactions. Some of the more noteworthy publications include: Tiina Pajuste, Julia Vassileva, “Inclusion of Women in the Ukrainian Peace Process – Can International Law Play a Bigger Role in Ensuring Inclusion?”, 42 *Polish Yearbook of International Law* (2022) 83-107; Tiina Pajuste, “Inclusion and Women in Peace Processes”, in Marc Weller *et al* (Eds), *International Law and Peace Settlements* (CUP, 2021); Tiina Pajuste, “The Status of the Human Rights of Older Persons”, in Andreas von Arnould, Kerstin von der Decken, Mart Susi (Eds), *The Cambridge Handbook on New Human Rights. Recognition, Novelty, Rhetoric* (CUP, 2020); Tiina Pajuste, “The Protection of Personal Data in a Digital Society: The Role of the GDPR”, in Mart Susi, *Routledge Handbook on Digital Society and Human Rights* (Routledge, 2019); Tiina Pajuste, “The Evolution of the Concept of Immunity of International Organizations”, 8 *East-West Studies* (2017) 6-20; Tiina Pajuste, “Women and Peace Agreements”, 7 *East-West Studies* (2016) 30-50; Tiina Pajuste, “Legality of International Territorial Administration by the

UN”, 18 *Finnish Yearbook of International Law* (2007) 261-281; Tiina Pajuste, *Mainstreaming Human Rights in the Context of European Security and Defence Policy* (the Erik Castrén Institute Research Reports 23/2008).



Heliona BELLANI (MIÇO)

Activity

Dr. Heliona Bellani (Miço) is a lecturer of Public and Constitutional Law in the Law department at “Epoka University” with a long experience in the education field. She has defended her Ph.D. at the University of Tirana with the thesis “*A general overview of the right to education in Albania. Development of this right following international standard and European legislation*”. She is engaged in various research projects in the framework of Erasmus+ programs, and Cost Actions, and is a member of the Association for Teacher Education in Europe. She is an external evaluation expert at the QAAHE and a national consultant in education for UNICEF Albania. She is a member of several editorial boards of international journals and is engaged as a reviewer in several international journals. Her research is focused on human rights, the right to education, quality assurance, educational systems and policy, child's rights, and social justice.

Publications

The main works published by Dr. Heliona Bellani (Miço) are: Miço, H., & (Methasani) Çani, E. (2023). *The Right to Information as a Means of Participation in Governance and Administration. Albanian Legislation Alignment with the Council of Europe Standards*. Proceedings of the International Scientific Conference "Social Changes in the Global World"; 1(10), 269-284. ISBN 978-608-244-998-2 (T.1); Miço, H. (2023). *The right to private and family life and the need for protection against the digital environment*. European Journal of Economics, Law and Social Sciences. Vol 7, No. 2, 2023; Miço, H., Cungu, J. (2022). *The Need for Digital Education in the Teaching Profession: A Path Toward Using the European Digital Competence Framework in Albania*. IAFOR Journal of Education: Technology in Education. Volume 10 – Issue 2. pp. 29-50; Miço, H. (2022). *The right to education of asylum seekers and refugees. The reflection of international instruments and standards in Albanian legislation*. EUWEB legal essays: global & international perspectives: 2, 2022. University of Salerno, Italy,

pp 115-127; Miço, H. (2020). *Addressing the right to education in Albania before and after the communist regime*, p. 91-117, National Library, Tirana Albania; Miço, H. Zaçellari, M. (2020). *Online learning as a means toward achieving an adaptable right to education in Albania*. Knowledge-International Journal, 2020, Vol 42/2, p. 293-298; Miço, H. Zaçellari, M. (2020). *Legal aspects of participation practices in the Albanian Education Context*. Polish Journal of Educational Studies (PJES) – Academy of Science, Poland. p. 94-108. Vol. II. (LXXII); Lauwers, G. Lumani (Zaçellari), M. Miço, H. (Eds.), *Introductory textbook On Law and Rights for Students in Teacher Training and Educational Sciences*, Mileniumi i Ri, 2019, Durres, Albania.



Sejla MASLO CERKIC

Activity

Sejla Maslo Cerkić holds a PhD from the “Džemal Bijedić” University of Mostar and master’s degree in law from the University of Sarajevo. She has been engaged as a lecturer in law and human rights at the Faculty of Law, “Džemal Bijedić” University in Mostar and School of Law, Governance and Society, Tallin University. She is currently employed by the OSCE (Organisation for Security and Co-operation in Europe), Mission to Bosnia and Herzegovina, serving as a national legal officer within the Human Rights Section. Her duties include advising on the harmonisation on domestic legislation and practices with international human rights standards. She is a regular

lecturer at the Sarajevo Faculty of Law Annual Medial Law School, a trainer in human rights topics for judges, prosecutors, students, journalists and civil society members in BiH, and panellist at regional and international conferences. She completed the Mediation Mentoring Programme of the Berghof Foundation Berlin and the OSCE Conflict Prevention Centre, taking part in an intensive programme focussing on dialogue facilitation, negotiation and mediation processes in different contexts. She regularly co-operates with the OSCE Representative on Freedom of Media and Office for Democratic Institutions and Human Rights on freedom of media and freedom of religion or belief topics. She is a member of the Global Digital Human Rights Network (COST project), where she leads one of the research working groups.

Publications

Dr. Maslo Cerkić's academic and professional interest include human rights with focus on freedom of expression and media and freedom of religion or belief. More recently, she has focused on digital aspects of human rights protection and regulation, safety of journalists and human right defenders, and intersectionality of gender and religion. Previously, her research focused on legal historical aspects of human rights in comparative perspective. Selected publications and research projects: Bosnia and Herzegovina | Media Ownership Monitor (mom-gmr.org), 2023 country research (<https://www.mom-gmr.org/en/countries/bosnia-and-herzegovina/>); Contributions to Global Digital Human Rights Network publications, submissions for BiH, 2021-22 (Working Paper Series, <https://gdhr-net.eu/publications/working-paper-series/>); Bubalo, Lana, Maslo Cerkić, Sejla (2022), *Protection of the Right to Honor and Reputation – A Historical Overview*. Journal on European History of Law (JEHL), vol. 13. Heft 1.s.21-35; *Historic, normative and practical aspects of plea bargaining*, co-authorship with dr. Denis Pajić and mr. Sunčica Hajdarović, Review for Law and Economy, Faculty of Law, “Džemal Bijedić” University of Mostar, year 18, no. 1., 2018; *Termination of pregnancy in national laws and the case law of the ECHR*, co-authorship with dr. Maja Čolaković and dr. Denis Pajić, presented at the 5th International Conference on Family Law „*The Reflections of the European Court of Human Rights Case Law in National Family Laws*“, organised by the Faculty of Law, „Džemal Bijedić“ University in Mostar, March 31st and April 1st, 2017, Mostar; *How Shari'a was Europeanized: on some efforts of the Supreme Shari'a court in Sarajevo to modernise Shari'a rules in Bosnia between the two world wars*, presented at the XXth Annual European Forum of Young Legal Historians, University of Cambridge, Faculty of Law, 2-5-4, 2014; *A Bosnian woman between family and law: a study of women's legal status in Bosnia and Herzegovina under Austro-Hungarian rule*, presented at the 19th European Forum of Young Legal Historians, Lille – Ghent, 15-18-5, 2013, (Wo)Men in Legal History, Lille, Centre d'Histoire Judiciaire, 2016.

COORDINATING EDITORS

Tiina Pajuste

Heliona Bellani (Miço)

Sejla Maslo Cerkić

Legal Perspectives in the Modern Era of Technological Transformations

Contributions to the 4th International Conference on FinTech,
Cyberspace and Artificial Intelligence Law
March 22, 2024, Bucharest



Bucharest, Paris, Calgary 2024

ADJURIS – International Academic Publisher

This is a Publishing House specializing in the publication of academic books, founded by the *Society of Juridical and Administrative Sciences (Societatea de Stiinte Juridice si Administrative)*, Bucharest.

We publish in English or French treaties, monographs, courses, theses, papers submitted to international conferences and essays. They are chosen according to the contribution which they can bring to the European and international doctrinal debate concerning the questions of Social Sciences.

ADJURIS – International Academic Publisher is included among publishers recognized by **Clarivate Analytics**.

ISBN 978-606-95862-5-9 (E-Book)

© ADJURIS – International Academic Publisher

Editing format .pdf Acrobat Reader

Bucharest, Paris, Calgary 2024

All rights reserved.

www.adjuris.ro

office@adjuris.ro

All parts of this publication are protected by copyright. Any utilization outside the strict limits of the copyright law, without the permission of the publisher, is forbidden and liable to prosecution. This applies in particular to reproductions, translations, microfilming, storage and processing in electronic retrieval systems.

Preface

Editors

Professor Tiina Pajuste,

Tallinn University, Republic of Estonia

Lecturer Heliona Bellani (Miço),

EPOKA University, Republic of Albania

Lecturer Sejla Maslo Cerkić,

“Džemal Bijedić” University in Mostar, Bosnia and Herzegovina

This volume contains the scientific papers presented at the 4th International Conference on FinTech, Cyberspace and Artificial Intelligence Law that was held on March 22, 2024, Bucharest, online on Zoom. The conference is organized by the *Society of Juridical and Administrative Sciences* in partnership with the *Romanian Academy of Scientists*. More information about the conference can be found on the official website: https://adjuris.ro/fintech/index_en.html.

The scientific studies included in this volume are grouped into three chapters:

- *Ethical Implications and Regulatory Frameworks.* The papers in this chapter refer to: some reflections on two of the most visible developments: the right to refuse internet use and the 'chilling effect'; the law in the internet of things era between created opportunities and vulnerabilities; artificial intelligence - the era of social inequalities: in regulating the future, we need to look at the risks; electronization of the healthcare sector and its responsibility in relation to IT and AI; digital currencies: individual perceptions of the impact on money laundering and the transition to a cashless environment.
- *Legal Strategies for Technological Innovation.* This chapter includes papers on: study on digital transformation and algorithmic law; scenarios for the future of the legal profession in the age of artificial intelligence?; liability of news platforms under the digital services act; the processing of personal data in contracts for the supply of digital content and services; artificial intelligence regulation: approaches and implications.
- *Practical Applications and Challenges in Technology Law.* The papers in this chapter refer to: hacking vehicles' computer system; cybercrime victimization; integrating AI in bank digitalization: strategies, challenges and future perspectives; information support for combating criminal offences by the State Border Guard Service of Ukraine.

This volume is aimed at practitioners, researchers, students and PhD candidates in cyberspace and artificial intelligence law, who are interested in recent

developments and prospects for development in this field at international and national level.

We thank all contributors and partners and are confident that this volume will meet the needs for growing documentation and information of readers in the context of globalization and the rise of dynamic elements in AI law.

Table of Contents

ETHICAL IMPLICATIONS AND REGULATORY FRAMEWORKS	12
<i>Cristina Elena POPA TACHE, Heliona MIÇO (BELLANI)</i> Some Reflections on Two of the Most Visible Developments: The Right to Refuse Internet Use and the 'Chilling Effect'	13
<i>Tiberiu T. BAN</i> The Law in the Internet of Things Era between Created Opportunities and Vulnerabilities	24
<i>Carmen Oana MIHĂILĂ, Lecturer Mircea MIHĂILĂ</i> Artificial Intelligence - The Era of Social Inequalities. In Regulating the Future, We Need to Look at the Risks	39
<i>Tereza JONÁKOVÁ</i> Electronization of the Healthcare Sector and Its Responsibility in Relation to IT and AI	64
<i>Cristina S. CĂPĂȚÎNA (DUMITRACHE), Dragoș BÎLTEANU</i> Digital Currencies: Individual Perceptions of the Impact on Money Laundering and the Transition to a Cashless Environment	75
LEGAL STRATEGIES FOR TECHNOLOGICAL INNOVATION	103
<i>Carmen Silvia PARASCHIV</i> Study on Digital Transformation and Algorithmic Law	104
<i>Verginia VEDINAȘ, Ioan Laurențiu VEDINAȘ</i> Scenarios for the Future of the Legal Profession in the Age of Artificial Intelligence?	115
<i>Sorin-Alexandru VERNEA</i> Liability of News Platforms under the Digital Services Act	126
<i>Sorana BRISC</i> The Processing of Personal Data in Contracts for the Supply of Digital Content and Services	138

Gabriel NIȚĂ
Artificial Intelligence Regulation: Approaches and Implications 154

**PRACTICAL APPLICATIONS AND CHALLENGES IN
TECHNOLOGY LAW** 177

Adriana-Iuliana STANCU
Hacking Vehicles' Computer System 178

Dora ARIFI, Besa ARIFI
Cybercrime Victimization 193

Isabelle OPREA, Daniela DUȚĂ
Integrating AI in Bank Digitalization: Strategies, Challenges and
Future Perspectives 205

Iryna KUSHNIR, Yuliia STEPANOVA
Information Support for Combating Criminal Offences by the State Border
Guard Service of Ukraine 217

**ETHICAL IMPLICATIONS AND
REGULATORY FRAMEWORKS**

Some Reflections on Two of the Most Visible Developments: The Right to Refuse Internet Use and the 'Chilling Effect'

Associate professor **Cristina Elena POPA TACHE**¹
Lecturer **Heliona MIÇO (BELLANI)**²

*Motto: In this theatre of freedom, the actors choose to move at their own rhythms, with the specific risks and rewards. Each step is a sequence of choices*³.

Abstract

The use of technology brings forth several dilemmas, as does internet usage. Not all individuals possess the necessary skills to master technological capabilities – a challenging feat for most of the world's population. The internet is considered by definition a technology, and in this capacity, it is natural to be attached to a series of rights and obligations. From society's accumulated experience, we have witnessed various metamorphoses of human rights, and one of the precursors to the right not to use the internet is the right to disconnect, increasingly encountered. In what stage is this concept of the individual's right to abstain from participating in the online sphere? Is it an El Dorado for modern human rights? How far can individual autonomy go? Why together with the "chilling effect"? Because the connection between individual autonomy and freedom of expression lies in the fact that freedom of expression is often a way in which people express and affirm their autonomy. Through liberal expression, an individual can express their identity, values, and preferences, contributing to the development and affirmation of their own autonomy. The chilling effect, seen as a modern form of lawfare, stifles the evolution of individual rights, reduces freedom, and diminishes the autonomy of individuals in deciding whether or not to use the internet and to what extent they choose to do so online. This article aims to initiate essential discussions regarding the legal and ethical aspects that may make this option of humanity not to use the internet possible or impossible.

Keywords: *internet, human rights, individual autonomy, chilling effect, lawfare, right to disconnect, digitization, new technologies, society, international law.*

JEL Classification: K24, K33

DOI: <https://doi.org/10.62768/ADJURIS/2024/1/01>

¹ Cristina Elena Popa Tache - Active Researcher at CIRET-Center International de Recherches et Études Transdisciplinaires Paris; associate professor at the Faculty of Psychology, Behavioral and Legal Sciences, Andrei Saguna University, Romania and Co-Chair of the Interest Group International Affairs and Human Rights of the European Society of International Law-ESIL. ORCID Researcher ID: <https://orcid.org/0000-0003-1508-7658>. E-mail: cristinapopatache@gmail.com.

² Heliona Miço (Bellani) - lecturer of public and constitutional law at the Law Department of Epoka University, Tirana, Albania. Her research is concentrated in the fields of human rights, the right to education, social inclusion, and quality in higher education institutions. ORCID Researcher ID: <https://orcid.org/0000-0002-2398-7798>. E-mail: hmico@epoka.edu.al.

³ The text of this motto belongs to the authors.

Please cite this article as:

Popa Tache, Cristina Elena & Heliona Miço (Bellani), „Some Reflections on Two of the Most Visible Developments: The Right to Refuse Internet Use and the 'Chilling Effect'”, in Pajuste, Tiina, Heliona Bellani (Miço) & Sejla Maslo Cerkic (eds.), *Legal Perspectives in the Modern Era of Technological Transformations*, ADJURIS – International Academic Publisher, Bucharest, Paris, Calgary, 2024, p. 13-23.

1. Introduction

There is currently a huge gap in international legal instruments for the protection of human rights in the digital domain. International law itself is currently undergoing some transformative stages. Its fragmentation is a double-edged phenomenon: positive in the sense that new branches of law can emerge, such as international law of digitization, and negative in the sense that he must now struggle for its autonomy as a discipline. Issues of adapting the law to modern challenges remain the main concern of doctrine and jurisprudence because indeed, nothing can be more telling in this regard than the efforts made to find an acceptable technique of international law, from the moment old conceptions clashed with realities⁴.

For international law (especially for human rights), today it's as if it has moved to a new place where the scenery changes and the customs are new. The various possibilities of personal choices enjoyed or to be enjoyed by modern humans urge the specialized theory to analyze the established fundamental rights, with a focus on the autonomy of will (as an intrinsic part of individual autonomy) and its delineation through numerous shaping attempts. Circumstances in which autonomy is limited are justified only to ensure the general welfare and respect for the rights and dignity of all individuals. However, all personal choices are umbilically linked to society. From this perspective, the works of sociologists can be a precious source for achieving research results through current methodologies such as inter-, multi-, or transdisciplinary. Discussions concern the effect of policies on the population, as well as standard demographic variables, considerations given by: race, location, age, etc.⁵ Any societal phenomenon has the potential to

⁴ Titulescu, Nicolae. *Documente diplomatice/Diplomatic documents*, Political Publishing House, Bucharest, 1967, p. 846.

⁵ For example, Livingstone, S., & Helsper, E. (2007), *Gradations in digital inclusion: Children, young people and the digital divide*, *New Media & Society*, 9(4), pp. 671-696, doi:10.1177/1461444807080335 or James, Natalie (2022). *Countering far-right threat through Britishness: the Prevent duty in further education*. *Critical Studies on Terrorism*, 15(1), 121–142. <https://doi.org/10.1080/17539153.2022.2031135>. For regression analysis in investigating the impact that tension and resilience, individuals' gender, economic situations, individual life experiences, and internet use have on their propensity to associate with, engage with, and support far-right ideologies and associated violence see Joshua Skoczylis & Sam Andrews (2022) *Strain theory, resilience, and far-*

become a legal phenomenon within the realm of technology usage, and from there, the path to the norm, to codification, is paved. The fundamental principles of law underpin branch principles, between which there exists a relationship of correspondence and amplification⁶; the principles of this new branch of law naturally stand in a relationship of dependency with the general principles of other corresponding fields in society. Principle does not have origin, whereas, the origin of standards is represented by principles, as all things are born from principle, but it cannot be born from anything⁷. The outcome of the application of principles in this field of law is indeed the certainty of law⁸.

The European Union currently leads in regulating new technologies. Article 8 of the Charter of Fundamental Rights explicitly recognizes this protection and serves as a necessary reference point for formulating internet principles globally. All internet rights are based on the full recognition of the freedom, equality, dignity, and uniqueness of each individual. Guaranteeing these rights is indispensable for ensuring democracy and the democratic functioning of institutions, to prevent the abuse of power by public or private authorities that could lead to a surveillance, control, and social selection society. The lingering question is who and why causes the chilling effect. The chilling effect refers to the phenomenon where individuals or groups refrain from exercising their rights or engaging in certain activities online due to fear of surveillance, censorship, or other forms of repression⁹. The entire process of normative adaptation is difficult in itself, and any actions resembling lawfare lead to the cessation of any progress under discussion. It is true that since January 23, 2023, we have the European Declaration on Digital Rights and Principles for the Digital Decade, a document promising that the European way of digital transformation places people at the center and is supported by European values and fundamental rights of the EU, reaffirming the universal human rights and bringing benefits to all individuals, businesses, and society as a whole¹⁰. At the same time, the first principle presented in the declaration is that of people-centered digital transformation. Starting from the date of

right extremism: the impact of gender, life experiences and the internet, Critical Studies on Terrorism, 15:1, 143-168, DOI: 10.1080/17539153.2022.2031137.

⁶ I. Dogaru, *Elemente de teoria generală a dreptului*, Ed. Oltenia, Craiova, 1994, p. 115.

⁷ *Principii autem nulla est origo; nam e principio oriuntur omnia, ipsum autem nulla ex re alia nasci potest.* Cicero, Tusculanae, disputationis.

⁸ In the sense of a guarantee given to individuals in the face of the sometimes unpredictable nature of coercive rules and the congruence of the legislative system. Nicolae Popa, *Teoria generala a dreptului*, Ed. Univ. Titu Maiorescu, 2002, p.111.

⁹ Penney, J. (2016), *Chilling Effects: Online Surveillance and Wikipedia Use*, Berkeley Technology Law Journal. Vol. 31, No. 1 (2016), pp. 117-182, Published By: University of California, Berkeley, School of Law, DOI: <http://dx.doi.org/10.15779/Z38SS13>. This study explores the chilling effect of online surveillance on internet users' behavior, particularly focusing on Wikipedia use. It analyzes traffic data from Wikipedia articles related to sensitive topics and finds evidence suggesting that traffic to these articles decreases following revelations about government surveillance programs.

¹⁰ At the European level, a source for principles and rights in communications and new technologies is: the European Declaration on Digital Rights and Principles for the Digital Decade 2023/C23/01/

publication of the Declaration in the Official Journal of the EU, on 23.01.2023, it is understood that any document must be interpreted based on the set of principles and rights from the Declaration. Following the path of legal logic, people-centeredness can be equivalent to focusing on personal rights, including autonomy of will. In the EU, another soft law rule, the Human Rights Guide for Internet Users¹¹ focuses on the following fundamental human rights and freedoms concerning the Internet: 1) access and non-discrimination; 2) freedom of expression and information; 3) freedom of assembly, association and participation; 4) protection of privacy and personal data; 5) education and literacy; 6) protection of children and young people; and 7) the right to an effective remedy for invoking fundamental human rights and freedoms¹².

2. Relevance of the subject and some observations

The research attention is directed toward the responsibility and legal protection of states. In this context, we are once again victims of our own disinterest in the development of international state responsibility, so the orientation is based on the trends of strategies and policies of a state or group of states. Their tendency is either to protect or restrict the right not to use the internet in the public interest. In the former case, protection is characteristic of democratic societies, while in the latter case of restricting rights, the danger is of abuse. Thus, we can discuss state bullying as a concept that describes the abuse of power by the state or authorities against individuals or groups, including political harassment, excessive surveillance, persecution of minorities, and systematic discrimination. Such actions can violate individual rights and freedoms, causing negative effects on society and undermining the principles of democracy and the rule of law.

It is an epiphenomenon of technological possibilities that brings to mind Francisco de Goya, resulting in a paraphrase according to which the sleep of reason has given birth to the monster named chilling effect. When reason and logical thinking are suspended or asleep, negative consequences or irrational and dangerous behaviors can occur. In the context of Goya's work¹³, the image illustrates

PUB/2023/89. Recently, on 23.01.2023, this Declaration was published in the Official Journal of the European Union.

¹¹ Recommendation CM/Rec (2014)6 of the Committee of Ministers to member states on the Human Rights Guidelines for Internet Users and Explanatory Memorandum adopted by the Committee of Ministers on 16 April 2014.

¹² On 16 April 2014, the Committee of Ministers adopted Recommendation CM/Rec(2014)6 on Human Rights Guidelines for Internet Users. The material is available here: <https://rm.coe.int/guide-to-human-rights-for-internet-users-romanian-/1680768064> and was accessed on 06.02. 2023.

¹³ "The Sleep of Reason Produces Monsters" is a famous phrase, used today in various contexts, and originally the title of a well-known engraving by the 18th-century Spanish painter Francisco Goya. In 1799, Goya exhibited a series of 80 engravings titled "Los Caprichos" (The Caprices), with "The Sleep of Reason Produces Monsters" being the 43rd. In contemporary language, whether in Romanian or any other language, the expression "The Sleep of Reason Produces Monsters" refers

the artist asleep on a table, while monsters and nightmare creatures surround his space. It is often interpreted as a critique of ignorance, superstition, and abuses of power, suggesting that the lack of reason and discernment can give rise to manifestations of evil and irrationality. In fact, this is how the chilling effect was born - the phenomenon in which people become hesitant to exercise their rights or freely express their opinions due to fear of repercussions or sanctions. It can result from a variety of factors, such as threats of legal action, intimidation, legislative restrictions, or any other action that creates a hostile or inhibiting environment for free expression. The term chilling effect is synonymous with a form of lawfare in certain contexts, especially when it results from state actions. Lawfare is the use of law as a weapon or tool of influence, including to obstruct or discourage opposition or free expression of opinion. In this sense, when individual rights are undermined or when the law is used to intimidate or discourage certain actions, including free expression of opinion, this can be considered an aspect of lawfare.

The chilling effect, as an ultra-chameleonic phenomenon, is not always associated with lawfare but sometimes encompasses all the reasons that lead individuals to refrain from using the internet. Thus, it can result from cultural, social, or political factors that create an environment in which people feel they cannot freely exercise their rights or that there are too many risks associated with expressing their opinions. Following the line of detail, we can see how abstaining from the internet can be, for some individuals, a way to protect themselves against digital dependence to maintain balance in their lives, as well as to avoid the negative impact of excessive internet use. Here, decisions by a portion of the global population to avoid the internet for ethical or philosophical reasons related to data collection, information manipulation, or other aspects of the online environment can also be listed¹⁴. Moreover, access to the internet can be limited due to financial or geographical resources, so abstaining from the internet can be a consequence of the lack of accessibility to technology. All of these factors weaken legal boundaries of individual autonomy to the point of fragility.

Balance must be sought primarily for antagonistic cases, such as putting those who choose to abstain from the internet against those for whom the internet has become an essential tool. Technology is gradually replacing humans in various activities. Many causes of the chilling effect are generated by the control of political power, especially when certain governments or political parties promote a particular political or ideological agenda, attempting to reduce or discourage

to moments in which, in individual or collective life, intelligence, balance, harmony, wisdom, culture, authentic human substance, and the spiritual dimension of being give way to instinct, chaos, disorder, arbitrariness, and fear.

¹⁴ See Aviv Weinstein & Michel Lejoyeux (2010) *Internet Addiction or Excessive Internet Use*, *The American Journal of Drug and Alcohol Abuse*, 36:5, pp. 277-283, DOI: 10.3109/00952990.2010.491880.

any voice that opposes or criticizes that agenda. In some conferences, we proposed the creation of new professions of the future such as human intermediaries or human internet or technology agents. Likewise, we can envision a world where politicians are replaced by software programs, any compatible artificial intelligence systems, etc. In this way, it seems that the risks associated with political abuses, including the form of lawfare characteristic of those in power in a state who wish to conserve and strengthen it using the chilling effect to discourage any opposition or challenge to the status quo, would be eliminated. The robot politician seems to be a solution against all forms of abuse, including the abuse of not regulating the legal regime of lawfare through instruments of international law or even domestic law. Lawfare and its countless faces have long been known, but it seems that we are very far from the result of its legal regulation.

These crises intensify when we fail to find established obligations to use the internet, the right not to use it, or the corresponding protections, leaving these two exposed to the risk of the chilling effect. In evaluating the social impact on individuals who choose not to use the internet, the rights of vulnerable individuals such as children and the elderly take precedence, for example, or the impact on personal and professional development. The imperative of reconciliation with the needs and interests of society, especially from a legal point of view, leads to situations where the solution is the identification of limits and rules that could ensure the balance between individual rights and the common good.

It is certain that individuals cannot be deprived of the possibility of voluntarily distancing themselves from the online environment, considering ethical options, personal values, or security concerns, without affecting fundamental rights to education and access to information in available non-digital alternatives. Any form of restriction on these rights can easily slip into the form of lawfare chilling effect. Medical sciences have brought some limits conferred by online dependence¹⁵. It has been found that there is internet addiction to a similar extent as there is abuse of drugs and alcohol, pathological gambling, and even video game addiction¹⁶.

Although not universally recognized, if we were to give a definition of the right not to use the internet, we can view it as the potential fundamental right of a person to choose not to directly and actively participate in the online environment, without facing negative consequences or discrimination, ensuring the freedom to manage their own digital presence and protect their personal privacy.

Who is the guarantor of human rights? The state is a structure for maintaining security and the proper functioning of society in the digital era. Ultimately, at the center of the triangle with equal sides - digitization, human rights,

¹⁵ Fortson B. L., Scotti J. R., Chen Y. C., Malone J., Del Ben K. S., *Internet use, abuse, and dependence among students at a southeastern regional university*. J Am Coll Health 2007; 56(2):137–144 and Young KS. *Internet Addiction: A new clinical phenomenon and its consequences*, in American Behavioral Scientist 2004; 48(4):402–415.

¹⁶ Aviv Weinstein & Michel Lejoyeux (2010), *op. cit.*, pp. 277-283.

and security - will be these reforms of models that protect rights and limit powers on a global scale. The Triangle (human rights, digitization, and security) and how they interact with each other, are based on the observation that the triangle is indeed a modern paradigm of international relations that focuses on the interconnectedness of its three equal sides. In other words, following the same correspondence, we can observe: legality, necessity, and proportionality.

Human rights contain principles that protect human freedoms and dignity and are safeguarded by international laws and treaties such as the UN Universal Declaration of Human Rights and the European Convention on Human Rights. In general terms, we list the right to life, liberty, and security of the person, the right to a fair trial, freedom of expression and opinion, the right to education, work, and privacy¹⁷.

The right of a person not to use the internet, as well as the forms of guaranteeing and protecting it, are directly proportional to their formal and detailed recognition in legislation, the elimination of chilling effect lawfare forms, societal awareness, and adaptation.

If we were to outline the general lines of arguments for or against the right not to use the internet, we could observe how, in the "pro" category, arguments may include: 1) the right to privacy as a way to protect intimacy and avoid excessive exposure of personal information online; 2) the right to make personal choices - a fundamental principle of democratic societies according to which the refusal to use the internet is an expression of individual autonomy; 3) preservation of mental health, reducing the negative impact of excessive use, such as online stress and anxiety; 4) avoiding digital dependence and the negative impact of excessive time spent online; 5) opting for an "offline" lifestyle; or 6) protecting individual religious, philosophical, or traditional values. These arguments are presented through the lens of the individual.

On the other hand, several arguments "against" the right not to use the internet can be identified, such as 1) access to information and education (to educational resources), in which case its refusal may limit learning and personal development opportunities; 2) the internet facilitates communication and social interaction, and absence from online platforms can lead to social isolation and limited connections with other people; 3) issues for labor rights regarding workplace efficiency or even professional opportunities, as most employers use the internet in the recruitment process, and online absence can limit career and professional opportunities; 4) exclusion from participation in the digital economy, affecting access to services and business opportunities; 5) the internet brings advantages in terms of communication efficiency, rapid access to information, and solving daily problems, and its refusal can lead to the loss of these advantages;

¹⁷ Cristina Elena Popa Tache, *The New International Triangle: Human Rights-Digitalization-Security*, International Investment Law Journal Volume 4, Issue 1, February 2024, pp. 4-17.

and 6) social exclusion. Many of the "against" arguments seem to align with issues raised by public authorities.

Considering the reflections of this work, we can affirm that the right not to use the internet is necessary nonetheless and contributes to maintaining a healthy balance between online and offline life, thus promoting a diversified lifestyle. If something contradicts the public interest here, then we turn to corresponding changes within the labor market, which is currently undergoing reform.

Ultimately, by emphasizing the issues of lawfare/chilling effect, attention is directed towards the numerous examples of lawfare threats to human rights in the context of digitization, which can continue on many pages. One of these is illustrated in recent doctrine and consists of greater governmental control over encrypted online communication, considered to violate the right to privacy and freedom of expression of ordinary internet users¹⁸. These loopholes of "escape" by state authorities must be subject to legal limits established through preferably international regulations. As detailed in previous work¹⁹, following this line of legal reasoning, some authors have reported that the importance of controlling online content has been fetishized by governments pressuring internet companies to introduce stricter mechanisms in this regard, which has proven not to have the quality to solve the issue of digital jihad, but has effectively raised concerns regarding the respect for human rights, including issues regarding freedom of expression and the right to privacy online²⁰.

Exemplifying, in international legal literature, the existence of another type of technological lawfare effect has been identified: Sieber stated in a study: "Undoubtedly, the newest human development is the relationship between humans and their increasingly sophisticated technologies. Modern technologies have grown without watchdogs capable of legal opposition to what could be called the colonization of the mind through modern technologies."²¹ In his study, Sieber refers to modern platforms and neurotechnological devices, which he considers colonizers of minds, against the backdrop of insufficient regulation regarding the protection of human rights against these threats. He invokes the courage of scientists to produce human rights protections "to safeguard not only the psychological life of human beings but also the human spirit itself, as both largely remain unaddressed."²² These threats to human rights protection are often likened

¹⁸ See Jeroen Veen and Sergei Boeke, *No Backdoors: Investigating the Dutch Standpoint on Encryption*, Policy and Internet, Volume12, Issue4, December 2020, pp. 503-524.

¹⁹ Cristina Elena Popa Tache, Cătălin-Silviu Săraru, *Lawfare, Between its (Un)Limits and Transdisciplinarity*, *Precedente Revista Juridica*, 23, 37-66, 2023. <https://doi.org/10.18046/prec.v23.5889>.

²⁰ Miron Lakomy, *Why Do Online Countering Violent Extremism Strategies Not Work? The Case of Digital Jihad*, in "Terrorism and Political Violence", Routledge, 2022, p. 14. DOI: 10.1080/09546553.2022.2038575.

²¹ Alexander Sieber, *Digital Barbarism: The New Colonization of the Mind*, *Critical Arts*, 35:5-6, 2021, p. 252.

²² *Ibid.*

to colonialism of the mind, with the definition of colonialism provided by the Oxford Advanced American Dictionary being cited: "the practice by which a powerful country controls another country or countries."²³ Such colonialism continues to happen today through less visible means, such as lawfare, Sieber concludes, in turn, along with other theorists who have set out to uncover lawfare²⁴.

Lawfare in the form of a chilling effect is certainly a reality, as it can entail the use of legal systems and institutions to deter a person from exercising their legal rights²⁵.

3. Conclusions

The internet has become a vital space for free expression, idea exchange, and access to information. The legal reaffirmation of the importance of individual rights in the modern context is a natural process, essential for safeguarding the freedoms and autonomy of each individual in the face of technological, social, and political developments. On one hand, individuals who choose these rights should seek alternatives that meet their needs and preferences, thereby reaffirming the importance of diversity in the process of personal formation and development. On the other hand, states must pursue finding adequate solutions to new technological metamorphoses, as there is no place for delay.

The chilling effect phenomenon undermines the right to free expression online, through deterrence or fear. The use of lawfare through chilling effect by some subjects of international law in the digital context generates significant consequences for freedom of expression and access to information. By imposing legislative restrictions or using the judicial system to intimidate or discourage the free expression of opinion, states or non-state actors are tempted to consolidate their power or promote their political or ideological agenda.

To counteract these negative effects, both legislative measures and policies to guarantee the protection of privacy and freedom of expression online are necessary, as well as the initiation of establishing the legal regime of lawfare. Efforts in this regard must be supported both locally and globally, to protect the rights and freedoms of all citizens equally valid online and offline.

²³ Hornby, Albert Sydney, *Oxford Advanced Learner's Dictionary of Current English*, London: Oxford University Press, 1995, p. 76.

²⁴ A. Sieber, *op. cit.*, p. 256; Cristina Elena Popa Tache, *The New International Triangle: Human Rights-Digitalization-Security*, International Investment Law Journal Volume 4, Issue 1, February 2024, pp. 4-17.

²⁵ See the full Report drafted by Michael Scharf & Elizabeth Andersen, assisted by Cox Center Fellows Effy Folberg, Michael Jacobson, & Katlyn Kraus, *Is Lawfare Worth Defining? Report of the Cleveland Experts Meeting September 11, 2010*, in *Case Western Reserve Journal of International Law*. 43 (1). 11 September 2010. Also see Kittrie, Orde F., 'Conclusion', *Lawfare: Law as a Weapon of War* (New York, 2016; online edn., Oxford Academic, 21 Jan. 2016), <https://doi.org/10.1093/acprof:oso/9780190263577.003.0009>, accessed 8 May 2024.

Bibliography

1. Dogaru, Ion, *Elemente de teoria generală a dreptului*, Ed. Oltenia, Craiova, 1994.
2. European Declaration on Digital Rights and Principles for the Digital Decade 2023/C23/01/PUB/2023/89. Recently, on 23.01.2023, this Declaration was published in the Official Journal of the European Union.
3. Fortson, B. L., Scotti J. R., Chen Y. C., Malone J. & Del Ben K. S., *Internet use, abuse, and dependence among students at a southeastern regional university*. *J Am Coll Health* 2007; 56(2):137–144.
4. Hornby, Albert Sydney, *Oxford Advanced Learner's Dictionary of Current English*, London: Oxford University Press, 1995.
5. James, Natalie (2022). *Countering far-right threat through Britishness: the Prevent duty in further education*. *Critical Studies on Terrorism*, 15(1), 121–142. <https://doi.org/10.1080/17539153.2022.2031135>.
6. Kitzie, Orde F., 'Conclusion', *Lawfare: Law as a Weapon of War* (New York, 2016; online edn, Oxford Academic, 21 Jan. 2016), <https://doi.org/10.1093/acprof:oso/9780190263577.003.0009>, accessed 8 May 2023.
7. Lakomy, Miron, *Why Do Online Countering Violent Extremism Strategies Not Work? The Case of Digital Jihad*, in 'Terrorism and Political Violence', Routledge, 2022, DOI: 10.1080/09546553.2022.2038575.
8. Livingstone, S. & Helsper, E. (2007), *Gradations in digital inclusion: Children, young people and the digital divide*, *New Media & Society*, 9(4), pp. 671–696. doi:10.1177/1461444807080335.
9. Penney, Jonathon. *Chilling Effects: Online Surveillance and Wikipedia Use*, *Berkeley Technology Law Journal*. Vol. 31, No. 1 (2016), pp. 117-182, Published By: University of California, Berkeley, School of Law.
10. Popa Tache, Cristina Elena & Cătălin-Silviu Săraru, *Lawfare, Between its (Un)Limits and Transdisciplinarity*, *Precedente Revista Juridică*, 23, 37-66, 2023. <https://doi.org/10.18046/prec.v23.5889>.
11. Popa Tache, Cristina Elena, *The New International Triangle: Human Rights-Digitalization-Security*, *International Investment Law Journal*, Volume 4, Issue 1, February 2024, pp. 4-17.
12. Popa, Nicolae, *Teoria generala a dreptului*, Ed. Univ. Titu Maiorescu, 2002.
13. Recommendation CM/Rec (2014)6 on Human Rights Guidelines for Internet Users. The material is available here: <https://rm.coe.int/guide-to-human-rights-for-internet-users-romanian-/1680768064> and was accessed on 06.02.2023.
14. Sieber, Alexander, *Digital Barbarism: The New Colonization of the Mind*, *Critical Arts*, 35:5-6, 2021, p. 252.
15. Skoczylis, Joshua & Sam Andrews (2022) *Strain theory, resilience, and far-right extremism: the impact of gender, life experiences and the internet*, *Critical Studies on Terrorism*, 15:1, 143–168, DOI: 10.1080/17539153.2022.2031137.
16. The report drafted by Michael Scharf & Elizabeth Andersen, assisted by Cox Center Fellows Effy Folberg, Michael Jacobson & Katlyn Kraus, *Is Lawfare Worth Defining? Report of the Cleveland Experts Meeting September 11, 2010*, in *Case Western Reserve Journal of International Law*. 43 (1). 11 September 2010.

17. Titulescu, Nicolae. *Documente diplomatice/Diplomatic documents*, Political Publishing House, Bucharest, 1967.
18. Veen, Jeroen & Sergei Boeke, *No Backdoors: Investigating the Dutch Standpoint on Encryption*, Policy and Internet, Volume12, Issue4, December 2020, pp. 503–524.
19. Weinstein, Aviv & Michel Lejoyeux (2010) *Internet Addiction or Excessive Internet Use*, The American Journal of Drug and Alcohol Abuse, 36:5, pp. 277-283, DOI: 10.3109/00952990.2010.491880.
20. Young, K. S., *Internet Addiction: A new clinical phenomenon and its consequences*, in American Behavioral Scientist 2004; 48(4):402–415.

The Law in the Internet of Things Era between Created Opportunities and Vulnerabilities

Assistant professor **Tiberiu T. BAN**¹

Abstract

In the context of computerization and automation of most economic sectors and private life, the increase in the number of attacks on computer systems that expose personal data to unauthorized persons is alarming. It started from a hypothesis already validated in the specialized literature that properly designed security policies and procedures can prevent attacks exploiting known vulnerabilities to a satisfactory extent. However, their simple existence is not enough, these security policies and procedures must be adapted to the specifics of each computer system, with the appropriate legal support. We followed a transdisciplinary analysis that combines elements of informatics and legal regulations regarding the opportunities and vulnerabilities of smart devices, face to face with the criminal phenomenon of cyber crime aimed at the security and confidentiality of personal data. The main objective of the present study is to identify and extract 'lessons learned' regarding vulnerabilities of the Internet of Things type information systems. These 'good practices' allow the development of procedures and security policies useful in preventing computer attacks criminalized as the crime of unauthorized access to a computer system.

Keywords: information security, information privacy, security policies, processing procedures, preventing cyber-attacks.

JEL Classification: K24

DOI: <https://doi.org/10.62768/ADJURIS/2024/1/02>

Please cite this article as:

Ban, Tiberiu T., „The Law in the Internet of Things Era between Created Opportunities and Vulnerabilities”, in Pajuste, Tiina, Heliona Bellani (Miço) & Sejla Maslo Cerkcic (eds.), *Legal Perspectives in the Modern Era of Technological Transformations*, ADJURIS – International Academic Publisher, Bucharest, Paris, Calgary, 2024, p. 24-38.

1. Introductory considerations

In everyday life, a user has come to rely on the computer systems that serve them. All the online activities of an ordinary user generate personal data that any marketing agency and any 'cybercriminal' can consider a valuable target, which also explains the fact that recent years have brought increasingly larger

¹ Tiberiu T. Ban - Faculty of Law, 'Bogdan Voda' University of Cluj Napoca, tiberiu.ban@gmail.com.

waves of cyber-attacks targeting personal data.

It is already universally accepted that standards regarding the protection of personal data are becoming increasingly high and impose stricter rules. The purpose of this endeavor is to provide an acceptable and reasonable degree of security, regardless of the state in which data processing takes place.

This aspect obliges companies² to carry out increasingly complex evaluation studies in order to provide guarantees that the data processing carried out complies with current standards in an international context.

The main difficulty relates to the fact that data processing is present in all areas and sectors of the economy and the daily activities of individual users, and the possibility of using new technologies should make all such processing easier, faster and more transparent, but it is often these that in reality introduce an additional series of problems relating to information security and the security of information systems, the solution of which is sometimes left to the individual user in the absence of specific uniform regulations.

The European Union has intervened over time with regulations offered to Member States to provide a common basis for the protection and security of personal data such as Directive 95/46/EC³ or for the protection of information systems such as the NIS Directive⁴ and recently the NIS Directive⁵.

In just the past few years, considering all these considerations, the European Union has adopted the General Data Protection Regulation⁶ due to the express desire to harmonize the rules imposed and respected by the member states regarding data processing. At the same time, the adoption of the GDPR had the effect of strengthening the level of confidentiality provided to the data subjects of these personal data processing activities.

In practice, over the past twenty years, the European Union has analysed the need for the alignment of the standards used by the member states when it comes to processing personal data, especially in the context where these processing activities are often online and tend to have a cross-border nature. The previously existing regulations allowed states to establish with a high degree of autonomy the level of data protection they consider appropriate and necessary to

² See P. Voigt, A. Bussche, *The EU General Data Protection Regulation (GDPR). A practical guide*, Springer International Publishing, 2017, pp. 2–7.

³ See Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, repealed on 24 May 2018, available at <http://data.europa.eu/eli/dir/1995/46/oj>.

⁴ See Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of network and information security across the Union, available at <http://data.europa.eu/eli/dir/2016/1148/oj>.

⁵ See Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 NIS2 available at <https://eur-lex.europa.eu/eli/dir/2022/2555>.

⁶ See Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals 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) available at <https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32016R0679&from=EL>

impose on operators who carry out data processing, often in an automated manner through increasingly sophisticated computer systems.

Furthermore, the previous regulations did not provide any legal certainty in terms of the legislative framework, neither for operators nor for their representatives. For example, through Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, it was intended to implement a guarantee for the protection of the fundamental rights of individuals in the context of interstate processing of personal data between the member states of the Union. These efforts had limited effects because, having the status of a Directive, it was necessary for each of the member states to introduce these provisions into national legislation through separate legislation, such as Law 677/2001 in the case of Romania.

In practice, it was considered⁷ that Directive 95/46/EC failed to achieve its intended objectives because there was no alignment of standards among the member states regarding the protection of personal data in the European Union. Furthermore, in recent years, even the ‘EU – US Privacy Shield’ has been considered outdated and no longer provides sufficient guarantees⁸ on data transfers between the Union and the United States of America and has been formally invalidated⁹ finally by the decision of the Court (Grand Chamber) in Maximillian Schrems v Facebook Ireland Limited. This ‘Shield’ refers to the legal framework adopted by the European Commission¹⁰, which allowed entities and data controllers in the United States to obtain certification – sometimes self-offered – of compliance with a certain level of protection for personal data.

This shortcoming has been overcome by the joint efforts of the European Union and the United States. On 10.07.2023 the European Commission announced¹¹ the adoption of the ‘EU – US Data Privacy Framework’, considering that the United States of America has now succeeded in providing a level of pro-

⁷ See P. Voigt, A. Bussche, *op. cit.*, p. 2.

⁸ See Joint Press Statement by European Commissioner for Justice Didier Reynders and US Secretary of Commerce Wilbur Ross, 10.08.2020 on the assessment of a possible enhanced Privacy Shield to meet the requirements of the 16 July 2020 Judgment – Facebook v. Schrems, available at https://ec.europa.eu/info/news/joint-press-statement-european-commissioner-justice-didier-reynders-and-us-secretary-commerce-wilbur-ross-7-august-2020-2020-aug-07_en accessed 15.08.2022.

⁹ See Judgment of the Court (Grand Chamber) of 16 July 2020 Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems. Case C-311/18. Available at <https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:62018CJ0311>.

¹⁰ See Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of the EU-US Privacy Shield (notified under document number C (2016)4176, available at http://data.europa.eu/eli/dec_impl/2016/1250/oj).

¹¹ See press release ‘Data Protection: European Commission adopts new adequacy decision for safe and trusted EU-US data flows’, available at https://ec.europa.eu/commission/presscorner/detail/en/IP_23_3721.

tection for the processing of personal data similar to that implemented in the European Union.

2. The reality and opportunities of new technologies

The changes¹² that technology and the widespread use of information systems in all aspects of everyday life¹³ undoubtedly open up opportunities and new ways in which data can be processed. Computer systems are becoming increasingly powerful, with impressive computing power and virtually infinite data storage capacity, which is becoming increasingly economically accessible.

The last decade has been marked by a spectacular leap forward in the evolution of information and communication technology. Internet connectivity for computers has become increasingly cost-effective and faster. This has led to a transition in terms of websites and online content availability. As a first step, the transition from static web 1.0 sites to dynamic sites, user-generated content, social media platforms, and a general trend towards encouraging users to share more information, life moments, memories, and even potentially sensitive data online can be observed. Consequently, there is an essential need to pay particular attention to ensuring an adequate level of security for computer networks and component systems, considering that a vast proportion of critical systems rely on computer systems, and an attack targeting them can have devastating effects¹⁴ at the level of an entire country.

User interaction with online devices has moved beyond the computer screen to the area of mobile devices, gadgets ‘always connected’ to computer system networks or the Internet. Data storage has become much more accessible through the technological advance that cloud-based technologies have demonstrated.

As the user becomes more and more dependent on internet-connected devices, they become part of the Internet of Things ecosystem, an ecosystem of ‘smart’ devices that collect data from the user, some of which is personal data, biometric data, and other devices are given a maximum ‘trusted’ role in the private network topology, being allowed to control other devices.

Internet-connected systems offer a standard of living that we are now unwilling to give up, there is unrestricted access to information, entertainment, socialising. However, each such technological revolution brings both a number of economic and social benefits, but also allows the exploitation of new paradigms

¹² See T. Ban, *The digital future of law between the opportunities of the cyber era and the acute need for security*, in *Curierul Judiciar*, no. 6, 2020, pp. 339–345.

¹³ See A. Ciurea, *The Digital Age and Justice (I). Objectives, algorithm design methods and consequences of their use in justice*, in *Revista Universul Juridic*, No. 1 January 2022, pp. 56–70, available at http://revista.universuljuridic.ro/wp-content/uploads/2022/03/06_Revista_Universul_Juridic_nr_1-2022_PAGINAT_BT_A_Ciurea.pdf.

¹⁴ See I. VasIU, *Criminalitatea informatică*, Ed. Nemira, Bucharest, 1998, p. 139.

previously unexplored or insufficiently protected by national legislation.

As we have previously argued¹⁵, the shift to the paradigm of an almost fully digitised society comes not only with advantages but also with a new set of vulnerabilities that allow malicious individuals to exploit totally innovative ways to coordinate attacks on information systems targeting data availability, integrity or confidentiality as well. This prospect raises a number of new challenges¹⁶ for the legislator regardless of the country, as the phenomenon has a cross-border dimension due to the elements of foreignness that arise very easily in a cyber, virtual environment, where often the concrete, the geographical location of the computer systems targeted by cyber attacks is not even known.

However, although the aim is to prevent criminal phenomena directed against a computer system or using a computer system, all measures taken by the legislator must be based on respect for the principle of proportionality between interference in individual rights and freedoms – in particular the right to privacy¹⁷ to the confidentiality of communications and the seriousness of these crimes, for the good of society as a whole.

In terms of the consequences of these offences, they can range from some directed against a specific person such as accessing a social networking account to read private conversations without the right to some directed against state institutions among those involved in the effective work of combating crime in the cyber environment, such as the Romanian Police and IGPR.

It is questioned whether there are distinctions between cybercrime in terms of the status of the active subject and the possible criminal participation in terms of the possibility of finding the criminal guilt of the legal person. The legal issue of criminal liability of the legal person with its legal characteristics is a fairly recent institution introduced in Romanian legislation, which has been previously analysed under the comparative aspect of the arguments for and against the appropriateness of its introduction in the legislative framework. The Internet certainly allows the advantage of possible anonymity from the illusion of security offered by the personal computer monitor, which explains why the online area has become an early target for a new type of attackers, those specialising in attacks on information systems, with cases of famous convictions¹⁸ in American jurisprudence since the 1990s, causing colossal damage.

As a new area of crime, the need to understand this totally new criminal

¹⁵ See T. Ban, *Fraud committed through information systems and electronic means of payment – Legislative challenges of the digital age*, in Preventing and Combatting Cybercrime. The International Conference, Accent Publishing House, Cluj Napoca, 2016, pp. 264–274.

¹⁶ See Law No. 302/2004 on international judicial cooperation in criminal matters, republished in the Official Gazette Part I, No. 411 of 27 May 2019.

¹⁷ See M. C. Dănişor, *The Rule of Law – Guaranteeing Privacy in the Cyber Era*, in the Rule of Law in the Digital Era. The International Conference, Accent Publishing House, Cluj Napoca, 2016, pp. 118–136.

¹⁸ See I. Vasîu, *Hackers. Cybercriminals or rebels with a cause? (All about hackers)*, Nemira Publishing House, Bucharest, 2001, pp. 114–133.

phenomenon has arisen in order to formulate a plan to prevent such attacks. A number of theories have been formulated¹⁹ in the field of criminology related to cybercrime, in a multidisciplinary approach that allows the formulation of prevention models.

In this new domain, it is easy to understand that classical investigation models specific to the criminal prosecution phase, evidence gathering to determine judicial truth, and ultimately determining the perpetrator's identity cannot be applied. There is a fundamental need for adaptation of these investigation techniques to remote modes of operation, sometimes disguised by a series of interposed computer systems in the chain of connections from the attacker to the target computer system. Not only the sphere of criminal law needed an update and openness to new models to cope with the increasing wave of crimes committed through or against computer systems. Procedural criminal law also needed a paradigm shift regarding methods of criminal investigation²⁰ used to achieve the purpose provided for in art. 285 of the Criminal Procedure Code, namely the collection of necessary evidence, while respecting the principle of legality. This often involves the preparation of a well-elaborated and adapted investigation plan based on the actual reality of the offence that is the subject of criminal action.

Because in many situations, the evidence needed by law enforcement agencies is recorded through computer systems – sometimes even involuntarily, for example, continuous geolocation via GPS systems or network cells from mobile network operators – determining the commission of offenses under criminal law and, by extension, preventing their future commission can be achieved through specialized new methods such as those expressly provided by the legislator aimed at obtaining specific data related to internet traffic or location by collaborating with telecommunications service providers or by conducting digital searches on these systems.

Although in Romanian jurisprudence, there have been criminal cases related to the commission of illicit acts involving computer systems, they have often been initially classified as common crimes such as theft, fraud, without noting a criminal trend that would prompt the legislator to begin judicial practice establishing these acts as offenses previously incriminated before the year 2014 in special laws that transpose into Romanian legislation exactly the offenses that Romania has undertaken to incriminate through the Convention²¹ since 2001.

However, there are famous cases²² of such cases in British as well as American case law, even from the 1980s, and these can rightly be considered as

¹⁹ See A. C. Moise, *The criminological dimension of crime in cyberspace*, 2nd edition, C. H. Beck, Bucharest, 2020, pp. 67–85.

²⁰ See G. I. Ionita, *Cybercrime offences. Incriminating, investigating, preventing and combating*, 3rd edition, Universul Juridic Publishing House, Bucharest, 2018, pp. 216–222.

²¹ See European Convention on Cybercrime, Budapest, 2011.

²² See I. Vasiu, *op. cit.*, 1998, pp. 106–120.

pioneering cases for the formulation of modern criminal rules in the field of computer crime.

This makes it easier and easier for any operator to process extremely large amounts of data in an increasingly easy, fast and cost-effective way, without investing in economic know-how. All these are business opportunities, but at the same time they may also present concerns about how a satisfactory level of privacy could be ensured for personal data and thus, in the perspective of the GDPR Regulation (EU) 2016/679, all the rights of the data subjects of such processing could be respected.

Online activities are becoming the de facto standard of service for users, offering solutions that rely on revolutionary technologies such as cloud computing, social media, advertising and targeted promotion based on customer behaviour.

It is also necessary that in situations where controllers carry out special activities involving the processing of very large amounts of data, these controllers must identify exactly which of the data processed are subject to the GDPR and to what extent they are able to provide the level of security and protection of the IT system, data integrity and confidentiality of personal data.

There are a number of technologies that practically open the future to new possibilities for data processing, for new kinds of *knowledge* extracted from simple, but enormously collected computer data.

3. Legal threats and safeguards for security and privacy of devices and data

The advancement of technology undeniably presents a range of much-needed advantages that allow for the computerisation and automation of most data processing processes and even real-time self-checking maintenance.

The same advancement of technology and extremely easy access to information is encouraging more and more people to explore the criminal side of the digital age, encouraged by the fact that there are more and more ‘tutorials’ showing how to exploit vulnerabilities of various systems and, moreover, there are malware resource sites that allow a person to initiate a cyber attack without even average computer skills.

Faced with the new challenges and threats, legislators in European countries had to develop a common standard for protecting information systems against different types of attacks through the common assumption of criminalisation of these criminal acts committed against a computer system or using a computer system, and these standards were implemented in national legislation. In the case of Romania, they had their place in special laws, and after the transition to the current Criminal Code on 1 February 2014, they found their natural place in the organic criminal law.

Some of these systems are not essential – if the personal assistant makes

an unnecessary appointment, it is a trivial effort to cancel it. If the home automation system doesn't hit the right temperature, it's an acceptable inconvenience to make manual adjustments to match the environment. If the facial recognition system misfires and allows a criminal to pay to use your identity so that the bank authorises payments ordered by the criminal, it is a considerable inconvenience to resort to the legal protection mechanisms that the bank offers. If in a state of alert and emergency law enforcement will use autonomous drones that are not remotely controlled by human factors and that can decide²³ on their own when a person poses a threat to make use of the non-lethal weapons of peace or lethal weapons of war on hand, it becomes a matter of life and death if that drone makes the wrong decision and authorizes by its own decisions the use of firearms.

On the other hand, thanks to the computerisation of almost all sectors of the economy, every simple gesture we make in our daily routine generates enormous amounts of computer data, the value of which is determined by the organisation interested in buying it on the free market for personal data. Once in the hands of a marketer, this data can be used to target advertising messages to a specific category of consumers or even automatically to users who meet certain pre-defined conditions.

Such a practice may seem innocent, as most people are willing to give their personal data to any merchant offering a pen and a discount promotion. However, at this point in time, when social networks know worrying amounts of personal information about each of their users, this allows them to treat users differently, using algorithms that decide which content appears higher up, directly accessible and which content becomes hidden, perhaps even invisible.

Depending on the intentions of the buyer of this personal data, it can create the illusion of a bubble of like-minded friends or pave the way for 'fake news' disinformation campaigns with devastating consequences from the economy to the exercise of democratic rights. Information is power, and the will of the wielder dictates data processing.

This is the context in which we now find ourselves surrounded by 'smart' devices that make our lives easier, but to an appreciable extent make us dependent on access to these information systems.

In a computerised and ultra-connected democratic society, there is a need for state criminal legal protection against attacks on information systems and the unlawful processing of personal data.

Devices in IoT ecosystems are essentially systems that possess the ability to adapt to user preferences and behaviour, and this can be achieved by collecting an incredibly large amount of personal data of different natures on which they perform statistical and data mining processing to learn and subsequently intuit the needs of the end user.

²³ See Yaacoub J. P., Noura H., Salman O., Chehab A., *Security analysis of drones systems: Attacks, limitations and recommendations, in the Internet of Things*, Elsevier Public Health Emergency Collection, 11:100218, September 2020.

For example, a simple fitness bracelet has a large number of sensors that can record geolocation data such as GPS coordinates, the routes the wearer usually takes in a day, health data such as pulse, heart rate, sleep quality, blood pressure.

It is now publicly recommended by the competent authorities that any company, regardless of its size, should develop and adapt a set of²⁴ cybersecurity policies and procedures to protect both critical business data and any sensitive data, as their effectiveness has been proven, especially since an overwhelming percentage of security breaches could²⁵ be avoided.

Devices that are part of an IoT Ecosystems are devices that present an additional vulnerability precisely because of the ‘link’ they constantly have with the Internet network, practically providing an always open gateway to receive legitimate commands, but at the same time also presenting an additional risk, providing a ‘bridge’ of connection between people with illicit intentions, having their identity protected by the anonymity that the Internet offers, who may try to use this communication channel to make an illicit connection to this device that allows them to access computer data stored on this device.

From a criminal law perspective, the protection offered by the legislator is primarily to criminalise illegal access to a computer system, as a subsidiary offence often in order to commit other offences once in control of the computer system.

The majority of attacks against information systems in the Internet of Things ecosystems target this personal data, due to the fact that – as we have previously pointed out²⁶ – by their very nature these systems collect huge volumes of computer data, most of which is personal to the extent that it is correlated with other information. This information is collected from even the most mundane video surveillance systems which are now priced to allow any home user to be able to remotely video watch their own property, raising new challenges about how this data can be legally used.

This is the main argument that illegal access crimes directed against a smart device not only exist, but are increasing in frequency, as shown by various reports by IOCTA, SOCTA, CERT-RO and similar bodies, without questioning the ethical²⁷ elements of the attackers.

It is also a topical issue who should be responsible for preventing such

²⁴ See Online Trust Alliance – IoT Security & Privacy Trust Framework v2.5, Internet Society, 2017.

²⁵ See Online Trust Alliance - 2018 Cyber Incident & Breach Trends Report. Review and Analysis of 2018 Cyber Incidents and Key Trends to Address, 9 July 2019.

²⁶ See T. Ban, *Current Standards for Information Security and Privacy*, in Nina Gumzej, Olga Sovova (eds.), *Recent Debates in Cyberspace and Artificial Intelligence Law*, ADJURIS International Academic Publisher, Bucharest · Paris · Calgary, 2023, p. 53-71, <https://adjuris.ro/reviste/rdca/Recent%20debates%20in%20cyberspace%20and%20artificial%20intelligence%20law.pdf>.

²⁷ See X. Moldovan, *Towards a new digital ethic*, in Romanian Journal for Personal Data Protection, No. 1, Universul Juridic Publishing House, 2020, pp. 114–119.

cybercrime – a first option would be to hold the owners of the IT systems and communication networks responsible, and in case of non-compliance we should rely on compliance control bodies with administrative sanctions. A second way is for the judiciary to be given the power to respond proportionately²⁸ to the seriousness of the crime in the hope of reducing the prevalence of these crimes, which has so far been achieved to a questionable extent.

Of course, in practice the answer is unanimous that a comprehensive approach to preventing cyber-attacks must be taken both through continued concern for the implementation of security policies and procedures on the part of organisations or end users of legally protected devices and systems due to the extremely dangerous nature if used for illicit purposes.

The advantages offered by technology and the accessibility with which an individual user can start using these new services without prior training often neglects the aspect of educating²⁹ users about online safety issues and the protective measures they can take³⁰ to secure their computer network and increase confidence in the privacy of their personal data. Even small and medium-sized entrepreneurs cannot neglect the need to secure the IT systems they own, and there are explicit recommendations including government³¹ recommendations to this effect.

It must become clear that any user who connects to technology and services offered online, whether this is in the context of carrying out work tasks or in their private life, can always become a target of cyber-attacks³² or online fraud, sooner or later.

Fortunately, the European Union has an active policy to increase its defences against these cyber attacks, developing a strategy³³ which has among its main objectives the protection of critical sectors which now includes the 5G mobile communications and network segment and the interconnected Internet of

²⁸ See A. Cobuz Băgnaru, *The indissoluble link between the need to protect personal data and resistance to cybercrime*, in Romanian Journal for the Protection of Personal Data, No. 1, Universul Juridic Publishing House, 2020, pp. 100–105.

²⁹ See Cybersecurity Framework Platform by the National Institute of Science and Technology (NIST) USA available at <https://www.nist.gov/cyberframework>.

³⁰ See E. Kritzinger, S. Solms, *Cyber Security for home users: A new way of protection through awareness enforcement*, November 2010, in Computers & Security 29(8), p. 840, 847, available via ResearchGate at https://www.researchgate.net/publication/222706832_Cyber_security_for_home_users_A_new_way_of_protection_through_awareness_enforcement.

³¹ See the Cyber Security Planning Guide produced by the U.S. Government, Federal Commission for Commerce (FCC), with input from the Department of Homeland Security, the National Cyber Security Alliance and The Chamber of Commerce, available at <https://www.fcc.gov/sites/default/files/cyberplanner.pdf>.

³² See B. Obotivere, A. Nwaezeigwe, *Cyber Security Threats on the Internet and Possible Solutions*, September 2020 in International Journal of Advanced Research in Computer and Communication Engineering, Vol. 9, Issue 9, 2020, available via ResearchGate at https://www.researchgate.net/publication/346861524_Cyber_Security_Threats_on_the_Internet_and_Possible_Solutions.

³³ See The EU Cybersecurity Strategy for the Digital Decade, December 2020, available at <https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0>.

Things devices³⁴.

The European Union has succeeded through the drastic reform imposed by Regulation (EU) 2016/679 GDPR and respectively the NIS and NIS2 Directive (soon to be implemented in Romanian law by October 2024 at the latest) to impose much more stringent rules on the ways in which personal data controllers will be able to continue processing personal data, being mandatory to provide a set of safeguards to respect the rights of data subjects.

4. Lessons learned

Even if we hypothetically accept that it is a technology that brings security breaches into our own lives and economic activity, foregoing these benefits is not the solution. There have also been opinions that have considered whether we are safer using computer systems that are not connected to absolutely any form of network or form of communication with other computer systems, in the hope that physical security measures might be sufficient to stop attackers.

Analysing existing studies and recommendations, two general but perfectly valid conclusions can be drawn in the context of cyber safety and security:

The first conclusion is that technology and information systems, interconnected devices and the global network of interconnected sensors offer both fantastic opportunities, but at the same time the threats are real.

The European Union, as the general guarantor of cybersecurity and privacy of personal data, is constantly monitoring new threats and contributing with increasingly specific legislation.

On 22 March 2021 the European Union adopted conclusions³⁵ on the cyber security strategy. *Building a resilient, green and digital Europe* is confirmed as a key strategic objective.

The aim is³⁶ to reduce the number of security breaches while increasing resilience to cyber attacks. It is already not only proven, but accepted and assumed that in the near future the number of cyber attacks will increase dramatically, that they will be difficult to stop, almost impossible to detect at times and can have extremely serious consequences.

The second conclusion is that educating, empowering and encouraging individual and small- and medium-sized corporate users about the measures they can implement and creating a corporate culture of attack prevention is the most

³⁴ See Outcome of Proceedings Council conclusions on cyber security of connected devices, Council of the European Union, December 2020, available at <https://www.consilium.europa.eu/ro/press/press-releases/2020/12/02/cybersecurity-of-connected-devices-council-adopts-conclusions/>.

³⁵ See Council conclusions on EU Cybersecurity Strategy for the Digital Decade, Council of the European Union, available at <https://data.consilium.europa.eu/doc/document/ST-6722-2021-INIT/en/pdf>.

³⁶ See Challenges to effective EU cybersecurity policy, briefing report by the European Court of Auditors, March 2019, available at https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf.

effective way to achieve quick but highly effective results.

So, the European Union, through its specialised agencies, has started an aggressive information and education campaign by urging people to act (call to action campaigns) but also by providing highly detailed and accessible guides to help the average user take the first essential steps towards securing their computer networks and the interconnected information systems and devices in the Internet of Things ecosystem.

This responsibility for the security of their own IT networks is, however, also laid down in the main EU Directives and Regulations (e.g. NIS, NIS2, GDPR and others). Now users are taught concrete and WHAT they can do to understand the threats and HOW to take the necessary action.

Open access to official, verified and secure information through official guidelines covers all new technologies such as the Internet of Things³⁷ ecosystems and interconnected³⁸ devices, recommendations on³⁹ cybersecurity challenges, concrete practical recommendations⁴⁰ for securing⁴¹ the Internet of Things devices respecting the Privacy by Design principle, cybersecurity recommendations for the⁴² Internet of Things devices market to reduce the risks of supply chain attacks.

There are a number of tools to prevent cyber-attacks on devices in the Internet of Things ecosystems, broadly grouped under the category of reasonable security measures⁴³, which are extra important now especially in the current increasingly context of home and office automation, both virtual and physical.

The notion of a ‘reasonable’ level of security is a concept that recent European directives bring to the fore. The standard to which the European legislator is moving is that of a ‘reasonable’ level and not that of the highest theoretical level of security, which becomes excessive both in terms of the actual methods of implementation⁴⁴. And in terms of cost, given the specific size of an organisation, the volume of personal data collected and processed and the harmonisation

³⁷ See Baseline Security Recommendations for IoT, ENISA, November 2017, report available at <https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot>.

³⁸ See IoT Security Standards Gap Analysis, ENISA, January 2019, report available at <https://www.enisa.europa.eu/publications/iot-security-standards-gap-analysis>.

³⁹ See Industry 4.0 – Cybersecurity Challenges and Recommendations, ENISA, May 2019, report available at <https://www.enisa.europa.eu/publications/iot-security-standards-gap-analysis>.

⁴⁰ See Good Practices for Security of IoT – Secure Software Development Cycle, ENISA, November 2019, report available at <https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot-1-2>.

⁴¹ See Guidelines for Securing the Internet of Things, ENISA, November 2020, report available at <https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things>.

⁴² See EU Cybersecurity Market Analysis – IoT in Distribution Grid, ENISA, April 2022, available at <https://www.enisa.europa.eu/publications/eu-cybersecurity-market-analysis-iot-in-distribution-grid-2>.

⁴³ See also the NIS Directive (EU 2016/1148) which defines risk as any *reasonably identifiable* circumstance in Article 4(9).

⁴⁴ See EU Directive 2016/679 General Data Protection Regulation which imposes ‘reasonableness’

with other data protection methods provided for by the European legislator such as anonymisation, pseudonymisation, encryption.

The role of reasonable security measures is especially important given that some devices in the Internet of Things ecosystems are purchased expressly to control other devices, based on a ‘trust⁴⁵’ relationship between devices that the user establishes.

A very relevant example of this is voice-activated ‘personal assistant’ devices, connected both to the internet and via ‘trusted⁴⁶’ relationships to other devices such as thermostats, smoke sensors, water sensors, window intrusion sensors, ventilation systems, external window blinds actuation systems and even home alarm systems and remote control of ‘smart’ central locking systems for external building access doors.

Compromising these types of devices will allow an attacker a default control relationship over all other devices in a ‘trusted’ relationship with the compromised personal assistant device, such as Google Home, Amazon Alexa, Apple Homepod and others.

Unfortunately, the reality is that simply educating and bringing to the public’s attention the problems that can arise in the case of unsecured networks or computing devices, non-compliance with the standards required by the GDPR for personal data processing is not enough.

A punitive state repressive component is also absolutely necessary as a response to culpable or bad faith failure to comply with these minimum standards.

On the one hand, making people accountable in terms of fines and administration is a first course of action. Under the regulations of Regulation (EU) 2016/679 GDPR and the NIS and NIS Directive², governmental and union-level entities are established that have the exact powers to control and sanction contravention and administrative offenders.

At the same time, accountability can also be achieved by criminalising certain activities, and it should be noted that even the mere possession of malicious software for the purpose of committing some of the offences provided for by criminal law against information systems is criminal.

Since crimes committed through computer systems can transcend geographical boundaries, an attacker can compromise a computer system remotely without having to be physically present in the vicinity.

For this reason, offences committed through or on computer systems are

as a standard for security measures to be taken to ensure data security, for time limits within which a controller must respond or disputes must be resolved, for a number of fees charged to respond to manifestly unfounded or excessive requests.

⁴⁵ See V. Engen, J. B. Pickering, P. Walland, *Machine Agency in Human Machine Networks. Impacts and Trust implications*, in Human Computer Interaction Novel User Experiences, 18th International Conference, HCI International, 2016, Toronto, Canada, Proceedings, p. 103.

⁴⁶ See Y. Liao, J. Vitak, P. Kumar, M. Zimmer, K. Kritikos, *Understanding the Role of Privacy and Trust in Intelligent Personal Assistant Adoption*, in Proceedings of the 13th Annual iConference, Lecture Notes in Computer Science, vol. 11,420, pp. 102-113.

most often criminal offences that have elements of foreignness and pose significant problems in terms of spatial application of criminal law and the practical establishment of effective jurisdiction.

In practice, this aspect is essential because it provides a concrete answer to the question of *which legal system should be applied in a specific situation*, which is essential when we have to relate the objective and subjective typicality in order to determine whether the act constitutes a crime, what is the legal framework of this act and, of course, from there, the concrete conditions of the application of the various institutions of substantive criminal law and criminal procedural law.

The solution is, of course, easy to see, interstate cooperation in criminal cases to stop cross-border crime, simplifying procedures with foreign elements, especially between EU Member States. Fortunately, these steps are already being taken and the legislative framework is increasingly adapted to the specific needs of investigations.

Bibliography

1. Ban, T., *Current Standards for Information Security and Privacy*, in Nina Gumzej, Olga Sovova (eds.), *Recent Debates in Cyberspace and Artificial Intelligence Law*, ADJURIS International Academic Publisher, Bucharest · Paris · Calgary, 2023, p. 53-71, <https://adjuris.ro/reviste/rdca/Recent%20debates%20in%20cyberspace%20and%20artificial%20intelligence%20law.pdf>.
2. Ban, T., *Fraud committed through information systems and electronic means of payment – Legislative challenges of the digital age*, in Preventing and Combating Cybercrime. The International Conference, Accent Publishing House, Cluj Napoca, 2016, pp. 264–274.
3. Ban, T., *The digital future of law between the opportunities of the cyber era and the acute need for security*, in Curierul Judiciar, no. 6, 2020, pp. 339–345.
4. Ciurea, A., *The Digital Age and Justice (I). Objectives, algorithm design methods and consequences of their use in justice*, in Revista Universul Juridic, No. 1 January 2022, pp. 56–70, available at http://revista.universuljuridic.ro/wp-content/uploads/2022/03/06_Revista_Universul_Juridic_nr_1-2022_PAGINAT_B_T_A_Ciurea.pdf.
5. Cobuz Băgnaru, A., *The indissoluble link between the need to protect personal data and resistance to cybercrime*, in Romanian Journal for the Protection of Personal Data, No. 1, Universul Juridic Publishing House, 2020, pp. 100–105.
6. Dănișor, M. C., *The Rule of Law – Guaranteeing Privacy in the Cyber Era*, in the Rule of Law in the Digital Era. The International Conference, Accent Publishing House, Cluj Napoca, 2016, pp. 118–136.
7. Engen, V., J. B. Pickering & P. Walland, *Machine Agency in Human Machine Networks. Impacts and Trust implications*, in Human Computer Interaction Novel User Experiences, 18th International Conference, HCI International, 2016, Toronto, Canada, Proceedings.
8. Ionita, G. I., *Cybercrime offences. Incriminating, investigating, preventing and combating*, 3rd edition, Universul Juridic Publishing House, Bucharest, 2018.

9. Kritzinger, E. & S. Solms, *Cyber Security for home users: A new way of protection through awareness enforcement*, November 2010, in *Computers & Security* 29(8), pp. 840-847, available via ResearchGate at https://www.researchgate.net/publication/222706832_Cyber_security_for_home_users_A_new_way_of_protection_through_awareness_enforcement.
10. Liao, Y., J. Vitak, P. Kumar, M. Zimmer & K. Kritikos, *Understanding the Role of Privacy and Trust in Intelligent Personal Assistant Adoption*, in *Proceedings of the 13th Annual iConference, Lecture Notes in Computer Science*, vol. 11, 420, pp. 102-113.
11. Moise, A. C., *The criminological dimension of crime in cyberspace*, 2nd edition, C. H. Beck, Bucharest, 2020.
12. Moldovan, X., *Towards a new digital ethic*, in *Romanian Journal for Personal Data Protection*, No. 1, Universul Juridic Publishing House, 2020, pp. 114–119.
13. Obotivere, B. & A. Nwaezeigwe, *Cyber Security Threats on the Internet and Possible Solutions*, September 2020 in *International Journal of Advanced Research in Computer and Communication Engineering*, Vol. 9, Issue 9, 2020, available via ResearchGate at https://www.researchgate.net/publication/346861524_Cyber_Security_Threats_on_the_Internet_and_Possible_Solutions.
14. VasIU, I., *Criminalitatea informatică*, Ed. Nemira, Bucharest, 1998.
15. VasIU, I., *Hackers. Cybercriminals or rebels with a cause? (All about hackers)*, Nemira Publishing House, Bucharest, 2001.
16. Voigt, P. & A. Bussche, *The EU General Data Protection Regulation (GDPR). A practical guide*, Springer International Publishing, 2017.
17. Yaacoub, J. P., Noura H., Salman O. & Chehab A., *Security analysis of drones systems: Attacks, limitations and recommendations, in the Internet of Things*, Elsevier Public Health Emergency Collection, 11:100218, September 2020.

Artificial Intelligence - The Era of Social Inequalities. In Regulating the Future, We Need to Look at the Risks

Associate professor **Carmen Oana MIHĂILĂ**¹
Lecturer **Mircea MIHĂILĂ**²

"All human beings are born free and equal in dignity and rights."
Universal Declaration of Human Rights

Abstract

AI brings ethical and legal issues, the discrimination, and workplace safety risks. Decision making through AI techniques is changing the relationships between individuals as we know them today. The development of AI and the integration of these systems into essential services for the population can accentuate imbalances in society and between states. Generating certain predictive models by identifying patterns in the collected data and grouping people in this way can lead to discrimination against certain groups (bias can be encoded in algorithms). Errors or biases may also occur that affect the integrity and confidentiality of information where it is difficult to understand how AI makes data security decisions. In the absence of human supervision and boundary drawing, autonomous AI may hold big surprises. The article will analyse some aspects related to the risks that the use of AI systems involves on fundamental rights, with reference to private life, data protection, non-discrimination regarding and to the effects that the development of AI has in creating new social inequalities.

Keywords: artificial intelligence system, privacy, discrimination, profiling, labour market, social inequalities.

JEL Classification: K24, K38

DOI: <https://doi.org/10.62768/ADJURIS/2024/1/03>

Please cite this article as:

Mihăilă, Carmen Oana & Mircea Mihăilă, „Artificial Intelligence - The Era of Social Inequalities. In Regulating the Future, We Need to Look at the Risks”, in Pajuste, Tiina, Heliona Bellani (Miço) & Sejla Maslo Cerkić (eds.), *Legal Perspectives in the Modern Era of Technological Transformations*, ADJURIS – International Academic Publisher, Bucharest, Paris, Calgary, 2024, p. 39-63.

¹ Carmen Oana Mihăilă - Department of Juridical and Administrative Sciences, Faculty of Law, University of Oradea, Romania, carmen.oana.mihaila@gmail.com; <https://orcid.org/0000-0002-4387-9575>.

² Mircea Mihăilă - Department of Computers and Information Technology, Faculty of Electrical Engineering and Information Technology, University of Oradea, mircea.mihaila@uoradea.ro.

1. Introduction

“Artificial intelligence system (AI system) means a machine-based system that is designed to operate with varying levels of autonomy and that can, for explicit or implicit objectives, generate outputs such as predictions, recommendations, or decisions, that influence physical or virtual environments”- this is the definition found in Amendment 165 to the *Proposal for a Regulation of the European Parliament and of the Council establishing laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union legislative acts* - (hereinafter - *AI Law*)³.

Medicine, education, design, transport, trade, agriculture, media, no matter which field we look at, AI has conquered important territory, with a market of approximately 191 billion USD expected in 2024⁴.

From the concept of science fiction, AI has become a force that influences history, but at the same time it is seen as a threat, a risk to humanity. Is AI “altering” our thinking and consciousness?⁵

Yet is this really how this unprecedented development should be viewed?

Interferences in people's private lives have been highlighted in recent years with the development of digital tools, especially AI. Collection and analysis of personal data, video surveillance systems, evaluation of candidates for employment, advertising and marketing, analysis of medical data, creation of profiles, evaluation of social behaviour or manufacture of images that may affect a person's reputation through the use of deep fake, etc., there are only a few examples that could affect the fundamental rights of natural persons, giving rise to material or immaterial damages, including physical, psychological, societal or economic damages.

2. What do the European regulations provide?

European Digital Rights (EDRi) and 119 other civil society organizations launched a collective statement in 2021 to call for an Artificial Intelligence Act

³ Amendments adopted by the European Parliament on 14 June 2023 on the Proposal for a Regulation of the European Parliament and of the Council on laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM – 2021 – 0206 – C9-0146/2021 – 2021/0106 – COD), 14 June 2023, document available online at https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.html, accessed on 11 February 2024.

⁴ WIPO, *Frontier Technologies Factsheet*, 2023, document available online at https://www.wipo.int/export/sites/www/about-ip/en/frontier_technologies/pdf/frontier-tech-6th-factsheet.pdf, accessed on 10 February 2024.

⁵ Ramona Duminică, Diana M. Ilie, *Freedom of thought, conscience and religion, 'resized' by the perspective of regulation of a 'right of the soul' – transdisciplinary analysis*, 'Journal of Law and Administrative Sciences' 20, 2023, 81–124, 111.

(AIA) that prioritizes fundamental rights, and adopts a coherent, flexible and prepared for the future of the "risk" of artificial intelligence systems.⁶

*The UNESCO Recommendation on the Ethics of Artificial Intelligence (UNESCO, 2021)*⁷ establishes among the values and principles that should be respected by all actors in the life cycle of the AI system: respect, protection and promotion of human rights and fundamental freedoms and human dignity; ensuring diversity and inclusion of peaceful society; proportionality and the prohibition of harm; safety and security; fairness and non-discrimination; the right to privacy and data protection; human oversight and determination; responsibility and accountability.

Another important document is the *White Paper on Artificial Intelligence*⁸, part of the European Digital Strategy for the development and application of safe and trustworthy AI, which states that AI „entails a number of potential risks, such as opaque decision-making, gender-based or other kinds of discrimination, intrusion in our private lives or being used for criminal purposes”.

*The proposal for a Regulation of the EP and of the Council establishing harmonized rules on Artificial Intelligence*⁹ - the AI Law and the adopted Amendments to the AI Law set among their important objectives the respect for the fundamental rights of individuals, non-discrimination, protection of personal data and transparency.

The AI Law points out that AI systems that provide an assessment of the social behaviour of individuals for general purposes by or on behalf of public authorities "may violate the right to dignity and non-discrimination, as well as the values of equality and justice." In the Amendments adopted to IA Law, it is explicitly stated that the regulation will not affect the fundamental rights to private life and the protection of personal data, as provided for in the Union law on the protection of data and private life and enshrined in the Charter of Fundamental Rights of the European Union.¹⁰

The European Commission for the Efficiency of Justice adopted in 2018 the *European Ethical Charter on the use of AI in the judicial system and in connection with it*¹¹, the first text that establishes ethical principles regarding the use

⁶ *Civil society calls on the EU to put fundamental rights first in the AI Act*, document available online at <https://edri.org/our-work/civil-society-calls-on-the-eu-to-put-fundamental-rights-first-in-the-ai-act/>, accessed on 10 February 2024.

⁷ UNESCO, *Recommendation on the Ethics of Artificial Intelligence*, 2021, document available online at https://www.cnr-unesco.ro/uploads/media/f1077_recomandari-unesco-ai-site.pdf, accessed on 11 February 2024.

⁸ European Commission, *White Paper on Artificial Intelligence – A European approach to excellence and trust*, Brussels, 19.2.2020, COM(2020) 65 final.

⁹ Proposals for Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (*Artificial Intelligence Act*) and amending certain Union legislative acts, COM(2021)0106 (COD)/206; Brussels, 21.4.2021). Recital 17.

¹⁰ Amendment 7, *IA Law*, Recital 2 b.

¹¹ CEPEJ, *European Ethical Charter on the use of Artificial Intelligence in judicial systems and their environment*, document available online at <https://rm.coe.int/ethical-charter-en-for-publica>

of AI in judicial systems.

Unfortunately, there are no single universal rules regarding the use of AI, most of the time they only have a recommendation character.¹²

The right to privacy and the right to data protection are strongly impacted by the collection, analysis and use of personal data using AI algorithms, for various purposes, but also by the use of facial recognition techniques (remote identification).

Local government, police stations, hospitals, pharmacies, airports, smart cities, all use facial recognition technology and the analysis of large amounts of data, creating the possibility of privacy and a sense of abuse. Surprising or not, it is the fact that among the states that invest heavily in AI surveillance techniques are also the weakest financially but with authoritarian systems.¹³ According to some authors¹⁴, surveillance systems operate by abstracting human bodies from their territorial framework, separating them into a series of flows that will be re-assembled. The process transforms the body and the individual into a new kind of entity that is "pure information." In this context, the authors suggest that the individual should be differentiated from the data generated by the AI ensemble.

The increasing use of new technological tools and AI for security, border control or access to social services has the potential to increase racism, racial discrimination¹⁵, xenophobia and other forms of exclusion, according to the Recommendation on Preventing and Combating Racial Profiling by Law Enforcement Officials.¹⁶

The European Court of Human Rights has shown that "the rapid development of increasingly sophisticated techniques that allow, among other things, facial recognition and facial mapping techniques to be applied to people, to photos of people, makes their photography, as well as the storage and the possible diffusion of the resulting data, problematic."¹⁷

tion-4-december-2018/16808f699c, accessed on 11 February 2024.

¹² Nataliia Martsenko, *Artificial Intelligence and human rights: a scientific review of impacts and interactions*, 'Studia Prawnoustrojowe' 58, 2022, 322, DOI: 10.31648/sp.8245.

¹³ Steven Feldstein, *The Global Expansion of AI Surveillance*, 'Carnegie Endowment for International Peace', Sept. 1019, 2019, 8, document available online at https://carnegieendowment.org/files/WP-Feldstein-AISurveillance_final1.pdf, accessed on 11 February 2024.

¹⁴ Kevin D. Haggerty, Richard V. Ericson, *The Surveillant Assemblage*, 'British Journal of Sociology' 51(4) (2000): 606, 613, DOI: 10.1080/00071310020015280.

¹⁵ See Sebastian Benthall, Bruce D. Haynes, *Racial Categories in Machine Learning*, 'FAT* '19: Proceedings of the Conference on Fairness, Accountability, and Transparency', Associations for Computing Machinery 9, 2019, <https://doi.org/10.1145/3287560.3287575>. The authors relate, for example, that Facebook introduced a feature in its advertising platform that allowed targeting of people in the United States based on racial criteria – 'ethnic affinity': African American, Hispanic, or Asian American, a feature that could be used to racially discriminate in housing advertising. Basically, real estate agents had ad targeting options that allowed them to exclude non-white groups such as blacks, Asians and Hispanics.

¹⁶ Committee on the Elimination of Racial Discrimination, *General Recommendation No. 36 (2020) on Preventing and Combating Racial Profiling by Law Enforcement Officials*, para. 12.

¹⁷ ECtHR, Guide to the Case Law of the European Court of Human Rights, Data protection, 86,

The risk classification of AI systems in the AI Law is particularly important for both software developers and users of AI systems, and the prohibition of certain AI systems, or the imposition of strict requirements, are intended to prevent possible violations of people's rights and abuses.¹⁸

It is thus prohibited according to art. 5 of the IA Law, the use of "real-time" **remote biometric identification systems** in publicly accessible spaces.

The notion of a *remote biometric identification system* is defined in the Amendments to the AI Law as: a *system intended for the identification of natural persons at a distance through the comparison of a person's biometric data with the biometric data contained in a reference database, and without prior knowledge whether the targeted person will be present and can be identified, irrespectively of the particular technology, processes or types of biometric data used, excluding verification systems which merely compare the biometric data of an individual to their previously provided biometric data (one-to-one)*.¹⁹

We already know that the rights and freedoms of individuals are significantly affected by the use of these systems for the "real-time" biometric identification of natural persons in publicly accessible spaces. Their prohibition is justified both by the violation of the right to private life, the right to freedom of assembly, but also by the erroneous results they sometimes generate, depending on age, sex, ethnicity, or disabilities²⁰. Regarding the prohibition of AI systems for analysing images recorded in publicly accessible spaces by means of "post" remote biometric identification systems, the regulation establishes an exception regarding the existence of a possible prior judicial authorization for use in the context of law enforcement, unless there is pre-judicial authorisation for use in the context of law enforcement, when strictly necessary for the targeted search connected to a specific serious criminal offense that already took place, and only subject to a pre-judicial authorisation.

Biometric classification systems that classify natural persons based on sensitive or protected attributes or characteristics or based on the inference of such attributes or characteristics (except for AI systems intended to be used for therapeutic purposes approved on the basis of specific informed consent cause of natural persons). Biometric categorisation means assigning natural persons to specific categories or inferring their characteristics and attributes on the basis of their biometric or biometric-based data, or which can be inferred from such data.

Artificial intelligence systems that create or expand **facial recognition** databases by directly extracting facial images from the Internet or CCTV footage are also prohibited.

document available online at https://www.echr.coe.int/documents/d/echr/Guide_Data_protection_ENG, accessed on 14 February 2024.

¹⁸ Raluca Anderco, *Inteligența artificială - ce probleme atrage lipsa cadrului legislativ*, 'Revista Universul Juridic' 10 October 2023, 69–77, 73–74.

¹⁹ Amendment 24, *IA Law*, Recital 8.

²⁰ Amendment 41, *IA Law*, Recital 18.

We must mention that facial images are not simple photographs, they represent biometric data through processing with technical means that allow the unique identification or authentication of a person,²¹ the source of this data can include both physical and psychological or behavioural elements²². Biometric data for the unique identification of the natural person cannot be processed, as stipulated in Article 9 para. (1) of the GDPR.²³

Profiling and discrimination. Another category of banned AI systems are those that can implement **subliminal and manipulation techniques**. AI systems capable of **monitoring and profiling natural persons** and AI systems targeting **vulnerable groups** also fall under the same classification.

Also, the 2021 *Report of the UN High Commissioner for Human Rights on the right to privacy in the digital age* looks at the effects of the widespread use of AI, including profiling or automated data collection, on the realization of the right to privacy.

Profiling, that is the use of automatic collection processes to process data available on the Internet and build profiles, can also lead to discrimination. According to Article 22 of the GDPR, automated decisions, including profiling, must not be based on sensitive data, and the operator is obliged to ensure measures to protect the rights, freedoms and legitimate interests of the data subject.

Profiling individuals, creating detailed user profiles (based on various criteria such as age, gender, location, interests, behaviours or other demographic and behavioural characteristics) may be used to predict their behaviours and preferences and may be used for targeted marketing, manipulation or discrimination, thereby affecting individual autonomy and freedom. For example, online services

²¹ Council of Europe, Directorate General of Human Rights and Rule of Law Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data. Convention 108, Guidelines on Facial Recognition, T-PD (2020)03rev4 28 January 2021, 3, the document is available online at <https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3>, accessed on 14 February 2024.

²² Article 29 Data Protection Working Party, Opinion 3/2012 on developments in biometric technologies, 00720/12/EN, WP193, Brussels, 27 April 2012, 4, <https://www.pdpjournals.com/docs/87998.pdf>.

²³ Article 9 para. (1) of GDPR: ‘Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation shall be prohibited.’ The European Parliament Resolution of 25 March 2021 on a European strategy for data 2020/2217 (INI) (2021/C 494/04), recalls that the processing of special categories of personal data under Article 9 of the GDPR is in principle prohibited, with certain strict exceptions, which involve specific processing rules and always include the obligation to conduct a data protection impact assessment; highlights the potentially disastrous and irreversible consequences of wrongful or unsecured processing of sensitive data for the individuals concerned – paragraph 33.

that use personalized rating systems are likely to lead to discriminatory practices.²⁴

Fundamental rights protected by the Charter are also adversely affected by **AI systems classified as high risk** in the new artificial intelligence law. AI systems identified as high risk refer to AI used in the education or training system, product safety, employment, worker management and access to self-employment, credit scoring, migration, asylum and border control²⁵, administration of justice and democratic processes.

Special attention will also be paid to biometric systems and biometric-based systems that are classified as high risk.

High-risk AI systems will also be considered those systems used to make decisions in determining the eligibility of natural persons for health and life insurance, with a discriminatory effect by limiting access to healthcare or by perpetuating discrimination based on personal characteristics. The AI systems used to evaluate and classify the emergency calls of natural persons will also be classified as high risk, but also those systems used in establishing the priorities of the beneficiaries of emergency services, because they make decisions in very critical situations for the life and health of individuals and their goods²⁶.

Freedom of expression and the right to information are influenced by the presence of AI algorithms and personal data processing techniques. The right to send and receive information is limited by the operation of those search engines that only show us certain types of content (filtering content from social media platforms through automatic processes). User preferences are thus used to personalize the results of online searches, whether we are talking about social media or news channels, limiting the right to information.

According to a 2015 UK Parliament Report,²⁷ there are automated techniques for identifying extremist or illegal content (that incites violence), techniques that even have the ability to automatically suspend that particular user.

The exercise of freedom of expression and the right to information may be subject to formalities, conditions, restrictions or sanctions, under the terms of

²⁴ Alex Rosenblat, Karen Levy, Solon Barocas, Tim Hwang, *Discriminating Tastes: Uber's Customer Ratings as Vehicles for Workplace Discrimination*, 'Policy & Internet', 9(3), January 2017, p. 256-279; DOI: 10.1002/poi3.153; Council of Europe, *Algorithms and Human Rights. Study on the human rights dimensions of automated data processing techniques and possible regulatory implications*, March 2018, 27, the document is available online at <https://rm.coe.int/algorithms-and-human-rights-en-rev/16807956b5>, accessed on 11 February 2024.

²⁵ According to Amendment 70 to the AI Law, those people to whom AI systems are applied for the management of migration, asylum and border control are also in a vulnerable situation.

²⁶ Amendment 67, *Law IA*, Recital 37.

²⁷ *UK Intelligence and Security Committee of Parliament Report, Privacy and Security: A modern and transparent legal framework*, March 2015, the document is available online at https://isc.independent.gov.uk/wp-content/uploads/2021/01/20150312_ISC_PSRptweb.pdf, accessed on 13 February 2024.

Article 10 (2) of the ECHR. These restrictions must be proportionate to the legitimate aim pursued and correspond to an urgent need. For example, in an attempt to remove illegal content, such as hate speech or extremists, online platforms monitor all communication flows to be able to detect this illegal content.²⁸

In addition, algorithms are not yet able to distinguish between hateful content and a pamphlet or simple critical analysis, and there is a risk of removing such content as well.

Freedom of assembly and the right to protest are also curtailed by the use of facial recognition systems. In Hong Kong, during a 2019 protest, protesters covered their faces and disabled facial recognition logins on their smartphones to prevent access by law enforcement, but at the same time took photos of police officers who had no badge and used facial recognition techniques to expose their identity online.²⁹ Closely related to these rights is the possibility of using AI algorithms to spread false information online, precisely to undermine protest movements. These AI algorithms are also used to censor or restrict online content associated with certain protests, so they can be programmed to do so, limiting individual rights to freedom of expression and access to information.

In the **justice system and crime prevention**, the use of AI algorithms has attracted a lot of criticism, especially related to the right to a fair trial, the presumption of innocence, or the right to defence (Article 5 of the ECHR - the right to liberty and security, Article 6 of ECHR - the right to a fair trial). Fundamental rights and the functioning of criminal justice can also be affected by AI technologies aimed at searching for suspects in databases, voice identification, identifying victims of human trafficking, monitoring social media platforms.³⁰ AI systems can be found from the document submission process, to determining offenders' recidivism risks. *The European Parliament's*³¹ *resolution on artificial intelligence in criminal law and its use by police and judicial authorities in criminal proceedings*, showed as early as 2021 that there are tools and applications in the field of AI that are used by some judicial systems (for example to substantiate detention orders preventive measures, establishing punishments, calculating recidivism probabilities, determining the probation period, online dispute resolution, etc.³²) Yet, at the same time, there are risks related to data leaks, data security

²⁸ *Algorithms and Human Rights. Study on the human rights dimensions of automated data processing techniques and possible regulatory implications*, 2018, 20.

²⁹ Paul Mozur, *In Hong Kong Protests, Faces Become Weapons*, 'New York Times', July 26, 2019, the document is available online at <https://www.nytimes.com/2019/07/26/technology/hong-kong-protests-facial-recognition-surveillance.html>, accessed on 13 February 2024.

³⁰ Committee on Civil Liberties, Justice and Home Affairs, *Report on Artificial Intelligence in Criminal Law and its use by the Police and Judicial Authorities in Criminal Matters*, 13.7.2021 – (2020/2016 – INI), the document is available online at https://www.europarl.europa.eu/doceo/document/A-9-2021-0232_EN.html, accessed on 13 February 2024.

³¹ European Parliament *Resolution of 6 October 2021 on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters* (2020/2016 – INI), Strasbourg.

³² Cristian Miheș, *Considerații asupra necesității adaptării unor instituții tradiționale ale dreptului*

breaches and unauthorized access to personal data and to other information related to, for example, criminal investigations or court cases that are processed through AI-based systems.

The right of access to a court is influenced by the implementation of AI systems. As stated in the doctrine³³, the fundamental right of access to a court and the formal procedural requirements must be balanced, the simple mechanical application of the procedural rules, without an appreciation from the human factor, not being consistent with the ECHR jurisprudence.

It is even circulated that in addition to the possibility of assisting judges or lawyers in a trial, AI systems may even take their place in the not too distant future. Replacing lawyers is not necessarily the ideal solution, as the AI system lacks subjectivity.

The robot lawyer on DoNotPay (online legal service) uses AI to challenge parking fines and provide various other legal services. However, in 2023 the company was sued in a San Francisco court for misleading customers³⁴.

Robo-judges, as they are also called, could be impartial and give a fair verdict, and a small company could win its case against one that has an army of lawyers behind it³⁵. And yet, as the literature³⁶ states, "algorithms cannot discern between moral and immoral, legal or illegal, fair or unfair." People need to be able to make their own assessments, not just rely on recommendations generated by AI algorithms.

The AI algorithms used to determine decisions of the European Court of Human Rights are also used to triage cases and prioritize those with the highest chance of success, which could affect a person's right to be heard.³⁷ It is expected that in the future, there will be AI-powered portals to solve simple cases quickly and efficiently.³⁸

In the US, Correctional Offender Management Profiling for Alternative

penal în condițiile societății dominate de tehnologia informației, in Flaviu Ciopec, Laura-Maria Stănilă, Ioana-Celina Pașca, *Previzibilitatea legislației și jurisprudenței în materie penală*, Universul Juridic, Bucharest, 2019, p. 103–118.

³³ Ioana Ciutacu, *Efectele implementării inteligenței artificiale în justiție asupra drepturilor fundamentale și asupra drepturilor procedurale*, "Avocatul", June 2022, p. 51.

³⁴ Faridian v. DoNotPay, Inc (3:23-cv-01692), the document is available online at <https://www.courtlistener.com/docket/67158596/faridian-v-donotpay-inc/>, accessed on 15 February 2024.

³⁵ Max Tegmark, *Life 3.0: being human in the age of artificial intelligence*, Alfred A. Knopf, New York, 2017, 138.

³⁶ Ovidiu Predescu, Ovidiu R. Predescu, *Inteligența artificială azi. O perspectivă a dreptului, a drepturilor omului, a eticii și nu numai*, Universul Juridic, București, 2023, 125.

³⁷ Nikolaos Aletras et al., *Predicting Judicial Decisions of the European Court of Human Rights: A Natural Language Processing Perspective*, 'PeerJ Computer Science' 2, 2016, 1–19, DOI: 10.7717/cs.93.

³⁸ The Right Hon. Sir Geoffrey Vos. *The Future for Dispute Resolution: Horizon Scanning*, 17 March 2022:8., the document is available online at <https://www.judiciary.uk/wp-content/uploads/2022/03/MR-to-SCL-Sir-Brain-Neill-Lecture-2022-The-Future-for-Dispute-Resolution-Horizon-Scannings-.pdf>, accessed on 11 February 2024.

Sanctions - COMPAS is used to assess risk by extracting historical data from offenders and analysing this data to produce an outcome based on the behaviour and background of the offender in question. In 2013 a convict who COMPAS indicated was at high risk of recidivism appealed to the Wisconsin Supreme Court on the grounds that the use of COMPAS in sentencing violated a defendant's right to a fair trial. In reasoning the Court held that a court's use of COMPAS was permissible as long as the judge made the final decision on sentencing and the judge was notified of the tool's limitations³⁹. ProPublica conducted an investigation⁴⁰ in 2016 that indicated that African-American defendants were more likely to receive a false positive COMPAS risk assessment score compared to white defendants.

Also, in the US, the Public Safety Assessment Algorithm (developed with \$1.2 million and based on a set of pre-trial records of 1.5 million cases from about 300 jurisdictions in the United States) emerged to help judges assess a defendant's risk before trial. It predicts the likelihood that an individual will reoffend if released before trial and the probability that the individual will not return for a future court hearing, and flags those defendants who are at high risk of committing a violent crime. The appellants argue, however, that the pre-trial phase should ensure, among other things, the constitutional rights of individuals, including the presumption of innocence⁴¹.

In Argentina, tax prosecutors use AI systems to draft court rulings.⁴²

In China, the online platform on mobile phones Mobile MiniCourt is considered a smart court, but it also has its limitations. Not all people know how to use such applications, documents are usually on paper, and converting to electronic format involves some additional costs.

In Brazil, the Supreme Court uses the VICTOR AI system, which analyses the high volume of appeals and automates the review process by identifying cases with *repercussão geral* (general impact), a requirement for processing an

³⁹ The Australasian Institute of Judicial Administration Incorporated, *AI Decision-Making and the Courts a guide for Judges, Tribunal Members and Court Administrators* Sydney, 2022, 29, the document is available online at: https://aija.org.au/wp-content/uploads/woocommerce_uploads/2022/06/AI-DECISION-MAKING-AND-THE-COURTS_Report_V5-2022-06-20-11zks.pdf, accessed on 17 February 2024.

⁴⁰ Julia Angwin, Jeff Larson, Surya Mattu, Lauren Kirchner, *Machine Bias There's software used across the country to predict future criminals. And it's biased against blacks*, 'ProPublica' May 23, 2016, the document is available online at <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>, accessed on 14 February 2024.

⁴¹ LJAF, *Public safety assessment: risk factors and formula*, the document is available online at <https://craftmediabucket.s3.amazonaws.com/uploads/PDFs/PSA-Risk-Factors-and-Formula.pdf>, accessed on 18 February 2024.

⁴² DeJusticia, *Conoce nuestra Investigación sobre PretorIA, la tecnología que incorpora la Inteligencia Artificial a la Corte Constitucional*, 2021, 5, <https://www.dejusticia.org/conoce-nuestrainvestigacion-sobre-pretoria-la-tecnologia-que-incorpora-la-inteligencia-artificial-a-la-corte-constitucional/>, accessed on 14 February 2024.

appeal before the Court⁴³.

In Colombia, the Constitutional Court is developing an AI system called PretorIA to assist in the selection of legal guardians, a system that does not replace humans but streamlines the process by analysing previous guardianship sentences⁴⁴. Also, in Colombia, in 2023 a judge said he used ChatGPT to determine whether an autistic child's insurance should cover all of his medical treatment expenses, sparking much controversy.⁴⁵

In India, an AI portal - Supreme Court Portal for Assistance in Court's Efficiency SUPACE⁴⁶ launched in 2020 assists judges in legal research by previewing files and providing a chatbot for case overviews.

Based on the algorithm created by researchers from 3 universities (Catholic University of Leuven, University of Sheffield, University of Pennsylvania), court decisions of the European Court of Human Rights were anticipated with an accuracy of 79%.⁴⁷

Automated CLAUse DETectEr - CLAUDETTE is an interdisciplinary research project hosted at the Department of Law of the European University Institute and a platform for automated legal document analysis and annotation as well as anomaly detection.⁴⁸

Mexico's EXPERTIUS system shows the court whether a claimant is eligible for a pension and can even calculate the amount of pension they are entitled to, based on specified socioeconomic criteria.⁴⁹

The Judicial Information Research System - JIRS - is an online database for judicial officers, courts, the legal profession and government agencies developed by the Judicial Commission of New South Wales, Australia, which combines sentencing statistics by reference to the relevant offences, but also includes details about the nature of the offense and the defendant⁵⁰.

⁴³ UNESCO, *Global toolkit on AI and the rule of law for the judiciary*, Paris, 2023, 78.

⁴⁴ DeJustitia, Victor Saavedra, Juan Carlos Upegui Pretor, *IA and automating the processing of human rights cases*, March 2021, the document is available online at https://www.derechosdigitales.org/wp-content/uploads/05_Informe-Colombia-EN_180222.pdf, accessed on 15 February 2024

⁴⁵ Luke Taylor, *Colombian judge says he used ChatGPT in the ruling*, 'The Guardian', 3 February 2023, the document is available online at <https://www.theguardian.com/technology/2023/feb/03/colombia-judge-chatgpt-ruling>, accessed on 15 February 2024.

⁴⁶ *AI Portal SUPACE*, 7 April 2021, the document is available online at <https://www.drishtiiias.com/daily-news-analysis/ai-portal-supace>, accessed on 14 February 2024.

⁴⁷ UNESCO, *Global toolkit on AI and the rule of law for the judiciary*, Paris, 2023, 57.

⁴⁸ By bringing together experts in machine learning, law and politics, the laborious tasks of reading and evaluating the terms of service and privacy policies of online platforms and applications can be automated, especially from the point of view of Directive 93/13 on unfair contract terms and of the GDPR. EUI, *Claudette*, <http://claudette.eui.eu/about/index.html>.

⁴⁹ Enrique Cáceres, *EXPERTIUS: A Mexican Judicial Decision-Support System in the Field of Family Law* in Enrico Francesconi, Giovanni Sartor, Daniela Tiscornia (eds), *Legal Knowledge and Information Systems*, IOS Press, 2008, 10.3233/978-1-58603-952-3-78. See also the Australasian Institute of Judicial Administration Incorporated, *AI Decision-Making and the Courts a guide for Judges, Tribunal Members and Court Administrators* Sydney, 2022, 32.

⁵⁰ *Judicial Information Research System (JIRS)*, the document is available online at <https://www.>

AI can also get involved in the legislative process. Thus, a bill written in a few minutes by ChatGPT was approved in Brazil for the first time in the world.⁵¹

Senator Barry Finegold and Representative Josh S. Cutler drafted a bill in 2023 to regulate artificial intelligence technology with the help of ChatGPT, which would require, among other things, companies to disclose information about AI algorithms to the attorney general, conduct periodic reviews of the risks and to establish means of detecting plagiarism⁵². However, even in this case some question marks are raised. Should developers of AI systems involved in the legislative process have access to this level and influence this process?

A problem with AI tools used in the justice system is the lack of control, information, transparency. Some judges may not fully understand the reasoning behind the AI systems they would be using.

A 2019 law in France prohibits the publication of statistical information, in this case the use of data analysis of judges' decisions (judicial behaviour patterns).⁵³

The question that arises more and more often in connection with the use of AI in the judicial process is the need to ensure an appeal, in the conditions where we believe that the decision given by the AI is correct, without the risk of an error of judgment. If a check is required, who will do this check? Still IA?⁵⁴ Can widespread use in the justice system erode the position and power of the judge?

A new concept, that of *AI Crime*, makes AI a threat. The authors of a study show us that AI can facilitate the commission of criminal acts (experiments were carried out targeting social network users and the manipulation of simulated markets through AI)⁵⁵.

Predictive policing (a practice involving the use of AI tools to profile

judcom.nsw.gov.au/judicial-information-research-system-jirs/, accessed on 14 February 2024.

⁵¹ 'Create a municipal law for the city of Porto Alegre, originating from the legislature and not the executive, which prohibits the Municipal Water and Sewage Department from charging the property owner for the payment of a new water meter when it is stolen.' Claudio Buttice, 'How AI Could Make Our Laws: First Bill Written by ChatGPT Gets Approved', 14 December 2023, the document is available online at <https://www.techopedia.com/how-ai-could-make-our-laws-as-the-first-law-written-by-chatgpt-gets-approved>, accessed on 14 February 2024.

⁵² *An Act drafted with the help of ChatGPT to regulate generative artificial intelligence models like ChatGPT*, the document is available online at <https://malegislature.gov/Bills/193/SD1827>, accessed on 14 February 2024.

⁵³ The identity data of judges and court clerks may not be reused for the purpose or effect of evaluating, analyzing, comparing or predicting their actual or alleged professional practices ('*Les données d'identité des magistrats et des membres du greffe ne peuvent faire l'objet d'une réutilisation ayant pour objet ou pour effet d'évaluer, d'analyser, de comparer ou de prédire leurs pratiques professionnelles réelles ou supposées*') – Art. 33 LOI n° 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice, JORF n° 0071 du 24 mars 2019.

⁵⁴ Ioana Ciutacu, *op. cit.*, p. 53.

⁵⁵ Thomas C. King, Nikita Aggarwal, Mariarosaria Taddeo, Luciano Floridi *Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions*, 'Science and Engineering Ethics' 26, 2020, 89–120, <https://doi.org/10.1007/s11948-018-00081-013>.

potential criminals) is increasingly being used to prevent crime. However, the use of these algorithms may be subject to human error. It has been proven that people of colour or other minorities such as LGBT people, children or the elderly can be negatively affected, harmed and discriminated against by AI predictions.

The *European Parliament Resolution on artificial intelligence in criminal law and its use by police and judicial authorities in criminal proceedings*⁵⁶ of 2021 sounded the alarm about the errors of identification systems based on AI algorithms in relation to racial or sexual minorities, but and in relation to minors.

These assessments in the context of crime prevention can give rise to those "echo chambers"⁵⁷ where racial or ethnic biases exist even more, because AI algorithms and automatic data processing do not allow law enforcement or the police to distinguish or identify them correctly.

The exercise of the right to vote can be affected by the use of AI systems, therefore, in order to guarantee a democratic society and the freedom of the citizen, these systems must be considered high risk. Robots, algorithms and automated fake accounts can be used to spread misinformation, manipulate public opinion and influence voter perceptions. The case of the 2016 US elections is well known, when false information was also spread with the help of automated techniques on social media platforms.

The labour market has always been affected by the development of technology, so the case of the emergence of "smart workers"⁵⁸ is no exception. In addition to the benefits, however, there are risks that could have a strong impact on the workforce. AI technologies can perform tasks more efficiently and accurately than humans, leading to the automation of certain jobs. The 2017 McKinsey Global Institute report, "Jobs lost, jobs gained: Workforce transitions in a time of automation", assesses the number and types of jobs that could be created under different scenarios by 2030 and compares them to the jobs that could be lost to automation. It is estimated that between 400 and 800 million people could be replaced by automation and should find new jobs by 2030 worldwide, and between 75 million and 375 million may have to change categories professional

⁵⁶ *European Parliament Resolution of 6 October 2021 on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters (2020/2016 – INI)*, the document is available online at https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_EN.html, accessed on 14 February 2024.

⁵⁷ An epistemic environment in which participants encounter beliefs and opinions that coincide with their own and amplify or reinforce their pre-existing beliefs through communication and repetition within a closed and isolated system, in Carlos D. Ruiz, Tomas Nilsson, *Disinformation and Echo Chambers: How Disinformation Circulates in Social Media Through Identity-Driven Controversies*, *Journal of Public Policy & Marketing* 4 (1), 2023, 18–35. doi:10.1177/07439156221103852. S2CID 248,934,562.

⁵⁸ Leonardo da Vinci, in the late fifteenth century, did technical drawings which have allowed the creation of a robotic knight capable of independent motion. In Nadia M. Thalmann, *Social Robots: Their History and What They Can Do for Us*, in: H. Werthner, E. Prem, E.A., Lee, C. Ghezzi (eds), *Perspectives on Digital Humanism*, Springer, 2022, 9–17, 11, https://doi.org/10.1007/978-3-030-86144-5_2.

and learn new skills.⁵⁹ OECD⁶⁰ research, for example, estimated in 2018 that, on average, around 14% of jobs in OECD countries are highly automated and another 32% of jobs could face substantial change.

The fact that AI can learn quickly makes it a formidable opponent for job seekers, especially in intellectual professions. Even though those physically demanding jobs will not be affected yet, it does not mean that AI will not be able to perform those tasks at a much lower cost than now.⁶¹ Already repetitive and high-volume tasks in factories can be replaced by robots, and over time, AI will be able to perform tasks of a much greater variety⁶². Low-skilled jobs, those that involve caring for and assisting others, cleaning services, construction, manufacturing or transportation will be affected.

OTP Bank has implemented the DRUID AI platform - the Octavian app⁶³ - which offers customers 24/7 access to banking products. A conversational AI assistant registers customer, collects their feedback, guides them through the process of applying for credit deferment online.

In the UK, the Small Robot Company has developed three robots Tom, Dick and Harry to destroy weeds in wheat fields while drastically reducing the use of chemical pesticides.⁶⁴

The intelligent robot Nadine (equipped with a 3D camera and microphone) was tested as a customer service agent and helper for people at a nursing home in Singapore.⁶⁵

White Castle, an American fast food chain will implement the Flippy 2 robot in more than 100 restaurants.⁶⁶ The robot takes over the activity of an entire

⁵⁹ McKinsey Global Institute, *Jobs lost, jobs gained: Workforce transitions in a time of automation*, 2017, 11, the document is available online at <https://www.mckinsey.com/~media>, accessed on 15 February 2024.

⁶⁰ OECD, *Putting faces to the jobs at risk of automation, Policy Brief on the Future of Work*, March 2018, the document is available online at <https://www.oecd.org/employment/Automation-policy-brief-2018.pdf>, accessed on 15 February 2024.

⁶¹ Arthur Mihăilă, *Exploring ethical concerns surrounding Artificial Intelligence* in Ionel Boldea, Cornel Sigmirean, Dumitru M. Buda, *New Perspectives on Multiculturalism: Literature and Dialogue*, Arhipelag XXI Press, Târgu Mureş, 2023, 94.

⁶² Jonathan Tilley, *Automation, robotics, and the factory of the future*, September 7, 2017, the document is available online at <https://www.mckinsey.com/capabilities/operations/our-insights/automation-robotics-and-the-factory-of-the-future>, accessed on 15 February 2024.

⁶³ *OTP Bank improves customer support with the use of DRUID AI virtual assistant*, 30 March 2023, the document is available online at <https://www.druidai.com/case-studies/conversational-ai-chatbot-banking-otp-bank>.

⁶⁴ Stephanie Bailey, *A robot is killing weeds by zapping them with electricity*, 'CNN', October 19, 2022, the document is available online at <https://edition.cnn.com/2021/06/09/tech/robot-zaps-weeds-spc-intl/index.html>, accessed on 15 February 2024.

⁶⁵ Nadine was able to answer customer questions and maintain a polite and professional demeanour during the interaction. In Nadia M. Thalman, *op. cit.*, p. 15.

⁶⁶ Aneurin Canham-Clyne, *White Castle brings cooking robot to 100 more restaurants*, February 15, 2022, the document is available online at <https://www.restaurantdive.com/news/white-castle-brings-cooking-robot-to-100-more-restaurants/618852/>, accessed on 15 February 2024.

roasting station. It has been stated that the robot will not be a job replacement, but instead may create new jobs, including "chef technicians" who are trained to handle the robot.

Fedha, an AI-powered news anchor debuted on the Twitter account of Kuwait News, a branch of the Kuwait Times.⁶⁷

In Romania, a farmer from Bistrița has 5 robots that milk and feed his animals and clean the stables.⁶⁸

Sophia is a social humanoid robot developed by Hanson Robotics, Hong Kong. A digital artwork by Sophia (in collaboration with Italian digital artist Andrea Bonaceto) was auctioned for \$688,888 as an NFT.⁶⁹ Yet, when Sofia the robot was asked in an interview in 2016 if she would destroy humanity, her answer was: "Okay, I will destroy humans."

Bob and Alice, a pair of robots developed by Facebook, were stopped in 2017 because they started conversing in their own language. Was it a programmer error, or is it a reason to be cautious and look more into the fact that one day humans will have to learn the language of robots and not the other way around?

It has often been claimed that AI does not have soft skills that are human traits such as empathy, compassion, emotion or creativity, however, the latest innovations in the field would begin to contradict these claims.

A disadvantage is related to the financial strength of the firms implementing/acquiring AI systems. Companies with a lot of money will have significant competitive advantages over small firms that will not be able to make investments in AI software, robots, automation.⁷⁰

One of the major problems in the labour market is related to artificial intelligence systems intended to be used for the recruitment or selection of natural persons, in particular for the placement of specific job advertisements, the selection or filtering of candidates, the evaluation of candidates in interviews or tests. Thus, prejudice and discrimination will also be present in the labour market. In New York, a law came into force in 2023 - "Bias Audit Law" - with the aim of fighting against discrimination that may occur due to the use of AI in making employment decisions. The legal text prohibits employers from using automated

⁶⁷ Antoinette Radford, *Kuwait news outlet unveils AI-generated presenter Fedha*, 'BBC News', 11 April 2023, the document is available online at <https://www.bbc.com/news/world-middle-east-65238950>, accessed on 18 February 2024.

⁶⁸ Alina Stanciu, *Un crescător de vite din Bistrița lucrează cu roboți pentru a-și întreține ferma de 280 de vaci. Aceștia mulg, fac curat și hrănesc animalele*, 14 Feb. 2020, the document is available online at https://www.economica.net/ferma-de-vaci-cu-roboti-peica_179894.html, accessed on 15 February 2024.

⁶⁹ Oscar Holland, *Sophia, the Robot 'self-portrait' NFT sells for almost \$700K*, 'CNN', 25 March 2021, the document is available online at <https://edition.cnn.com/style/article/nft-art-sophia-robot-self-portrait-scn/index.html>, accessed on 15 February 2024.

⁷⁰ European Parliament, James Eager, Mark Whittle, Jan Smit, Giorgio Cacciaguerra, Eugénie Lale-Demoz, *Opportunities of Artificial Intelligence*, 2020, 46.

employment decision tools (AEDT⁷¹) to evaluate applicants unless the employer meets several requirements before using them, including conducting an independent audit of the AEDT and providing a notice of its use.

The same discussion goes on in the case of the selections of candidates for admission to the university. Some universities use such AI systems. For example, in admissions at Brown University in the United States, each student's application was evaluated in just 12 minutes, although in addition to standardized documents it was necessary to analyse several essays.⁷² Can a candidate be evaluated in such a short time? Isn't a template being created, ignoring the individuality of each of us? It is equally true that even in the case of a person evaluating a candidate's file there may be a risk of expressing prejudices.

3. The digital age and AI - the age of social inequalities

People in poor and developing countries do not have access to the internet or stable internet, and access to AI technologies such as advanced machine learning algorithms is often limited to individuals, corporations and rich countries that have the resources needed to invest in AI research and development. Thus, the digital divide will further accentuate social inequalities.

There are states where the implementation of AI is quite difficult to achieve. Yet, countries such as China, the USA, Canada⁷³, Japan⁷⁴, France, Germany or Great Britain⁷⁵ are investing a lot in research and implementation of AI technologies. Europe has 25% of the world's AI start-ups driving AI innovation.⁷⁶

⁷¹AEDT is defined as 'any computational process derived from machine learning, statistical modelling, data analytics, or artificial intelligence, which issues simplified output, including a score, classification, or recommendation that is used to substantially assist or replace discretionary decision-making'. In Christopher J. Stevens, Jenny L. Holmes, *Complying with New York City's Bias Audit Law*, the document is available online at <https://www.nixonpeabody.com/insights/alerts/2023/11/13/complying-with-new-york-city-bias-audit-law>, accessed on 15 February 2024.

⁷²Tetyana (Tanya) Krupiy, *A vulnerability analysis: Theorising the impact of artificial intelligence decision-making processes on individuals, society and human diversity from a social justice perspective*, 'Computer Law & Security Review' 38, 2020, 1–25, 2, <https://doi.org/10.1016/j.clsr.2020.105429>.

⁷³Canada was the first country to launch a national strategy on artificial intelligence. Detailed in the 2017 federal budget, the Pan-Canadian Artificial Intelligence Strategy is a C\$125 million five-year plan to invest in AI research and talent, in Tim Dutton, *An Overview of National AI Strategies*, June 28, 2018, the document is available online at <https://medium.com/politics-ai/an-overview-of-national-ai-strategies-2a70ec6edfd>, accessed on 18 February 2024.

⁷⁴Japan was the second country to develop a national AI strategy. The AI Technology Strategic Council was established, tasked with developing 'research and development goals and a roadmap for the industrialization of artificial intelligence', in Tim Dutton, *An Overview of National AI Strategies*.

⁷⁵In April 2018, the UK government published the AI Sectoral Agreement, the document is available online at <https://www.gov.uk/government/publications/artificial-intelligence-sector-deal>, accessed on 18 February 2024.

⁷⁶Bongs Lainjo, *The global social dynamics and inequalities of artificial intelligence*, 'International

Increased surveillance of people through AI techniques and discrimination against poor and black people may discourage them from seeking social services or healthcare for fear of leaving too many digital traces, so their data will be processed and misinterpreted by some algorithms⁷⁷.

In medical practice AI systems can even create errors in diagnosis and treatment or establish poor treatment for certain minorities.⁷⁸

Jobs held by low-skilled people could be replaced by AI, thus creating the risk that those already low-paid people will not find other jobs and exacerbating social class differences.

Inequalities can also be observed at the educational level.⁷⁹ The educational system will have to be adapted to the labour market, therefore it will also have to undergo changes that require financial as well as human investments.

Some authors⁸⁰ even believe that the intervention of AI systems in certain decision-making processes reduces the human individual to a statistical value, without taking into account lived experiences or other feelings.

In computer science terms are used such as *overfitting* (the model has been overfit or when it contains too much complexity, leading to high error rates on the test data) and *underfitting* (a data model is not able to accurately capture the relationship between input and output variables, generating a high error rate on both the training set and the contingency data). From a sociological perspective, according to some authors, the AI system can thus include too little data to reflect the social world or, on the contrary, too much, thus producing fluctuations, with reference to the biases that appear in data processing.⁸¹

Yet there are companies trying to create unbiased AI systems that treat all people equally when decision-making impacts people's lives. Facebook uses Fairness Flow⁸², Google created the ML Fairness Effort⁸³, IBM created open source tools to help examine and report discrimination in AI applications.⁸⁴

If society is unequal and sometimes unfair, AI algorithms should work to

Journal of Innovation Scientific Research and Review' Vol. 05, Issue, 8 Aug. 2023, 4966–4974, <http://www.journalijisr.com>.

⁷⁷ Kelly Joyce, Laurel Smith-Doerr, Sharla Alegria, Susan Bell, Taylor Cruz, Steve G. Hoffman, Safiya Umoja Noble, and Benjamin Shestakofsky, *Toward the Sociology of Artificial Intelligence: A Call for Research on Inequalities and Structural Change*, 'Socius' 7, 2021, <https://doi.org/10.1177/2378023121999581>.

⁷⁸ Bongs Lainjo, *op. cit.*, p. 4969.

⁷⁹ Idem, 4971.

⁸⁰ Reuben Binns at all, *It's Reducing a Human Being to a Percentage; Perceptions of Justice in Algorithmic Decision*, 'Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems', Montreal, April 2018, <https://dl.acm.org/doi/10.1145/3173574.3173951>.

⁸¹ Kelly Joyce et. all, *Toward a Sociology of Artificial Intelligence: A Call for Research on Inequalities and Structural Change*, 'Socius', 2021.

⁸² <https://ai.meta.com/blog/how-were-using-fairness-flow-to-help-build-ai-that-works-better-for-everyone/>, consulted on 1 March 2024.

⁸³ <https://ai.google/responsibility/responsible-ai-practices/>, consulted on 1 March 2024.

⁸⁴ <https://aif360.res.ibm.com/>, consulted on 1 March 2024.

change this, not reproduce it.⁸⁵ AI does not sleep, does not get tired, does not get sick, does not have emotions, learns quickly to solve problems, can adapt. All this is a real cause for concern in the labour market.

4. Liability of providers and users of AI systems

As far back as 2018, Council of Europe⁸⁶ research has shown us that the use of AI algorithms in decision-making processes has an impact on human rights. And in these situations, it is important to identify the responsible person who can be held accountable. Yet it remains to be seen who that person is? That is why, especially in the justice system, a decision that involves holding a person legally responsible must belong to the human factor, and the person held responsible must have the possibility of having access to an appeal.

AI systems classified as high risk will be subject to transparency and security requirements (information about the general characteristics, capabilities and limitations of the system, algorithms, data, training, testing and validation processes, documentation on the relevant risk management system), with the aim of reducing risks to health, safety and fundamental rights. Therefore, providers and their users will be obliged to adopt state-of-the-art technical and organizational measures to protect these rights (anonymization, encryption, use of a technology that allows bringing algorithms to data and obtaining valuable information without transmission between parties or unnecessary copying of raw or structured data itself).⁸⁷ The users of AI systems will also have a number of responsibilities.

Fundamental rights impact assessment must be done before these AI systems are put into operation. In addition, measures must be established to mitigate the risks of AI systems. The new *AI law* establishes the possibility for people affected by the operation of AI systems in fundamental rights, to have the possibility to report, to be compensated, to have access to appeals if they are dissatisfied with the way their complaints are resolved.

We believe that public authorities should also take responsibility for decisions made with the help of AI algorithms. Liability will probably need to be considered for each area separately.

The requirement to ensure the right to compensation and criminal liability of those who violate human rights as a result of discrimination caused by the use of AI systems is set out in the 2018 Toronto Declaration: Protecting the Right

⁸⁵ Mike Zajko, *Artificial intelligence, algorithms, and social inequality: Sociological contributions to contemporary debates*, 'Sociology Compass', Volume 16, Issue 3 Mar 2022, 1–16, DOI: 10.1111/soc4.12962.

⁸⁶ Council of Europe, *Algorithms and Human Rights, Study on the human rights dimensions of automated data processing techniques and possible regulatory implications*, March 2018, the document is available online at https://rm.coe.int/algorithms-and-human-rights-en-rev/16807956_b5, accessed on 11 February 2024.

⁸⁷ Amendment 80, *IA Law*, Recital 45.

to Equality and Non-Discrimination in Machine Learning Systems.⁸⁸ This document was created out of a desire to make human rights an essential element, being a tool to develop recommendations for avoiding the violation of fundamental human rights when using AI systems.

There are already many proposals to give robots rights (on the grounds that they would have consciousness, autonomy and intelligence) similar to humans and animals, but at the same time a new concept of robot responsibilities is beginning to develop, just as humans have rights, respectively correlative obligations. The 2017 *EP report on robotics*⁸⁹ suggested “creating a specific legal status for robots in the long run, so that at least the most sophisticated autonomous robots could be established as having the status of electronic persons responsible for making good any damage they may cause, and possibly applying electronic personality to cases where robots make autonomous decisions or otherwise interact with third parties independently”.

In practice, this responsibility can also be analysed when we talk about automatic machines or their programming, for example, in the event of an accident. Whom should control this kind of programming so that there are no distinctions based on gender or age? The government or the manufacturing company? To this end, MIT created the Moral Machine⁹⁰ website, which asks people to express their opinions on autonomous vehicles. The study shows that people prefer the life of a child to that of an adult. The majority of respondents indicated that they do not agree with governments ensuring how self-driving cars are programmed and would prefer to have cars whose programming is not centrally regulated and thus can behave in situations critical in any way predetermined by the manufacturer.⁹¹

5. Brief final considerations

The complexity of AI systems forces us to be aware and understand the impact that the use of these algorithms has on human rights. Errors, risks or just prejudices, it remains to be seen to what extent the new regulations will be able to fix these problems. One thing is certain: the level of autonomy of AI must remain in the control of humans.

The field is of an unprecedented complexity, therefore the fact that there will be a clear and extensive regulation of AI, does not mean that the implementation will be easy, and the involvement of public authorities, private companies,

⁸⁸ *The Toronto Declaration: Protecting the right to equality and non-discrimination in machine learning systems*, the document is available online at https://www.accessnow.org/wp-content/uploads/2018/08/The-Toronto-Declaration_ENG_08-2018.pdf, accessed on 16 February 2024.

⁸⁹ European Parliament, *REPORT with recommendations to the Commission on Civil Law Rules on Robotics* 27.1.2017 – (2015/2103 – INL).

⁹⁰ <https://www.moralmachine.net/>, consulted on 1 March 2024.

⁹¹ Tomas Hauer, *Importance and limitations of AI ethics in contemporary society*, ‘Humanit Soc Sci Commun’ 9, 272, 2022, 6. <https://doi.org/10.1057/s41599-022-01300-7>.

the academic world, individuals must be transformed into a close collaboration.

We believe that the attention of those determining how AI systems make decisions must be directed to the vulnerability of humans and to the goal of creating equity in access to such resources.

By pointing out some potential and actual risks of using AI in areas that affect fundamental rights and freedoms, we wanted to draw attention to the potential for manipulation and discrimination of the *challenge of our times*⁹² that is AI, without researching and reproducing the undeniable advantages of AI.

Bibliography

I. Books and journals

1. Aletras, Nikolaos et al, *Predicting Judicial Decisions of the European Court of Human Rights: A Natural Language Processing Perspective*, 'PeerJ Computer Science' 2, 2016, DOI: 10.7717/cs.93.
2. Anderco, Raluca, *Inteligența artificială - ce probleme atrage lipsa cadrului legislativ*, 'Revista Universul Juridic' 10 October 2023.
3. Benthall, Sebastian & Bruce D. Haynes, *Racial Categories in Machine Learning*, 'FAT* '19: Proceedings of the Conference on Fairness, Accountability, and Transparency', Associations for Computing Machinery 9 (2019), <https://doi.org/10.1145/3287560.3287575>.
4. Binns, Reuben et al, *It's Reducing a Human Being to a Percentage: Perceptions of Justice in Algorithmic Decision*, 'Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems', Montreal, April 2018, <https://dl.acm.org/doi/10.1145/3173574.3173951>.
5. Cáceres, Enrique, *EXPERTIUS: A Mexican Judicial Decision-Support System in the Field of Family Law* in Francesconi, Enrico, Giovanni Sartor & Daniela Tiscornia (eds), *Legal Knowledge and Information Systems*, IOS Press, 2008, 10.3233/978-1-58603-952-3-78.
6. Ciutacu, Ioana, *Efectele implementării inteligenței artificiale în justiție asupra drepturilor fundamentale și asupra drepturilor procedurale*, "Avocatul", June 2022.
7. Cristian Miheș, *Considerații asupra necesității adaptării unor instituții tradiționale ale dreptului penal în condițiile societății dominate de tehnologia informației*, in vol. *Previzibilitatea legislației și jurisprudenței în materie penală* (coord. Flaviu Ciopec, Laura-Maria Stănilă, Ioana-Celina Pașca), Universul Juridic, București, 2019.

⁹² The Director General of UNESCO, Audrey Azoulay stated that 'this is the challenge of our time', and the self-regulation of this industry is not enough to avoid the ethical damage caused by the continuous development of AI systems, and the implementation of the recommendation on the ethics of artificial intelligence is imperative. In March 2023 UNESCO called on governments to implement much stricter ethical rules in the field of AI. In UNESCO, *Artificial Intelligence: UNESCO calls on all Governments to implement Global Ethical Framework without delay*, the document is available online at <https://www.unesco.org/en/articles/artificial-intelligence-unesco-calls-all-governments-implement-global-ethical-framework-without>, accessed on 18 February 2024.

8. Duminičă, Ramona & Diana M. Ilie, *Freedom of thought, conscience and religion, 'resized' by the perspective of regulation of a 'right of the soul' – transdisciplinary analysis*, "Journal of Law and Administrative Sciences" 20, 2023.
9. Haggerty, Kevin D. & Richard V. Ericson, *The Surveillant Assemblage* 'British Journal of Sociology' 51(4), 2000, DOI: 10.1080/00071310020015280.
10. Hauer, Tomas, *Importance and limitations of AI ethics in contemporary society*, "Humanit Soc Sci Commun" 9, 2022, <https://doi.org/10.1057/s41599-022-01300-7>.
11. Joyce, Kelly, Laurel Smith-Doerr, Sharla Alegria, Susan Bell, Taylor Cruz, Steve G. Hoffman, Safiya Umoja Noble & Benjamin Shestakofsky, *Toward a Sociology of Artificial Intelligence: A Call for Research on Inequalities and Structural Change*, 'Socius' 7, 2021, <https://doi.org/10.1177/2378023121999581>.
12. King, Thomas C., Nikita Aggarwal, Mariarosaria Taddeo & Luciano Floridi *Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions*, 'Science and Engineering Ethics' 26, 2020, <https://doi.org/10.1007/s11948-018-00081-01> 3.
13. Krupiy, Tetyana (Tanya), *A vulnerability analysis: Theorising the impact of artificial intelligence decision-making processes on individuals, society and human diversity from a social justice perspective*, "Computer Law & Security Review" 38, 2020, <https://doi.org/10.1016/j.clsr.2020.105429>.
14. Lainjo, Bongs, *The global social dynamics and inequalities of artificial intelligence*, 'International Journal of Innovation Scientific Research and Review' Vol. 05, Issue, 08, Aug. 2023, <http://www.journalijisr.com>.
15. Martsenko, Nataliia, *Artificial Intelligence and human rights: a scientific review of impacts and interactions*, «Studia Prawnoustrojowe» 58, 2022, DOI : 10,31648/sp.8245.
16. Mihăilă, Arthur, *Exploring ethical concerns surrounding Artificial Intelligence in Boldea, Ionel, Cornel Sigmirean & Dumitru M. Buda, New Perspectives on Multiculturalism: Literature and Dialogue*, Arhipelag XXI Press, Târgu Mureș, 2023.
17. Mike Zajko, *Artificial intelligence, algorithms, and social inequality: Sociological contributions to contemporary debates*, "Sociology Compass", Volume 16, Issue 3, Mar 2022, DOI: 10.1111/soc4.12962.
18. Predescu, Ovidiu & Ovidiu R. Predescu, *Inteligența artificială azi. O perspectivă a dreptului, a drepturilor omului, a eticii și nu numai*, Universul Juridic, București, 2023.
19. Rosenblat, Alex, Karen Levy, Solon Barocas & Tim Hwang, 'Discriminating Tastes: Uber's Customer Ratings as Vehicles for Workplace Discrimination', *SSRN Electronic Journal*, January 2017, DOI:10.2139/ssrn.2858946 in *UK Intelligence and Security Committee of Parliament Report, Privacy and Security: A modern and transparent legal framework*, March 2015.
20. Ruiz, Carlos D. & Tomas Nilsson, *Disinformation and Echo Chambers: How Disinformation Circulates in Social Media Through Identity-Driven Controversies*, "Journal of Public Policy & Marketing" 4 (1), 2023, doi:10.1177/07439156221103852. S2CID 248,934,562.
21. Sartor, Giovanni & Daniela Tiscornia (eds), *Legal Knowledge and Information Systems*, IOS Press, 2008, 10.3233/978-1-58603-952-3-78.

22. Tegmark, Max, *Life 3.0: being human in the age of artificial intelligence*, Alfred A. Knopf, New York, 2017.
23. Thalmann, Nadia M., *Social Robots: Their History and What They Can Do for Us*, in: Werthner, H., E. Prem, E.A., Lee & C. Ghezzi, (eds), *Perspectives on Digital Humanism*, Springer, 2022, 9–17, 11, https://doi.org/10.1007/978-3-030-86144-5_2.

II. Legislation and official documents

1. Amendments adopted by the European Parliament on 14 June 2023 on the Proposal for a Regulation of the European Parliament and of the Council on laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM–2021–0206–C9-0146/2021–2021/0106–COD), 14 June 2023, the document is available online at https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.html, accessed on 11 February 2024.
2. Article 29 Data Protection Working Party, *Opinion 3/2012 on developments in biometric technologies*, 00720/12/EN, WP193, Brussels, 27 April 2012, <https://www.pdpjournals.com/docs/87998.pdf>.
3. CEPEJ, *European Ethical Charter on the use of Artificial Intelligence in judicial systems and their environment*, the document is available online at <https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c>, accessed on 11 February 2024.
4. Council of Europe study, Committee of experts on internet intermediaries (MSI-NET), *Algorithms and Human Rights. Study on the human rights dimensions of automated data processing techniques and possible regulatory implications*, 2018.
5. Council of Europe, Directorate General of Human Rights and Rule of Law Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data Convention 108, *Guidelines on Facial Recognition*, T-PD (2020)03rev4 28 January 2021, the document is available online at <https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3>, accessed on 14 February 2024.
6. Council of Europe, *Algorithms and Human Rights, Study on the human rights dimensions of automated data processing techniques and possible regulatory implications*, March 2018, the document is available online at <https://rm.coe.int/algorithms-and-human-rights-en-rev/16807956b5>, accessed on 11 February 2024.
7. Council of Europe, *Algorithms and Human Rights. Study on the human rights dimensions of automated data processing techniques and possible regulatory implications*, March 2018, the document is available online at <https://rm.coe.int/algorithms-and-human-rights-en-rev/16807956b5>, accessed on 11 February 2024.
8. ECHR, *Guide to the Case-Law of the of the European Court of Human Rights, Data protection*, the document is available online at https://www.echr.coe.int/documents/d/echr/Guide_Data_protection_ENG, accessed on 14 February 2024.

9. European Commission, *White Paper On Artificial Intelligence – A European approach to excellence and trust*, Brussels, 19.2.2020, COM(2020) 65 final.
10. European Parliament, *Resolution of 25 March 2021 on a European strategy for data*(2020/2217 – INI) (2021/C 494/04).
11. European Parliament, Committee on Civil Liberties, Justice and Home Affairs, *Report on Artificial Intelligence in Criminal Law and its use by the Police and Judicial Authorities in Criminal Matters*, 13.7.2021 – (2020/2016 – INI).
12. European Parliament *Resolution of 6 October 2021 on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters* (2020/2016 – INI)6 October 2021 – Strasbourg.
13. *Faridian v. DoNotPay Inc* (3:23-cv-01692), the document is available online at <https://www.courtlistener.com/docket/67158596/faridian-v-donotpay-inc/>, accessed on 15 February 2024.
14. European Parliament, James Eager, Mark Whittle, Jan Smit, Giorgio Cacciaguerra, Eugénie Lale-Demoz, *Opportunities of Artificial Intelligence*, 2020.
15. European Parliament, *REPORT with recommendations to the Commission on Civil Law Rules on Robotics* 27.1.2017 – (2015/2103 – INL).
16. OECD, *Putting faces to the jobs at risk of automation, Policy Brief on the Future of Work*, March 2018, the document is available online at <https://www.oecd.org/employment/Automation-policy-brief-2018.pdf>, accessed on 15 February 2024.
17. *Proposal for Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts*, COM(2021)/0106 (COD)/206; Brussels, 21.4.2021.
18. *The Toronto Declaration: Protecting the right to equality and non-discrimination in machine learning systems*, the document is available online at https://www.accessnow.org/wp-content/uploads/2018/08/The-Toronto-Declaration_ENG_08-2018.pdf, accessed on 16 February 2024.
19. The Australasian Institute of Judicial Administration Incorporated, *AI Decision-Making and the Courts a guide for Judges, Tribunal Members and Court Administrators*, Sydney, 2022, the document is available online at https://aija.org.au/wp-content/uploads/woocommerce_uploads/2022/06/AI-DECISION-MAKING-AND-THE-COURTS_Report_V5-2022-06-20-11zkl.pdf, accessed on 17 February 2024.
20. The General Court of the Commonwealth of Massachusetts, *An Act Drafted with the Help of ChatGPT to Regulate Generative Artificial Intelligence Models Like Chat GPT*, the document is available online at <https://malegislature.gov/Bills/193/SD1827>, accessed on 14 February 2024.
21. The Right Hon, Sir Geoffrey Vos, *The Future for Dispute Resolution: Horizon Scanning*, 17 March 2022, the document is available online at <https://www.judiciary.uk/wp-content/uploads/2022/03/MR-to-SCL-Sir-Brain-Neill-Lecture-2022-The-Future-for-Dispute-Resolution-Horizon-Scannings-.pdf>, accessed on 11 February 2024.
22. UN, Committee on the Elimination of Racial Discrimination, *General Recommendation No. 36 (2020) on Preventing and Combating Racial Profiling by Law Enforcement Officials*.
23. UNESCO, *Recommendation on the Ethics of Artificial Intelligence*, 2021 the document is available online at <https://www.cnr-unesco.ro/uploads/media/f10>

- 77_recomandari-unesco-ai-site.pdf, accessed on 11 February 2024.
24. UNESCO, *Global Toolkit on AI and the rule of law for the judiciary*, Paris, 2023.
 25. UNESCO, *Artificial Intelligence: UNESCO Calls on All Governments to Implement Global Ethical Framework Without Delay*, the document is available online at <https://www.unesco.org/en/articles/artificial-intelligence-unesco-calls-all-governments-implement-global-ethical-framework-without>, accessed on 18 February 2024.
 26. WIPO, *Frontier Technologies Factsheet*, the document is available online at https://www.wipo.int/export/sites/www/about-ip/en/frontier_technologies/pdf/frontier-tech-6th-factsheet.pdf, accessed on 11 February 2024.

III. Online resources

1. *AI Portal SUPACE*, 7 April 2021, the document is available online at <https://www.drishtiiias.com/daily-news-analysis/ai-portal-supace>, accessed on 14 February 2024.
2. Angwin, Julia, Jeff Larson, Surya Mattu & Lauren Kirchner, *Machine Bias There's software used across the country to predict future criminals. And it's biased against blacks*, 'ProPublica' May 23, 2016, the document is available online at <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>, accessed on 14 February 2024.
3. Bailey, Stephanie, *A robot is killing weeds by zapping them with electricity*, 'CNN', October 19, 2022, the document is available online at <https://edition.cnn.com/2021/06/09/tech/robot-zaps-weeds-spc-intl/index.html>, accessed on 15 February 2024.
4. Canham-Clyne, Aneurin, *White Castle brings cooking robot to 100 more restaurants*, February 15, 2022, the document is available online at <https://www.restaurantdive.com/news/white-castle-brings-cooking-robot-to-100-more-restaurants/618852/>, accessed on 15 February 2024.
5. Dejusticia, *Conoce nuestra Investigación sobre PretorJA, la tecnología que incorpora la Inteligencia Artificial a la Corte Constitucional*, 2021, <https://www.dejusticia.org/conoce-nuestra-investigacion-sobre-pretoria-la-tecnologia-que-incorpora-la-inteligencia-artificial-a-la-corte-constitucional/>, accessed on 14 February 2024.
6. DeJustitia, Saavedra, Victor & Juan Carlos Upegui Pretor, *IA and automating the processing of human rights cases*, March 2021, the document is available online at https://www.derechosdigitales.org/wp-content/uploads/05_Informe-Colombia-EN_180222.pdf, accessed on 15 February 2024.
7. Dutton, Tim, *An Overview of National AI Strategies*, June 28, 2018, the document is available online at <https://medium.com/politics-ai/an-overview-of-national-ai-strategies-2a70ec6edfd>, accessed on 18 February 2024.
8. Feldstein, Steven, *The Global Expansion of AI Surveillance*, 'Carnegie Endowment for International Peace', Sept. 2019, the document is available online at https://carnegieendowment.org/files/WP-Feldstein-AISurveillance_fi_nal1.pdf, accessed on 11 February 2024.
9. Holland, Oscar, *Sophia the Robot 'self-portrait' NFT sells for almost \$700K*, 'CNN', 25 March 2021, the document is available online at <https://edition.cnn.com/style/article/nft-art-sophia-robot-self-portrait-scn/index.html>, accessed on

- 15 February 2024.
10. *Judicial Information Research System (JIRS)*, the document is available online at <https://www.judcom.nsw.gov.au/judicial-information-research-system-jirs/>, accessed on 14 February 2024.
 11. LJAF, *Public safety assessment: risk factors and formula*, the document is available online at <https://craftmediabucket.s3.amazonaws.com/uploads/PDFs/PSA-Risk-Factors-and-Formula.pdf>, accessed on 18 February 2024.
 12. McKinsey Global Institute, *Jobs lost, jobs gained: Workforce transitions in a time of automation*, 2017, the document is available online at <https://www.mckinsey.com/~media>, accessed on 15 February 2024.
 13. Mozur, Paul, *In Hong Kong Protests, Faces Become Weapons*, 'New York Times', July 26, 2019, the document is available online at <https://www.nytimes.com/2019/07/26/technology/hong-kong-protests-facial-recognition-surveillance.html>, accessed on 13 February 2024.
 14. Radford, Antoinette, *Kuwait news outlet unveils AI-generated presenter Fedha*, 'BBC News', 11 April 2023 the document is available online at <https://www.bbc.com/news/world-middle-east-65238950>, accessed on 18 February 2024.
 15. Stanciu, Alina, *Un crescător de vite din Bistrița lucrează cu roboți pentru a-și întreține ferma de 280 de vaci. Aceștia mulg, fac curat și hrănesc animalele*, 14 feb. 2020, the document is available online at https://www.economica.net/ferma-de-vaci-cu-roboti-peica_179894.html, accessed on 15 February 2024.
 16. Stevens, Christopher J. & Jenny L. Holmes, *Complying with New York City's Bias Audit Law*, the document is available online at <https://www.nixonpeabody.com/insights/alerts/2023/11/13/complying-with-new-york-city-bias-audit-law>, accessed on 15 February 2024.
 17. Taylor, Luke, *Colombian judge says he used ChatGPT in ruling*, 'The Guardian', 3 February 2023, the document is available online at <https://www.theguardian.com/technology/2023/feb/03/colombia-judge-chatgpt-ruling>, accessed on 15 February 2024.
 18. Tilley, Jonathan, *Automation, robotics, and the factory of the future*, September 7, 2017, the document is available online at <https://www.mckinsey.com/capabilities/operations/our-insights/automation-robotics-and-the-factory-of-the-future>, accessed on 15 February 2024.

Electronization of the Healthcare Sector and Its Responsibility in Relation to IT and AI

JUDr. Tereza JONÁKOVÁ¹

Abstract

The modern phenomenon of electronization and digitalization of the contemporary information society affects many areas of human life, and produces, mainly due to the unclear construction of legal liability in relation to AI and its activities, many relevant questions. If AI and the activities and services linked to it is to be responsible to society, they should, above all, be fair, accountable, transparent, confidential and secure to their users, not only with legal implications, but also with moral and ethical ones, all with the aim of mitigating technical and technological risks while maintaining the guarantee of fundamental human rights and freedoms.

Keywords: artificial intelligence, information technologies, accountability, healthcare, telemedicine.

JEL Classification: K24, K32

DOI: <https://doi.org/10.62768/ADJURIS/2024/1/04>

Please cite this article as:

Jonáková, Tereza, „Electronization of the Healthcare Sector and Its Responsibility in Relation to IT and AI”, in Pajuste, Tiina, Heliona Bellani (Miço) & Sejla Maslo Cerkić (eds.), *Legal Perspectives in the Modern Era of Technological Transformations*, ADJURIS – International Academic Publisher, Bucharest, Paris, Calgary, 2024, p. 64-74

1. Introduction

The electronization of society connects the human communities with their activities in many spheres of their existence. These include not only transport, network management, and critical infrastructure, but also the areas of health and healthcare, which provide their users with relevant services. Given the fact that medical and therapeutic interventions are a clear interference with the integrity of the individual - even with his or her consent - the provision of specific health care, in relation to the electronic boom, remote electronic tools and, above all, in connection with the use of artificial intelligence, resonates with legitimate questions, not only in relation to the safety of their use, but also to the application of liability, for example, in the event of damage caused by the relationship.

¹ Tereza Jonáková - Department of Public Administration, Police Academy of the Czech Republic, jonakova@polac.cz.

Responsible service providers should fully respect their limits within the information society, as they should be aware of the interconnectedness of technology, which is not absolute in its nature². At the same time, it is more than appropriate to apply systemic approaches in this matter, not only at the level of conceptual, congruent, and substantive contexts, but also at the level of organisational and procedural ones. Thus, at the very least, a basic, consistent, general, international legal framework and subsequent control by the competent EU institutions would seem appropriate.

2. Electronization of health care

The domestic legislator has historically had suitable inspiration for the area of the electronization of health care in the context of information society services, for example in Act No. 480/2004 Coll. on certain information society services, including the regulation of the liability of service providers, as amended, who provide, through the Internet or other electronic means, for or without payment, the service of data connection³, temporary storage of information⁴ and storage of user data⁵, primarily on the basis of automatically set technical algorithms⁶. In this context, the European legislator has introduced the e-Commerce Directive 2000/31/EC, which, among other things, elaborates the consideration of the limitation of information society service providers in the form of the so-called *safe harbour regime*, which imports the conditions for the emergence from liability.^{7,8,9}

The process of the electronization of healthcare aims to optimise and accelerate healthcare processes and improve accessibility and quality of care¹⁰.

² For more information see Al-Alawy K., Moonesar IA. *Perspective: Telehealth – beyond legislation and regulation*. SAGE Open Medicine. 2023;11. doi:10.1177/20503121221143223.

³ *Mere conduit*, simple data transfer.

⁴ Caching.

⁵ Hosting.

⁶ For more information see also H. Gao, Y. Wu, S. Xu, C. Guo, X. Hou and J. Xu, "TRAC: A Therapeutic Regimen - Oriented Access Control Model in Healthcare," 2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC), Tokyo, Japan, 2018, pp. 388-393, doi: 10.1109/COMPSAC.2018.10263.

⁷ Domestic legislation defines the topic in a positive interpretation, European legislation defines the topic in the opposite way.

⁸ For more details see EUR-LEX. Directive 2000/31/EC of the European Parliament and of the Council [online] [cited 15.1.2024] Available from: <<https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=CELEX%3A32000L0031>>, where Article 12 regulates the limitation of liability and summarises the conditions under which the provider is not liable for the information transmitted.

⁹ For more information see Frosio G., Geiger C. *Taking fundamental rights seriously in the Digital Services Act's platform liability regime*. European Law Journal, 2023; 29(1-2): 31-77. doi:10.1111/eulj.12475.

¹⁰ For more information see Hubmann, M., Pätzmann-Sietas, B. & Morbach, H. *Telemedizin und digitale Akte – Wo stehen wir?*. Monatsschr Kinderheilkd 169, 711–716 (2021). <https://doi.org/10.1007/s00112-021-01241-6>.

The legislator has reflected the basic domestic legislation in Act No. 325/2021 Coll. on the electronization of health care, as amended, and thus anchored, for example, a central repository of electronic prescriptions - ePrescriptions or a central repository of vaccination records. Another service offered by the Social and Financial Policy Party is the "eSick leave", which reports a patient's inability to work. With international overlap, there is also an optional option for health service providers to share electronic summaries of patient data and services provided in other EU Member States. Thus, through the National Contact Point (eHealth)¹¹, the roles and responsibilities of the entities involved in this communication are defined, by mutual agreement, including the definition of an integrated data interface (with so-called tribal registers - of health professionals, providers and patients), through which data between the relevant entities are shared and linked by mutual identifiers in a secure and state-guaranteed manner. Practical considerations of the implementation of the institute of electronic health care could be inspired by the set rules of eGovernment¹² (e.g. in the treatment of the birth number as a possible identifier for accessing electronic health records as an agency identifier of a physical person for eGovernment (AIFO)¹³ or by adjusting the authorization of records in health records including qualified electronic signatures, seals and time stamps, for which the trust services for electronic transactions already defined in eIDAS¹⁴ could be used) including the consistent protection of personal data within the relevant digitization processes, e.g. Also, with the social health sector or with the public control of health insurance companies.

In the European context, it is worth mentioning the creation of a common European Health Data Space (EHDS)¹⁵, which contains both anonymised and pseudo-anonymised data for the purposes of science, research, but also for use in the verification of terms and conditions in risk-sharing and similar contracts between pharmaceutical manufacturers and health insurers, all while maintaining the full functionality of individual certification authorities and qualified AI trust

¹¹ For example, NIX-ZD. The National Contact Point for eHealth information system has been put into operation. [Online]. [cited 16.1.2024] Available from <Informační systém Národní kontaktní místo pro elektronické zdravotnictví spuštěn do ostrého provozu - Zavedení přeshraniční služeb eHealth v České republice – NIXZD.CZ> or e.g. WikiScripts. eHealth. Available from: <eHealth – WikiSkripta>.

¹² More information GOV.CZ. Czech eGovernment. [Online]. [cit.16.1.2024] Available from: <Český eGovernment - gov.cz>.

¹³ This is a general principle of eGovernment, where one person is kept under a different identifier in different government agendas so that it is not easy to identify him/her across different agendas, where the ORG identifier converter is used between the different agendas.

¹⁴ More information e.g. EUROPEAN COMMISSION. eIDAS Regulation [online]. [cit.15.1.2024] Available from: <nařízení eIDAS | Shaping Europe's digital future (europa.eu)>.

¹⁵ For more information see Saelaert, M., Mathieu, L., Van Hoof, W., et al. *Expanding citizen engagement in the secondary use of health data: an opportunity for national health data access bodies to realise the intentions of the European Health Data Space*. Arch Public Health 81, 168 (2023). <https://doi.org/10.1186/s13690-023-01182-4>.

services for the healthcare sector.¹⁶

3. Telemedicine services

The provision of health care to patients by remote means is essentially a new service, which is mentioned by the domestic legislator in the current amendment to Act No. 372/2011 Coll. on Health Services, as amended (hereinafter referred to as the Health Services Act). Telemedicine services (also referred to as "telemedicine" as part of the broader field of "telematics in healthcare")¹⁷ are health services that can be provided remotely using telecommunications and information technologies, under the conditions set out in the law, and subject to technical requirements on the quality and security of communication. The telemedicine spectrum of services is thus considered in the case of telemedicine consultation, telemonitoring and teleconsultation.¹⁸ The provision of care at a distance is equated by the legislator with personal physical contact between the patient and the health care professional and carries with it all the attributes of a responsibility relationship in the process of providing medical and therapeutic services. In relation to the above, the expert public has a clear obligation to establish the form of implementation and the conditions under which health services can be provided in this way, and to create a possible, free, joint, contractual relationship between doctor and patient concluded in a remote manner, with proper instruction to the patient by means of informed consent, the provision of care by a proper professional, and the determination of the standard for the provision of remote health services while compensating for damages¹⁹.

In the international context, a proposal for a unified legal framework for the provision of telehealth services, including related implementing measures, a concept guide for health service providers, and reference information on the different forms of telemedicine, including teleconsultation, is necessary for the field of telemedicine, for the selection of medical specialities and telemedicine procedures suitable for inclusion in health services and their reimbursement, the identification of responsible persons in the provision of telehealth services, the design of a methodology for assessing appropriate hardware and software equipment for the provision of telehealth services, cybersecurity, training opportunities, etc.

¹⁶ For more details see European Commission. European Health Data Space. [Online]. [Cited 24.1.2024] Available from: <Evropský prostor pro zdravotní data - Evropská komise (europa.eu)>.

¹⁷ The term eHealth (electronic health), defined by the WHO as electronic health, is a more cost-effective and safer use of communication and information technologies to promote health.

¹⁸ For more information see Society of General Medicine ČLS JEP. Recommended practices [online]. [cit.2.1.2024] Available from: <<https://www.svl.cz/doporucene-postupy/doporucene-postupy-pro-pl-zpracovane-2020-2022/>>.

¹⁹ For more information see Brönneke, J.B., Debatin, J.F. *Digitalisierung im Gesundheitswesen und ihre Effekte auf die Qualität der Gesundheitsversorgung*. Bundesgesundheitsbl 65, 342–347 (2022). <https://doi.org/10.1007/s00103-022-03493-3>.

4. Artificial intelligence

Artificial intelligence in general, and certainly even more so in the field of health, has so far, its limits, and does not reach the same qualities as the natural personality of a particular person. The ability of AI is characterized by imitating human reasoning, learning, planning or creativity. It is also assumed that AI systems are capable of working autonomously and adapting their actions based on evaluating the effects of previous actions.²⁰ However, the acceleration of the progress of development in the field anticipates a close and realistically comparable intelligence to humans, or even more so, smarter and more complex in reasoning in both the physical and digital worlds, including related connotations fitting into the subject matter²¹. The European Commission states that "Artificial Intelligence (AI) systems are software (but also hardware) systems created by humans that are given the complex task of acting in the physical or digital dimension using their perception of their surroundings by collecting data, interpreting the collected structured or unstructured data, reasoning with knowledge or processing the information derived from the data and selecting the best course of action to achieve a set goal. AI systems can use symbolic rules or learn numerical models, and can also adapt their behavior based on an analysis of how their previous behavior has affected their environment."²²

Not only for the reason outlined above, when artificial intelligence has a significant potential to replace many professions of human life, including in the field of health care, it is necessary to define clear boundaries for artificial intelligence, including a purposeful construction of its **responsibility** and its implementation within a transparent liability relationship, which forms the complex of artificial intelligence itself²³.

There are several expert opinions on the **responsibility of artificial intelligence**, which are linked to the very logical fact that a new entity - artificial intelligence - is relevant as an additional, new entity in the interaction relationship between the provider and the client, either as an intermediary or as a substitute for the service provider itself. Relevant discussions thus need to be directed not only to the actual final liability, but also to its scope of 'incremental' legal limits,

²⁰ For more information see News European Parliament. *What is artificial intelligence and how is it used?* [Online]. [cit. 15.1.2024] Available from: <https://www.europarl.europa.eu/_news/en/headlines/priorities/artificial-intelligence-in-the-eu/20200827STO85804/what-is-artificial-intelligence-and-how-is-it-used>.

²¹ For more information see Sharma, Sachin; Rawal, Rajl; Shah Dharmesh. *Addressing the challenges of AI-based telemedicine: Best practices and lessons learned*. Journal of Education and Health Promotion (1):338, September 2023. | DOI: 10.4103/jehp.jehp_402_23.

²² Kolaříková, Linda and Filip Horák. *Artificial Intelligence & Law*. Prague: Wolters Kluwer, 2020. Legal monographs (Wolters Kluwer ČR). ISBN 978-80-7598-783-9, p. 7.

²³ For more information see also Enas Mohammed Alqodsi & Dmitry Gura (2023) *High tech and legal challenges: Artificial intelligence-caused damage regulation*, Cogent Social Sciences, 9:2, DOI: 10.1080/23311886.2023.2270751.

including compliance options²⁴. A complicated question of liability thus arises not only in the case of the position of the AI towards the end user, but also in its very multilayered nature in terms of its final form and the varying scope of ownership or copyright. Artificial intelligence creates a non-standard complex of the very conduct of individual layers of different characters, and often impossible to determine the primary originator of the autonomous structure itself. The solution to the situation outlined above would be to grant artificial intelligence a legal personality by which it would become another type of person within a relevant, accountable relationship, alongside the *bearer provider* and the *addressee client*, i.e. alongside natural and legal persons²⁵. However, a different construction of liability for legal and natural persons would imply further exploration of the construction of AI liability, e.g. from the perspective of the possibility of active or passive legal status, including the concept of imputability of the conduct in question. If artificial intelligence has the natural ambition to go beyond human decision-making, then it would be logical for it to have the full scope of active and passive legal status, but quite logically also the corresponding equal protection of rights and ethical rules²⁶, which in the given context may in the future imply many obligations and limitations for humans. The liability of AI as a whole would thus anticipate, for example, the possibility of owning property and being liable for compensation for damage caused by the operation of autonomous systems, things or product defects. Equally, on the other hand, there would be the possibility of the AI being exploitable, not only in relation to the developers and manufacturers of the AI²⁷, but also the very risk of an AI with its own personality, possessing the bias of the AI manufacturer (or all its individual parts) and the associated interpretation of the data used, the processes and controls involved. As part of the ongoing progression of responsible and safe AI in healthcare, the professional community is talking about the requirements for designing and implementing systems that are legally and ethically transparent, fair to all participants, understandable, and explainable in their decision-making.

AI activities are quite legitimately related to the issue of compulsory AI insurance, which would contribute to greater protection of third parties against

²⁴ Polcak Radim. *Responsibility of artificial intelligence and information services without legal personality*. *Advocacy Bulletin*.

²⁵ For more information see also Simona Tiribelli, Annabelle Monnot, Syed F. H. Shah, Anmol Arora, Ping J. Toong and Sokanha Kong, *Ethics Principles for Artificial Intelligence-Based Telemedicine for Public Health*, *American Journal of Public Health* 113, no. 5 (May 1, 2023): pp. 577-584. <https://doi.org/10.2105/AJPH.2023.307225>.

²⁶ For more information see European Commission. Ethical guidelines for trustworthy artificial intelligence. [Online]. [cited 10.1.2024] Available from: <Etické pokyny pro důvěryhodnou umělou inteligenci | Utváření digitální budoucnosti Evropy (europa.eu)>.

²⁷ For more information see *The Guardian*. Tesla has confirmed that Autopilot was involved in the Utah crash, but is trying to blame the driver. [Online]. [Cited Jan 12, 2024]. Available from: <<https://www.theguardian.com/technology/2018/may/16/tesla-autopilot=utah=crash=confirms=investigation>>.

damage that may be caused by the operation of AI activities. The scope of insurance in relation to AI activities can then range from a failure of service to the client, to loss of data, to deliberate acts by the owners' employees, e.g. in the event of theft or unauthorised use of AI. The AI could receive compensation funds from, for example, insurance or from the authorities involved in its activities. Insurance for AI in the healthcare and telemedicine sector could then cover e.g. breach or negligence of duty, errors, omissions in connection with the development, production, management and implementation of software, hardware, telecommunications equipment, inadvertent infringement of intellectual or proprietary rights, damage caused by viruses, breach of trust or misuse of information, failure of the proprietary system, dishonest or fraudulent conduct by employees or freelancers, etc.

5. Conclusion

The right to health protection can be generally declared from the Resolution of the Presidium of the Czech National Council No. 2/1993 Coll. the Charter of Fundamental Rights and Freedoms, as amended (hereinafter referred to as the "CFR"), the provisions of Article 31, where "Everyone has the right to health protection. Citizens shall have the right to free health care and to medical aids under the conditions laid down by law on the basis of public insurance." Article 3 of the Communication of the Ministry of Foreign Affairs No. 96/2001 Coll. on the adoption of the "Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine, as amended" states, quote: "The Parties, having regard to health needs and available resources, shall take appropriate measures to ensure equitable access to health care of appropriate quality within their jurisdiction." In relation to exceptional cases, the provisions of "Article 2 of the Communication of the Federal Ministry of Foreign Affairs on the Negotiation of the Convention for the Protection of Human Rights and Fundamental Freedoms and the Protocols thereto, as amended", the right to life may also be cited.

However, the legal declaration of health protection as a fundamental right of the individual is not so much at stake as the real impact of synergistic effects on the rising costs of demographic and technological developments in the health sector, declared by the WHO, which states that by 2030 there will be a global shortage of 10 million health professionals, which will quite logically reduce the availability of health care. If we think in terms of specific figures on the availability of medical care in the Czech Republic, it can be noted that "the number of full-time physicians and dentists in the Czech Republic increased by 40.6% between 1993 and 2016 (from 34 934 to 49 101), when the population of the Czech Republic increased by 2.4% over the same period"²⁸. If we put this information

²⁸ See *Czech Republic in data*. Availability of health care in the Czech Republic. [Online]. [cited

into context with the fact of the development of the demographic structure and the ageing population, the uneven distribution of doctors within the Czech Republic and the increase in the number of hospital admissions, the whole situation starts to become very uncomfortable. The appropriate solution for maintaining access to healthcare and the right to health seems to be the possibility of telemedicine, which the WHO describes as²⁹:

- consultation between a remote patient and a health professional,
- remote monitoring of health status and diagnostic data by a provider,
- transmission of health data, and
- consultation in clinical decision-making between health professionals.

The state of telemedicine in the Czech Republic entered a clearer picture in the form of an amendment to the Health Services Act in the summer of 2023, which the legislator stated, in the proposed wording of the provisions of Section 11c(1) of the Health Services Act, as follows: '[First legal definition:] Telemedicine health services means health services that are provided remotely using information and telecommunication technologies or a medical device. Telemedicine health services may be provided only if the technical requirements for the quality and security of the communication are met, the communication channel is encrypted, and the verification of the identity of the communicating parties is ensured. The communication may only be recorded by the provider with the consent of the patient.' For the proper provision of health services 'lege artis', often used by case law and judicial interpretation, the critical question arises as to who could provide distance health services and under what conditions, and whether it is possible to modify the standard of proper professional care for remote health services. At the same time, it should be noted that the government's proposal on distance provision declared that 'it is not a separate form or type of health service, but a method of providing healthcare'.

Doubts over the process of remote provision of health services are created by the discourse where the legislation in the Health Care Act does not specifically speak about an explicit prohibition of remote provision of health services; however, the legislation assumes the provision of health services to the patient in places designated for these purposes – i.e. in healthcare facilities listed under authorisation to provide health services. On the subject, an amendment to the Health Care Act was adopted in January 2022 to the effect that 'consultation services' can be provided remotely outside healthcare facilities, which allows for the possibility of part of the practice of telemedicine. Thus, the legislator must

31.1.2024] Available from: <<https://www.ceskovdatech.cz/clanek/112-dostupnost-zdravotni-pece-v-cesku/#article-content>>.

²⁹ For more information see also Arama, E., Maximilian, S., Rotaru, L., Vovc, V. (2020). *Telemedicine—Advanced Technology at the Service of Society*. In: Tiginyanu, I., Sontea, V., Railean, S. (eds) 4th International Conference on Nanotechnologies and Biomedical Engineering. ICNBME 2019. IFMBE Proceedings, vol. 77. Springer, Cham. https://doi.org/10.1007/978-3-030-31866-6_116.

clearly define not only the term of telemedicine services (if it is a field within the meaning of Section 4 – 4 – of the Health Care Act, a type within the meaning of Section 5 of the Health Care Act or a form within the meaning of Section 6 of the Health Care Act), but also the basic framework of their use and legal certainty for the entities interested in the given relationship, not only within the framework of domestic legislation, but also in the cross-border provision of the given services.³⁰

The range of providers and services within the legally safe provision of telehealth services can thus be defined as those who:

- are not providers of health services and are merely facilitators between the patient and the provider;
- are health service providers and who provide consultative services (not basic diagnosis or decision-making on the course of treatment);
- are entities that only use information and telecommunication technologies without the presence of the patient (possibly also using remote access or a medical device – e.g. teleradiology, telepathology);
- are entities that obtain health information remotely or by means of a medical device and automatically send this information to the provider (telemonitoring).

A range of health service providers who would not have the patient ‘physically’ in their care could, under the principle of legal licensing, provide consultancy services (including e.g. second opinions) and sub-services e.g. In the sense of Section 4(5) of the Health Care Act, this would be an objective corrective to the rules of science and proper professional practice, while respecting the individuality of the patient and taking into account specific conditions and objective possibilities.

The standard of care *lege artis* brings quality improvement in the remote care, e.g. in the areas of cardiology (e.g. screening for atrial fibrillation), remote postoperative wound monitoring, remote glycaemic control, applications for coeliacs and reduction of GI symptoms, evaluation of cochlear implant function, etc. However, at the same time, there is also a possible increase in risks, especially in the form of diagnostic errors, due to limitations in patient contact (palpation examination, posture and movement of the patient, etc.).

A possible reduction in the required objective standard of care for the distance mode of care is possible if we accept that individually performed procedure is always evaluated on the basis of risk-benefit ratios, where the primary aspects on the benefit side are autonomy of the will and preservation of access to care. Within the framework of autonomy of the will, a fully informed patient should be able to prioritise the benefits of telemedicine/e.g. time, convenience,

³⁰ For more information see Regulation (EC) No. 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I), Regulation (EC) No. 864/2007 of the European Parliament and of the Council of 11 July 2007 on the law applicable to non-contractual obligations (Rome II).

accessibility/even at the cost of necessarily increased risk, which must be consistently communicated. Thus, preserving access to care may ultimately outweigh the risks, where the absence of care would be a greater violation of the right to health protection than the necessary increase in risk, but all of this is subject to consistently overcoming legislative ambiguities and creating its own standard for the different branches of healthcare provided under telemedicine services.

Bibliography

1. Al-Alawy K., Moonesar IA. *Perspective: Telehealth – beyond legislation and regulation*. SAGE Open Medicine. 2023, 11. doi:10.1177/20503121221143223.
2. Arama, E., Maximilian, S., Rotaru, L., Vovc, V. *Telemedicine—Advanced Technology at the Service of Society*. In: Tiginyanu, I., Sontea, V., Railean, S. (eds) 4th International Conference on Nanotechnologies and Biomedical Engineering. ICNBME 2019. IFMBE Proceedings, vol. 77. Springer, 2020, Cham. https://doi.org/10.1007/978-3-030-31866-6_116.
3. Brönneke, J.B., Debatin, J.F. *Digitalisierung im Gesundheitswesen und ihre Effekte auf die Qualität der Gesundheitsversorgung*. Bundesgesundheitsbl 65, 2022, 342–347. <https://doi.org/10.1007/s00103-022-03493-3>.
4. *Czech Republic in data*. Availability of healthcare in the Czech Republic. [Online]. [cited 31.1.2024] Available from: <<https://www.ceskovdatech.cz/clanek/112-dostupnost-zdravotni-pece-v-cesku/#article-content>>.
5. Enas M. A. & Dmitry G. *High tech and legal challenges: Artificial intelligence-caused damage regulation*, Cogent Social Sciences, 2023, 9:2, DOI: 10.1080/23311886.2023.2270751.
6. Eur-Lex. Directive 2000/31/EC of the European Parliament and of the Council [online] [cited 15.1.2024]. Available from: <<https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=CELEX%3A32000L0031>>.
7. European Commission. eIDAS Regulation [online]. [cit.15.1.2024] Available from: <nařízení eIDAS | Shaping Europe’s digital future (europa.eu)>.
8. European Commission. Ethical guidelines for trustworthy artificial intelligence. [Online]. [cited 10.1.2024] Available from: <<https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai>>.
9. European Commission. European Health Data Space. [Online]. [Cited 24.1.2024]. Available from: https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space_cs.
10. Frosio G., Geiger C. *Taking fundamental rights seriously in the Digital Services Act’s platform liability regime*. European Law Journal, 2023; 29 (1–2): 31–77. doi:10.1111/eulj.12475.
11. Gao H., Wu Y., Xu S., Guo C., Hou X. and Xu J., *TRAC: A Therapeutic Regimen-Oriented Access Control Model in Healthcare*, 2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC), Tokyo, Japan, 2018, 388–393, doi: 10.1109/COMPSAC.2018.10263.
12. GOV.CZ. Czech eGovernment. [Online]. [cit.16.1.2024] Available from: <Český eGovernment – gov.cz>.
13. Hubmann, M., Pätzmann-Sietas, B. & Morbach, H. *Telemedizin und digitale Akte – Wo stehen wir?* Monatsschr Kinderheilkd 169, 2021, 711–716, <https://>

- doi.org/10.1007/s00112-021-01241-6.
14. Kolarikova, L. & Horak F., *Artificial Intelligence & Law*. Prague: Wolters Kluwer, 2020. Legal monographs (Wolters Kluwer ČR). ISBN 978-80-7598-783-9.
 15. News European Parliament. *What is artificial intelligence and how is it used?* [Online]. [cit.15.1.2024] Available from: <<https://www.europarl.europa.eu/news/en/headlines/priorities/artificial-intelligence-in-the-eu/20200827STO85804/what-is-artificial-intelligence-and-how-is-it-used>>.
 16. Regulation (EC) No. 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I).
 17. Regulation (EC) No. 864/2007 of the European Parliament and of the Council of 11 July 2007 on the law applicable to non-contractual obligations (Rome II).
 18. Saelaert, M., Mathieu, L., Van Hoof, W., et al. *Expanding citizen engagement in the secondary use of health data: an opportunity for national health data access bodies to realise the intentions of the European Health Data Space*. Arch Public Health 81, 2023, 168. <https://doi.org/10.1186/s13690-023-01182-4>.
 19. Sharma, S., Rawal, R. Shah D. *Addressing the challenges of AI-based telemedicine: Best practices and lessons learned*. Journal of Education and Health Promotion (1), September 2023, 338, DOI: 10.4103/jehp.jehp_402_23.
 20. Society of General Medicine ČLS JEP. Recommended practices [online]. [cit.2.1.2024] Available from: <<https://www.svl.cz/doporucene-postupy/doporucene-postupy-pro-pl-zpracovane-2020-2022/>>.
 21. *The Guardian*. Tesla has confirmed that Autopilot was involved in the Utah crash, but is trying to blame the driver. [Online]. [Cited Jan 12, 2024]. Available from: <<https://www.theguardian.com/technology/2018/may/16/tesla-autopilot=utah=crash=confirms=investigation>>.
 22. Tiribelli S., Monnot A., Shah S. F. H. Arora A., Toong P. J., and Kong S., *Ethics Principles for Artificial Intelligence – Based Telemedicine for Public Health*, American Journal of Public Health 113, no. 5 May 2023, 577–584, <https://doi.org/10.2105/AJPH.2023.307225>.

Digital Currencies: Individual Perceptions of the Impact on Money Laundering and the Transition to a Cashless Environment

PhD. student **Cristina S. CĂPĂȚÎNA (DUMITRACHE)**¹
PhD. student **Dragoș BÎLTEANU**²

Abstract

Based on the correlation between the use of cash and criminal activity demonstrated in the literature, we conducted a survey to identify the civilian community's perception of the extent to which the adoption of cashless transactions could mitigate criminal behaviour. Our study investigates both attitudes towards digital currencies and the feasibility of transitioning to a cashless society. The survey results show scepticism towards limiting cash as a comprehensive solution to combat illicit financial activities, highlighting the importance for policymakers to weigh the potential benefits against criminal adaptability. The varied perspectives among legal and public policy respondents highlight the nuanced considerations surrounding cash restrictions, with some advocating their benefits in combating money laundering while others remain sceptical. Concerns expressed by respondents about privacy, institutional control and economic autonomy highlight the multiple implications of the transition to a cashless society. These findings underline the need for robust legal and regulatory frameworks to protect individual privacy rights and ensure transparency in the use of transaction data. In addition, respondents' concerns about oversight and trust in digital payment systems underscore the need for thorough analysis prior to the adoption of centralised digital currencies.

Keywords: money laundering, cryptocurrency, CBDC, blockchain, cash.

JEL Classification: E42, H26, K14, K24

DOI: <https://doi.org/10.62768/ADJURIS/2024/1/05>

Please cite this article as:

Căpățîna (Dumitrache), Cristina S. & Dragoș Bîlteanu, „Digital Currencies: Individual Perceptions of the Impact on Money Laundering and the Transition to a Cashless Environment”, in Pajuste, Tiina, Heliona Bellani (Miço) & Sejla Maslo Cerkić (eds.), *Legal Perspectives in the Modern Era of Technological Transformations*, ADJURIS – International Academic Publisher, Bucharest, Paris, Calgary, 2024, p. 75-102.

1. Introduction

Cash remains the preferred medium for illicit funds in the initial phases

¹ Cristina S. Căpățîna (Dumitrache) - Doctoral School of Finance, Bucharest University of Economic Studies, Romania, capatinacristina12@stud.ase.ro.

² Dragoș Bîlteanu - Doctoral School of Finance, Bucharest University of Economic Studies, Romania, d.bilteanu@gmail.com.

of money laundering³. In the placement phase, criminals strive to integrate the proceeds of criminal activity into legitimate financial channels or bank accounts. This phase presents a vulnerability for criminals as they attempt to inject significant amounts of money into the financial system, often in bulk. Even in cases of wire fraud, criminals resort to withdrawing stolen funds from bank accounts, transporting cash across borders or transferring it to alternative accounts to disrupt audit trails.

Law enforcement agencies face a multitude of challenges arising from different legislative frameworks, administrative structures and regulatory authorities in different jurisdictions. Each state operates within distinct criminal justice systems, civil procedures and financial supervision mechanisms, which adds complexity to the anti-money laundering task. These inherent complexities may partly explain the perceived inadequacy of conventional anti-money laundering measures. In addition, the continued reliance on cash as the primary means of carrying out illicit activities is a significant obstacle to effective law enforcement efforts. Given the anonymity, lack of connection and untraceability inherent in cash transactions, it continues to be a preferred instrument for criminal transactions.

This paper is the next step in the research aimed at exploring the advantages and disadvantages of replacing cash with digital currencies (cryptocurrency and Central Bank Digital Currency – CBDC) as a means of combating money laundering from the perspective of private actors through a survey. In the first approach carried out in this direction⁴, we argued that replacing cash with a central bank digital currency (CBDC) or cryptocurrency could be a feasible strategy to reduce financial crime, i.e. money laundering. By replacing cash with cryptocurrencies, the crime rate could be reduced, primarily by limiting the number of criminals due to the technical expertise required to navigate these platforms. We showed that despite their association with certain criminal activities, cryptocurrencies were still a relatively safe medium in 2021, with only 0.15% of the total volume of cryptocurrency transactions related to money laundering. However, just moving to cryptocurrencies does not guarantee a future with less money laundering, as transactions are not transparent and often take place anonymously. This challenge could be addressed through collaboration between law enforcement agencies and stakeholders driving blockchain technology. Efforts towards such partnerships show promising prospects for harnessing the technology used by criminals to help apprehend them. We have

³ Guerino Ardizzi, Pierpaolo De Franceschis, and Michele Giammatteo, *Cash Payment Anomalies and Money Laundering: An Econometric Analysis of Italian Municipalities*, *International Review of Law and Economics* (Print) 56 (December 1, 2018): 106, <https://doi.org/10.1016/j.irle.2018.08.001>.

⁴ Cristina Căpățină and Raluca Ghețu, *Investigating Cash Replacement as a Means of Fighting Money Laundering: The Case of Digital Currency and Its Economic Impact*. Proceedings of the 39th International Business Information Management Association (IBIMA) (2022): 3502–3504. Accessed March 4, 2024.

also shown that CBDCs offer a potentially more effective solution for reducing financial crime due to their inherent transparency and lack of anonymity. The technology supporting CBDCs ensures both security and privacy while maintaining traceability. However, the centralized nature of CBDCs raises concerns about government oversight, and it is unclear whether people would prefer a centralized approach over a decentralized one that relies on banks and other private entities.

This study presents the perception of the civil community based on the results of a detailed survey conducted on a sample of 100 respondents, predominantly from Romania, to which were added participants from various countries, including the UK, Canada, France, Germany, Ireland and Brunei. Conducted until October 2023, the survey was designed to assess individuals' perceptions of cryptocurrencies and central bank digital currencies (CBDCs). Specifically, the survey sought to elucidate respondents' views on the potential of these digital currencies to mitigate money laundering by replacing conventional cash transactions. In addition, the survey sought to deepen participants' perceptions of the feasibility and desirability of transitioning from cash to digital currencies. Through this research, we aim to shed light on individuals' attitudes towards the role of digital currencies in the fight against financial crime. By exploring their perspectives on both cryptocurrencies and CBDCs, as well as their desire to embrace a cashless society, we sought to uncover insights into the perceived benefits and threats of these emerging technologies. The results of this survey provide valuable insight into the prevailing sentiments among the public regarding the usefulness of cryptocurrencies and CBDCs as potential tools for increasing financial transparency and reducing illicit financial activities. By disseminating these findings, we hope to contribute to informed discussions and policymaking efforts aimed at harnessing the transformative potential of digital currencies in promoting financial integrity and security.

This paper is divided into three sections. After this introduction, section II discusses the literature on the nuemark and its link to money laundering, and section III is devoted to presenting the current state of cryptocurrency and the digital currencies we have previously proposed as an alternative way to combat money laundering. Section IV deals with conclusions and recommendations drawn from the results of the study.

2. Literature

Between 2011 and 2015, the European Union recorded an average cash usage rate of around 42%, although there were considerable disparities between Member States. In particular, Finland, the United Kingdom, France and Sweden had cash usage rates below 30%, while Greece, Bulgaria and Romania relied on banknotes and coins for more than 80% of transactions. In addition, larger economies such as Germany and Italy reported high cash usage rates of 65% and

53.2% respectively⁵. According to the Payment and Market Infrastructures Commission and the Markets Commission⁶, the accessibility and continued use of physical currency can contribute to greater resilience by providing a means of communication less susceptible to disruptions caused by natural or man-made disasters affecting electricity and communication infrastructures.

The role of cash in facilitating money laundering has long been recognised, leading to different measures taken by individual countries to monitor cash transactions that exceed specific thresholds. However, the upward trajectory of this phenomenon indicates that these actions are insufficient. When cash plays a crucial role in the offender's decision-making process, reducing the movement of cash would lead to a decrease in acquisitive crime. Cashless transactions not only provide speed and convenience, but also contribute to lower crime rates. This is attributed to the absence of physical currency to steal, launder or evade taxes, as digital transactions leave a wider audit trail⁷. The Ethiopian government has responded to the challenge posed by the cash-based nature of the Ethiopian economy by imposing limitations on cash withdrawals from financial institutions, setting maximum limits on cash holdings, and demonetizing certain banknotes to address the proliferation and spread of financial crime linked to the cash-centric economy, to encourage the adoption of non-cash payment methods, and to protect the integrity and efficiency of the nation's payment infrastructure. The authors concluded in their study that the ultimate objective of these measures is to ensure the transition of Ethiopia's cash-intensive economy to a cashless model, thereby mitigating the prevalence of illegal activities associated with cash transactions. The study highlights the need not only to adopt and implement sound financial regulatory frameworks, but also to promote a comprehensive transformation of the cash-based economy and to establish an accessible and compatible financial infrastructure adapted to the needs of society. Based on primary data from interviews with 20 stakeholders representing the NBE, the Ethiopian Financial Intelligence Centre, commercial banks and law enforcement agencies, the authors argued that while these directives are necessary, they are not comprehensive enough to effectively curb future criminal activity. Regarding the correlation between cash and the underground economy, ⁸ showed that as the proportion of

⁵ Michele Riccardi and Michael Levi, *Cash, Crime and Anti-Money Laundering*, in Springer eBooks, 2018, 139, https://doi.org/10.1007/978-3-319-64498-1_7.

⁶ Committee on Payments and Market Infrastructures and Markets Committee, Bank for International Settlements. 'Central Bank Digital Currencies.' (2018): 7. Accessed March 12, 2024. <https://www.bis.org/cpmi/publ/d174.pdf>.

⁷ Messay Asgedom Gobena and Derege Kebede, 'Cash Economy, Criminality and Cash Regulation in Ethiopia,' *Journal of Money Laundering Control* 25, no. 3 (August 28, 2021): 9, <https://doi.org/10.1108/jmlc-06-2021-0065>.

⁸ Schneider, Friedrich. *Restricting or Abolishing Cash: An Effective Instrument for Fighting the Shadow Economy, Crime and Terrorism?*, Conference Paper at International Cash Conference 2017 – War on Cash: Is There a Future for Cash? : 6–9, 25–27 April 2017, Island of Mainau, Germany, April 2017.

cash in total payments increases, so does the extent of the underground economy, with the relationship supported by a correlation coefficient of 0.50, indicating a strong and statistically significant association between the two variables. The author showed that a 10% decrease in cash payments correlates with a 2% reduction in the underground economy. In contrast, the assumption of a no-cash scenario would lead to a substantial 20% decrease in the underground economy, while cash limits do not produce statistically significant effects on the underground economy. Schneider (2017) also used a micro-study approach, exploring responses to the hypothetical scenario of a cashless society. Of the respondents who paid cash for services because it is anonymous, a significant proportion would seek alternative payment methods in the absence of cash. Specifically, 33% would opt for cashless transactions, 13% would proceed with increased tax considerations, 13% would no longer need these services, and 41% would explore alternative anonymous payment options such as vouchers or gifts. The author concludes that overall, while cash remains entrenched in the underground economy, its influence is not paramount, with a 10 to 20% reduction expected following its elimination, a reduction in corruption of between 1.8 and 18 percentage points (extreme case: cashlessness), a reduction in crime of between 5 and 10%. The same author also showed that cash is used predominantly in eight of the twelve most common laundering methods, indicating its significant role in facilitating these illicit financial activities. The prevalence of cash in money laundering underlines the challenges of combating illicit financial activities. Many common laundering methods, such as cash deposits, smuggling and ATM operations, predominantly involve cash transactions.

Another study⁹ showed that the EBT program (electronic benefit transfer program, a digital, debit card-based system) demonstrated a notable and statistically significant decrease in the overall crime rate, particularly in cases of burglary, assault, and theft. Point estimates showed a 9.8% reduction in the overall crime rate following the implementation of the EBT programme. According to the same authors, this decline in the crime rate in the United States over successive decades has corresponded with a steady decline in the proportion of financial transactions conducted with cash.

3. Cryptocrime and the challenges of digital currencies

In the area of cryptocurrency-related crime, money laundering usually involves the transfer of funds to platforms where they can be exchanged for cash, often accompanied by additional measures to hide their original source. A prominent argument that virtual currencies such as cryptocurrencies are an

⁹ Richard Wright., Volkan Topalli, Chandler Mccellan and Erdal Tekin. *Less Cash, Less Crime: Evidence from the Electronic Benefit Transfer Program*. The Journal of Law and Economics, 60, no. 2 (2017): 361–383. Accessed March 15, 2024:18, 25, <https://doi.org/10.1086/693745>.

effective mechanism for money laundering is their ability to facilitate cross-border payments without relying on the services of traditional financial institutions¹⁰. A primary criticism of cryptocurrencies, particularly in terms of their use on the dark net, revolves around the level of anonymity they offer¹¹. While cash transactions offer complete anonymity, cryptocurrencies offer less anonymity. Bitcoin, being the predominant cryptocurrency, operates under pseudonymity. Users are identified by addresses, but the real identity behind these addresses remains undisclosed to the public. However, the degree of anonymity in practice is subject to debate. Extensive academic research^{12,13} has shown that the level of anonymity in Bitcoin does not match the original assumptions. Cash remains the main tool for criminal activity, given its superior anonymity and utility compared to cryptocurrencies¹⁴. However, the future trajectory of the currency is uncertain, highlighting the importance for policymakers to research beyond sensational headlines and understand the complexity of the cryptocurrency debate.

In its most recent examination of cryptocurrency laundering through chain analysis¹⁵, it has been shown that in 2023, there was a notable decrease in the amount of cryptocurrency, worth \$22.2 billion, sent from illicit addresses to various services. This figure represents a substantial drop compared to the \$31.5 billion sent in 2022. While some of this decline can be attributed to an overall reduction in the volume of cryptocurrency transactions, including both legitimate and illicit transactions, the decline in money laundering activity was even more pronounced. Specifically, there was a 29.5% decrease in money laundering activity, exceeding the 14.9% decrease observed in total transaction volume. In 2023, the majority of illicit funds sent to¹⁶ fiat currency settlement services were concentrated in just five platforms, accounting for 71.7% of the

¹⁰ US Department of Justice, National Drug Intelligence Centre. 'Money Laundering and Digital Currencies.' www.justice.gov. US Department of Justice, June 3, 2008:1, <https://www.justice.gov/archive/ndic/pubs28/28675/28675p.pdf>.

¹¹ Simon Butler, *Criminal Use of Cryptocurrencies: A Great New Threat or Is Cash Still King?*, *Journal of Cyber Policy* 4, no. 3 (September 2, 2019): 335, <https://doi.org/10.1080/23738871.2019.1680720>.

¹² Dorit Ron and Adi Shamir, *Quantitative Analysis of the Full Bitcoin Transaction Graph*, in *Lecture Notes in Computer Science*, 2013, 10, https://doi.org/10.1007/978-3-642-39884-1_2.

¹³ Elli Androulaki et al., *Evaluating User Privacy in Bitcoin*, in *Lecture Notes in Computer Science*, 2013, 47, https://doi.org/10.1007/978-3-642-39884-1_4.

¹⁴ Simon Butler, *op. cit.*, p. 331, <https://doi.org/10.1080/23738871.2019.1680720>.

¹⁵ Chainalysis. *The Chainalysis 2024 Crypto Crime Report*. (2024): 23, Accessed March 9, 2024. <https://go.chainalysis.com/crypto-crime-2024.html>.

¹⁶ 'Fiat currency disconnection services' refers to platforms or services that allow the conversion of cryptocurrencies into traditional fiat currencies, such as US dollars, euros or yen. These services provide users with a means to exchange their digital assets into fiat currency, thereby facilitating their withdrawal or use in traditional financial transactions. Common examples of fiat currency settlement services include centralised cryptocurrency exchanges, peer-to-peer (P2P) exchanges, over-the-counter (OTC) counters, cryptocurrency ATMs and platforms offering cryptocurrency-to-fiat currency conversion services.

total. This represents a slight increase from the previous year, when these top five services accounted for 68.7% of illicit funds flow. The concentration of illicit funds in off-ramping services indicates that cash is still desired by those who wish to hide the origin of their funds or use them in traditional financial transactions. Despite the rise of digital currencies and blockchain technologies, cash remains a widely accepted and versatile form of value exchange, particularly in certain illicit or underground economies where anonymity and liquidity are valued. According to Chainalysis¹⁷, a significant portion of cryptocurrency laundering involves relatively simplistic methods, where malicious actors simply transfer funds directly to cryptocurrency exchanges without using sophisticated techniques. However, cryptocurrency criminals with more advanced chain laundering capabilities, such as the infamous North Korean cyber criminals linked to hacker groups such as the Lazarus Group, often use a wider range of cryptocurrency services and protocols.

As far as CBDCs are concerned, in recent years various countries have started pioneering initiatives in the field of central bank digital currencies. China in particular launched its digital yuan pilot project in 2020, marking an important step in exploring the potential of digital currencies. The project, which runs in twelve cities from March 2022, aims to facilitate small-scale retail transactions and combat the diminishing role of cash. Similarly, Sweden has been testing the feasibility of introducing an e-krona, responding to the trend of declining cash usage and tailored to meet public preferences. The lessons from these initiatives underline the transformative potential of CBDC, albeit accompanied by the imperative for further technological exploration and risk management strategies, as demonstrated by the results of Phase 1 of the Swedish pilots. In addition, other jurisdictions have moved forward with their CBDC efforts, each tailored to address unique socio-economic contexts and objectives. The Sand Dollar in the Bahamas stands out as the world's first CBDC that provides inclusive access to financial services and increases the efficiency of remote island transactions. Meanwhile, Nigeria's eNaira, launching in October 2021, underscores the commitment to financial inclusion and security, leveraging transparency to effectively combat criminal activity. These diverse initiatives collectively highlight the evolving landscape of digital currencies, revealing both opportunities and challenges in reshaping financial ecosystems and addressing societal needs. Georgieva, Managing Director of the IMF in 2022, has stated that a virtual currency issued by a national bank, referred to as a 'central bank digital currency (CBDC)', could potentially offer, 'increased resilience, greater security, increased accessibility and reduced costs compared to privately issued digital currencies, provided it is designed with careful consideration'¹⁸. Georgieva also

¹⁷ Chainalysis, *op. cit.*, p. 29.

¹⁸ Kristalina Georgieva, *The Future of Money: Gearing up for Central Bank Digital Currency*. www.imf.org. International Monetary Fund, February 9, 2022. <https://www.imf.org/en/News/Articles/2022/02/09/sp020922-the-future-of-money-gearing-up-for-central-bank-digital-currency>.

points out that CBDC development is unique to each country, tailored to its specific circumstances and requirements. Legal frameworks, motivations, governance structures and democratic processes vary from jurisdiction to jurisdiction. The Centre for International Governance Innovation examines programmability and oversight, proposing specific technical issues and governance mechanisms to address these concerns, stressing the importance of public trust, which extends beyond central banks to include democratic institutions that protect individual rights and the balance of power. According to them, if programmable money is introduced without regard to privacy issues, CBDCs could become a digital financial data ecosystem, which could raise concerns about state power and oversight¹⁹.

4. Research methodology

The present study uses a survey approach with a sample of 100 respondents mainly from Romania, with participants also from the UK, Canada, France, Germany, Ireland and Brunei, from various areas of expertise, predominantly financial services, legal, business, management and administration, education, and science and technology.

The survey, comprising 13 questions, was conducted until October 2023, allowing for a comprehensive examination of participants' perceptions of cryptocurrencies and central bank digital currencies (CBDCs). The survey was designed to comprise a combination of single-answer and multiple-answer questions, with respondents also given the opportunity to enter their own response, in order to capture nuanced information about participants' attitudes, preferences and understanding of digital currencies. Particular attention was paid to develop questions that elicited detailed responses, ensuring a comprehensive understanding of the varied perspectives surrounding the topic. Data collection was carried out using an online survey platform, which allowed for efficient dissemination and collection of responses from a geographically diverse group of participants. Rigorous data validation procedures were implemented to ensure the accuracy and reliability of the data collected. In addition, ethical considerations were paramount throughout the survey process, and steps were taken to protect the confidentiality and privacy of participants.

In the following, we detail the results of the survey, addressing each question asked in the survey.

Question 1: *When it comes to money laundering, cash is still the king. Do you think that eliminating or limiting cash could help reduce this type of financial crime?*

The results indicate that 19 out of 100 respondents believe that limiting

¹⁹ Centre for International Governance Innovation. *CBDC Governance: Programmability, Privacy and Policies*. Prod. Digital Policy Hub – Working Paper (2024): 10–11, Accessed March 15, 2024. <https://www.cigionline.org/static/documents/DPH-paper-Freiman.pdf>.

or eliminating cash could help reduce money laundering, while only 9 respondents were totally sceptical about the usefulness of eliminating or reducing cash in reducing money laundering (Figure 1).

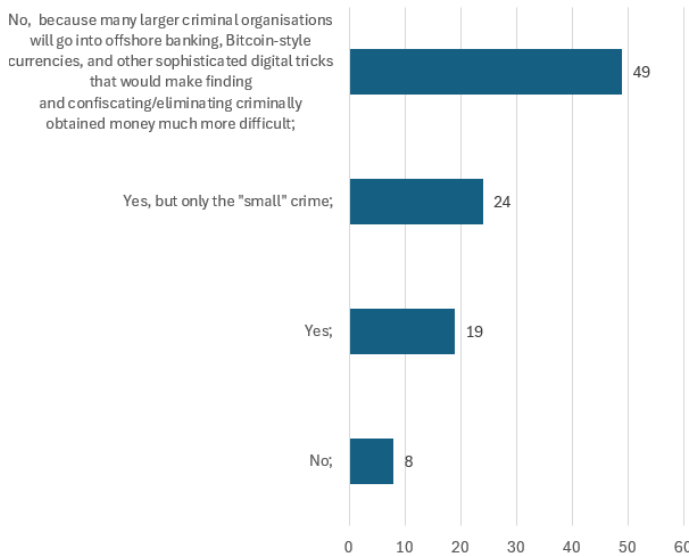


Figure 1. Answers to Question 1: Could eliminate or limiting cash help reduce money laundering?

The majority of respondents (49 out of 100) say that if cash were eliminated or limited, larger criminal organisations would adapt, moving to offshore banking, cryptocurrencies such as Bitcoin or other sophisticated digital methods. This suggests that while limiting cash may prevent some forms of money laundering, criminals are likely to find alternative ways to conduct their illegal activities. Respondents who believe that limiting cash could reduce ‘small’ crimes (24 out of 100) suggest that while it may not eradicate money laundering entirely, it could deter smaller-scale criminals who rely on cash for their operations. Limiting or eliminating cash could be seen as a regulatory measure to combat money laundering. Governments often adopt laws and regulations aimed at increasing the transparency of financial transactions to detect and prevent illicit activities. However, as respondents who expressed scepticism pointed out (49 out of 100), the implementation of such measures could pose significant challenges. Criminal organisations may use sophisticated techniques to evade detection and continue their operations through alternative means, such as offshore banking or cryptocurrencies. This underlines the importance of comprehensive and adaptable legal frameworks to address evolving money laundering methods.

In relation to the field of activity of those interviewed, a significant proportion of respondents in the Business and Administration area of expertise (8 out of 13) express scepticism about the effectiveness of eliminating or limiting

cash in reducing money laundering. Respondents from the financial services sector have mixed views. While some (9 out of 19) share the view that restricting cash may not be effective due to the adaptability of criminals, others (5 out of 19) believe that limiting cash could help reduce ‘small’ crimes associated with money laundering. Legal and public policy professionals have mixed views, with 8 out of 14 believing that cash limits could be beneficial in combating money laundering and 5 out of 14 sceptical because of the adaptability of criminals to alternative financial channels. Only one respondent in this area of expertise strongly believes that eliminating or limiting cash would not help reduce money laundering.

Question 2: *The G7 Financial Action Task Force (FATF) designates tax evasion as a predicate offence for money laundering. Do you believe replacing cash with a more traceable currency could discourage tax evasion?*

Figure 2 shows the survey responses on the possibility of discouraging tax evasion by replacing cash:

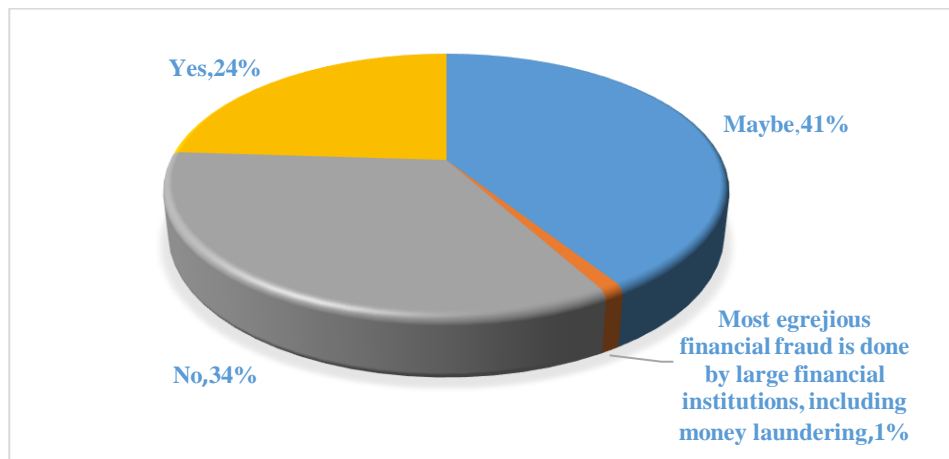


Figure 2. *Answers to Question 2: Do you think that replacing cash with a more traceable currency could discourage tax evasion?*

The results collected present interesting insights, both from an economic and legal point of view, into the potential impact of replacing cash with a more traceable currency on tax evasion. The high proportion of respondents expressing uncertainty (‘Maybe’) about the effectiveness of traceable currencies in deterring tax evasion (41%) suggests a lack of consensus within the community. This uncertainty may stem from a variety of factors, including concerns about the implementation of traceable currencies and their potential effectiveness in deterring tax avoidance behaviour. In addition, responses indicating scepticism (‘No’) about the ability of traceable currencies to deter tax evasion (34%) highlight the inherent complexity of tackling financial crime through technological interventions alone. This scepticism may reflect concerns about the

wider legal and ethical implications of moving to a more traceable currency system. In addition, the proportion of respondents (1%) highlighting that the most serious financial fraud is committed by large financial institutions, including money laundering, underlines the importance of strong regulatory mechanisms to combat financial misconduct, regardless of currency traceability. However, the presence of respondents who expressed a belief in the potential effectiveness of traceable coins in deterring tax evasion ('Yes', 24%) suggests that some individuals perceive traceable coins as a promising tool for increasing financial transparency and combating illicit financial activities.

It is noted that a significant number of respondents from the financial services industry are uncertain ('Maybe') about the effectiveness of traceable currencies in reducing tax evasion (11). This uncertainty could stem from concerns within the financial sector about the practicality and effectiveness of implementing traceable currency schemes. In contrast, legal and public policy respondents express greater confidence ('Yes') in the potential of traceable currencies to deter tax evasion (7). This optimism likely reflects the belief of legal and public policy professionals that increased traceability can facilitate more robust enforcement and compliance measures. However, the diverse range of views reflected in the survey underscores the need for further interdisciplinary research and dialogue to inform policy decisions on the adoption of traceable currencies and their implications for effectively addressing tax evasion.

Question 3: *In some countries, the demand for cash has steadily declined. Why would you give up cash? (multiple choice).*

Fear of theft and robbery associated with large amounts of cash is a predominant concern among respondents (reason found in 52 out of 174 options). From a legal and economic point of view, the risk of theft is not only a physical danger, but also a financial loss for individuals and businesses, requiring investment in security measures. Another substantial group (24 out of 174) highlights, as a reason for giving up cash, the costs associated with cash handling, including counting, processing, security, distribution and staff training. This resonates with economic principles, as businesses and financial institutions incur tangible costs for handling cash transactions that could be minimised or avoided with digital alternatives. Some respondents express concern about the decline in the value of money due to inflation (a reason found in 24 out of 174 options). This is in line with economic theory, according to which holding cash can lead to loss of purchasing power over time, especially if inflation exceeds interest rates on cash deposits. In addition, a subset of respondents cites restrictions on the maximum amount of cash transactions as a factor influencing their willingness to give up cash (25 out of 174). Such restrictions, often imposed by regulators, can limit the usefulness of cash for larger transactions, leading people to explore alternative payment methods.

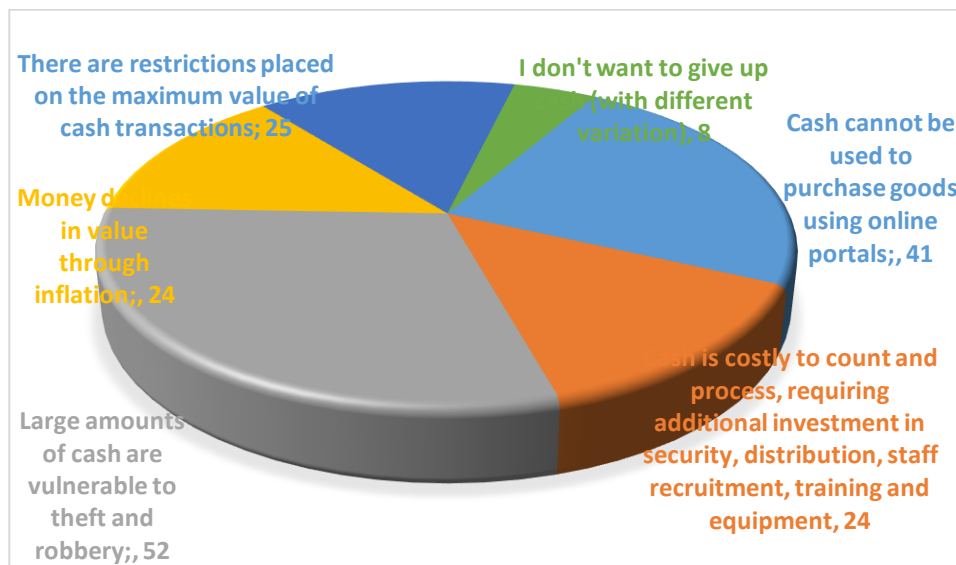


Figure 3. Answers to Question 3: Why would you give up cash?

Despite the practical disadvantages and limitations associated with cash, the reluctance to give it up is found in 8 out of 174 choices made by respondents. This sentiment underlines deep-seated cultural and personal preferences for cash as a tangible form of payment, highlighting resistance to adopting digital alternatives.

These responses highlight the multifaceted considerations involved in individuals' decisions about the use of cash. While technological advances and legislative changes may influence the adoption of digital payment methods, factors such as security, convenience, financial implications and personal preferences continue to shape the dynamics of cash use in society.

Question 4: What do you think are the main reasons why a cashless society is not a good idea? (multiple choice)

The results reveal various concerns and criticisms about the transition to a cashless society (Figure 4).

Forty-four (44) respondents chose the fact that cash is reliable in crisis as a reason against a cashless society: large-scale natural disasters can cause large-scale disruptions to critical infrastructure, affecting financial institutions.

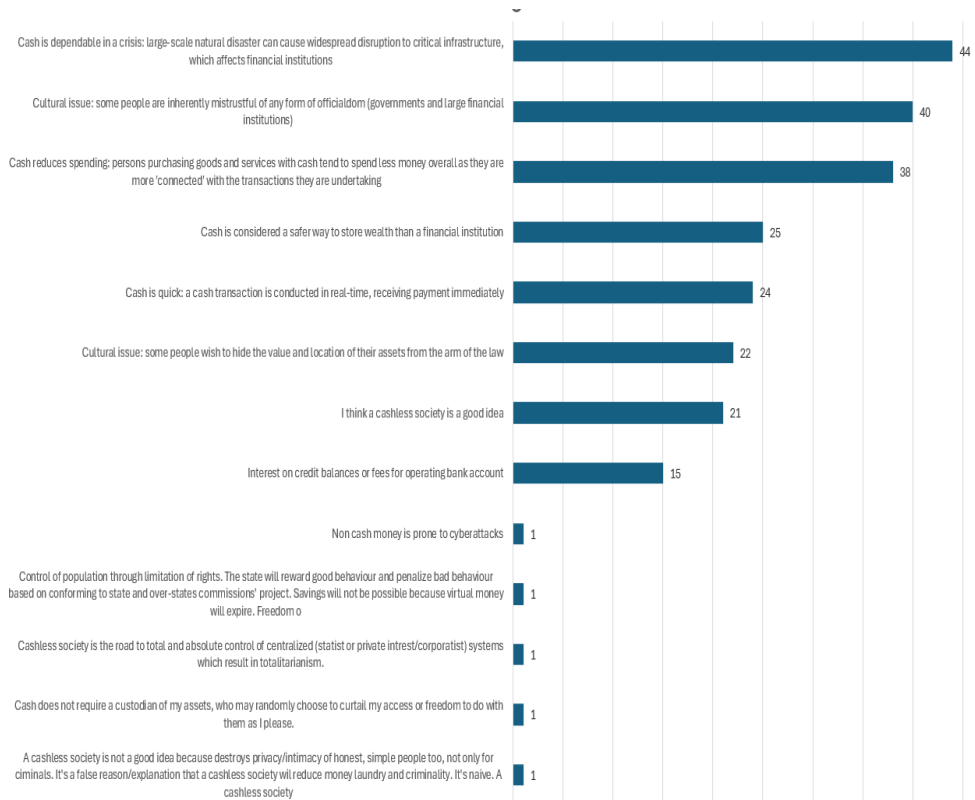


Figure 4. Answers to Question 4: What do you think are the main reasons why a cashless society is not a good idea?

This response highlights the reliability of cash as a form of payment in emergency situations and disruptions, reflecting concerns about the resilience of financial infrastructure and highlighting the importance of stability and accessibility of transactions. Forty (40) respondents cited cultural issues as the main reason, agreeing that some people are inherently distrustful of any form of officialdom (governments and large financial institutions). This response highlights the cultural and behavioural factors that influence attitudes towards government and financial institutions, indicating widespread distrust and scepticism, which may have implications for regulatory compliance and consumer behaviour. Practical and behavioural factors were cited by 38 respondents, citing the fact that cash reduces spending as a reason against a cashless society: people who buy goods and services with cash tend to spend less money in general because they are more ‘connected’ to the transactions they make. This perspective highlights the behavioural aspect of cash transactions, suggesting that the tangibility of cash encourages people to be more mindful of their spending, ultimately leading to reduced expenditure. An interesting 22% of respondents chose as a reason against a cashless society the fact that some people

want to hide the value and location of their assets from the law. This response reflects concerns about privacy and individual autonomy in financial matters, suggesting a desire to maintain privacy in asset management, possibly for legal reasons or personal preference. Twenty-five respondents believe that cash is a safer way to store wealth than a financial institution. This view reflects distrust of financial institutions and suggests a preference for physical cash as a means of protecting wealth, highlighting concerns about the legal and economic risks associated with institutional failures or malpractices. According to 24 other respondents, the main reason for not giving up cash is that it is fast: a cash transaction is carried out in real time, receiving payment immediately. This highlights the practical advantage of cash transactions in terms of speed and immediacy, suggesting a preference for cash over digital payments in certain contexts, which may have implications for the efficiency and convenience of transactions. Of the 100 respondents, a significant proportion (21%) think that the cashless society is a good idea. This represents a contrasting view advocating the benefits of a cashless society, which may include efficiency, transparency and financial innovation, suggesting a recognition of the potential of digital payment systems to address various societal challenges. Interest on credit balances or fees for operating bank accounts were the reasons chosen by 15 respondents against a cashless society. This reflects economic considerations related to the financial costs and fees associated with cashless transactions, suggesting affordability concerns that may have legal implications for consumer protection and financial inclusion.

Other respondents were totally against a cashless society, with the following arguments:

'Cashless society is the road to total and absolute control of centralized systems which result in totalitarianism' (1 respondent): This viewpoint highlights apprehensions about the potential for increased government or corporate control in a cashless society, expressing concerns about the erosion of individual freedoms and democratic principles, which are fundamental legal and ethical considerations.

'Non-cash money is prone to cyberattacks' (1 respondent): This response underscores concerns regarding the vulnerability of digital transactions to cyber threats, suggesting a recognition of the legal and economic risks associated with cybercrime in a cashless society.

'A cashless society is not a good idea because it destroys privacy/intimacy of honest, simple people too, not only for criminals ...' (1 respondent): This response extends the privacy concern beyond criminal activities, suggesting broader implications for personal privacy and intimacy, which have legal and ethical dimensions.

'Cash does not require a custodian of my assets, who may randomly choose to curtail my access or freedom to do with them as I please.' (1 respondent): This highlights concerns about institutional control and autonomy

in asset management, emphasizing the legal and economic implications of custodial arrangements and property rights.

'Control of population through limitation of rights. The state will reward good behaviour and penalize bad behaviour based on conforming to the state and over-state commissions' project. Savings will not be possible because virtual money will expire. Freedom of buying will be very impacted as you will only be allowed to buy products and services that the state allows you to.' (1 respondent): This response raises concerns about potential governmental control and limitations on individual rights in a cashless society, indicating broader socio-political implications for governance and civil liberties, which are fundamental legal and ethical considerations.

Question 5: *Cash allows us to make purchases anonymously. Without cash, we would be forced to leave a record of everything we buy. Do you think governments and or corporations could use one's acquisition history to follow, monitor, or intimidate?*

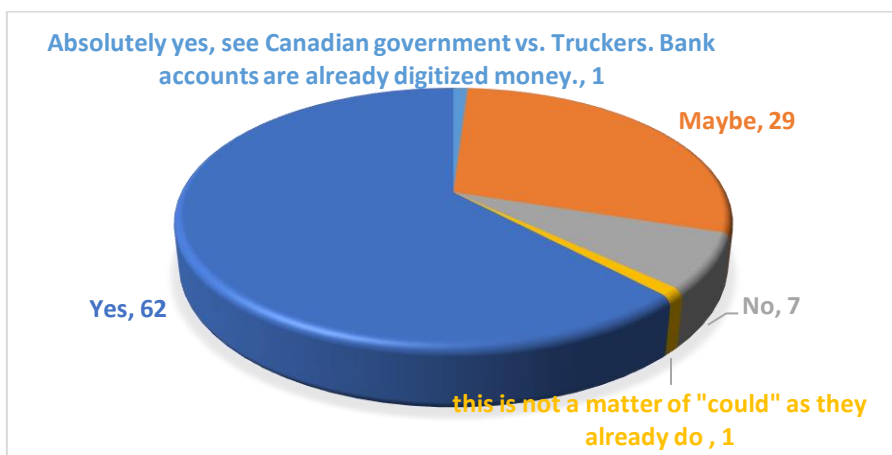


Figure 5. *Answers to Question 5: Do you think governments and/or corporations could use a person's purchase history to track, monitor or intimidate them?*

The results of this survey suggest significant concerns about privacy and government/corporate oversight in a cashless society. The overwhelming majority of respondents (62%) believe that governments and corporations could indeed use people's purchase histories to track, monitor or intimidate them. This view highlights the potential misuse of cashless transaction data, highlighting the need for strong legal frameworks to protect individuals' privacy rights.

Twenty-nine percent of respondents indicated 'Maybe', demonstrating the perception that governments and corporations could exploit individuals' purchase histories for monitoring or intimidation purposes. One respondent asserted their concerns by referencing the Canadian Government v. Truckers case, which likely alludes to events where digital financial records were allegedly used

to target and penalize protest participants, illustrating a real-world example of how purchase history can be used for surveillance and control purposes. This example can serve as a catalyst for discussions about government overreach and the balance between security measures and individual freedoms in a cashless society. Survey responses also indicate scepticism about the feasibility of maintaining anonymity in a cashless society, with only a minority (7%) expressing total distrust of the potential for misuse of purchase history. This may suggest that the majority of respondents recognise the inherent risks associated with digital transactions and the collection of personal data by governments and corporations.

The findings underscore the importance of legal and regulatory mechanisms to protect individual privacy rights and to ensure transparency and accountability in the use of transaction data by government and corporate entities. In addition, concerns about surveillance and intimidation could have implications for consumer behaviour and trust in digital payment systems, potentially impacting economic activities in a cashless society.

Question 6: *According to the Chainalysis 2022 Crypto Crime Report, money laundering accounted for just 0.15% of all cryptocurrency transaction volume in 2021. Law enforcement can use software to track and trace bitcoin transactions and give them the leads they need to follow the money trail. Do you believe replacing cash with cryptocurrencies could help reduce money laundering?*

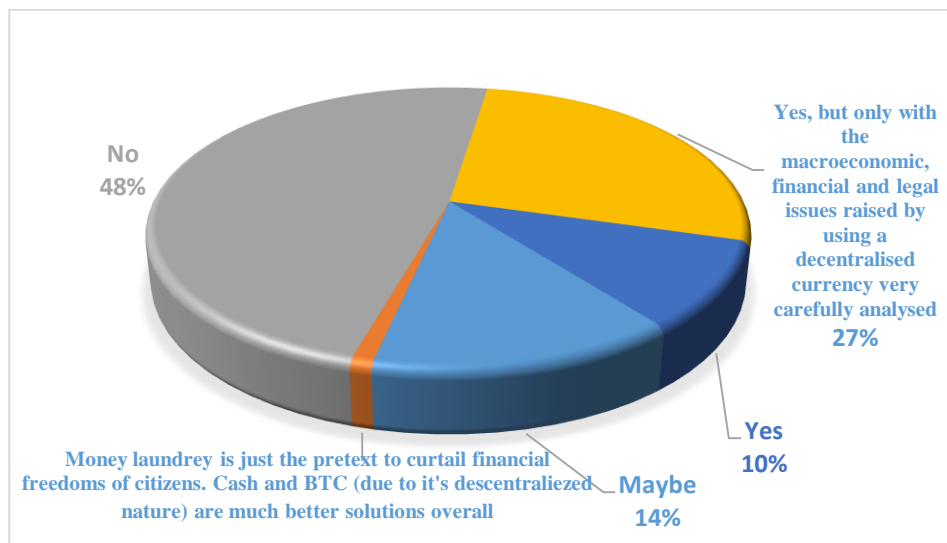


Figure 6. *Answers to Question 6: Do you think replacing cash with cryptocurrencies could help reduce money laundering?*

The survey results present a nuanced perspective on whether

cryptocurrencies, especially Bitcoin, can effectively reduce money laundering compared to traditional cash transactions (Figure 6).

The majority of respondents (48%) expressed scepticism that these cryptocurrencies will not effectively curb money laundering. This view likely stems from recognition of the challenges cryptocurrencies pose, such as their inherent anonymity and decentralised nature, which can facilitate illicit activities despite the transparency offered by blockchain technology. A significant proportion of respondents (27%) indicated that cryptocurrencies could indeed reduce money laundering, but stressed the need for careful analysis of macro-economic, financial and legal aspects before implementation. This perspective underlines the importance of comprehensive regulatory frameworks to address the unique challenges posed by decentralised currencies and to mitigate potential risks.

A smaller proportion of respondents (14%) answered 'Maybe', reflecting a recognition of the complexity of this issue. They probably recognise both the potential benefits of cryptocurrencies in terms of traceability and concerns about their possible misuse, highlighting the need for further examination and possibly regulation. Confidence in the potential of cryptocurrencies to reduce money laundering was at 10%. While this view acknowledges the challenges and complexities involved, it suggests optimism about the effectiveness of cryptocurrencies in increasing transparency and traceability, which could mitigate illicit financial activities. Only one respondent (1%) expressed the view that money laundering concerns serve as a pretext to limit citizens' financial freedoms. They argued that both cash and Bitcoin, due to their decentralised nature, offer good global solutions.

Overall, these results illustrate the diverse perspectives within the community on the role of cryptocurrencies in combating money laundering. They highlight the need for careful analysis of regulatory frameworks, economic stability and law enforcement mechanisms to effectively address the complexities of using decentralised currencies.

Question 7: *According to IMF, Central Bank Digital Currency (CBDC) might offer more resilience, more safety, greater availability, and lower costs than private forms of digital money. What do you think about CBDCs as cash alternative?*

One respondent expresses scepticism about the usefulness of CBDCs, while acknowledging their potential benefits, warning of possible negative consequences. This view suggests caution about unforeseen implications and highlights the need to consider the wider impact on society. Another respondent highlights the limited applications of virtual currency and its susceptibility to manipulation and speculation. This view raises doubts about the stability and reliability of CBDCs, suggesting that they may not be as resilient or secure as claimed. One respondent expresses fears that CBDC could lead to a centralised and controlled society, drawing parallels with Bolshevik regimes. This view

highlights concerns about government control and surveillance, highlighting the potential erosion of individual freedoms and privacy. A total of 27 respondents support CBDC as an alternative to cash, citing reasons such as better financial inclusion, efficient welfare payments and simplified international transactions.

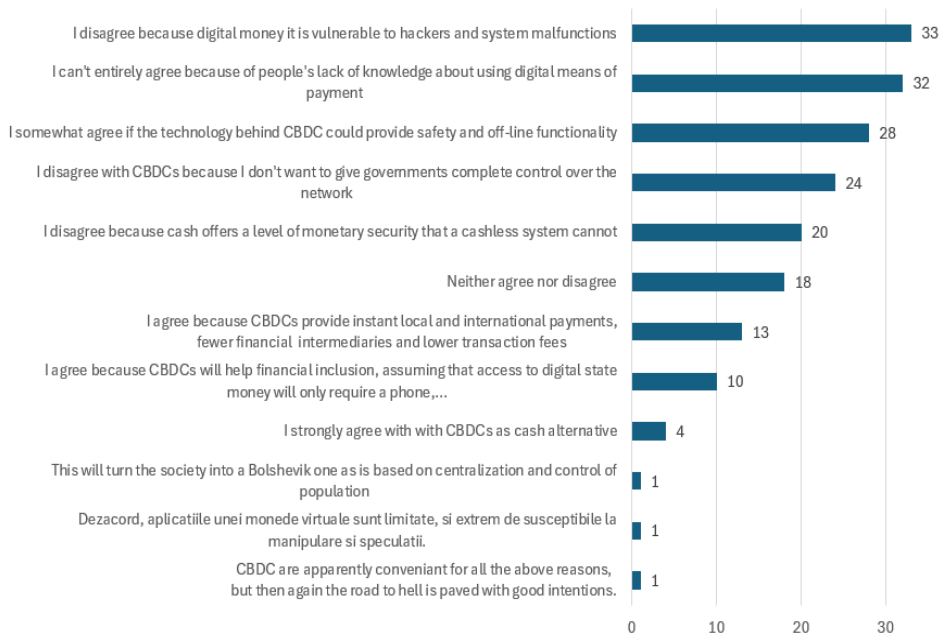


Figure 7. Answers to Question 7: What do you think of CBDC as an alternative to cash?

This perspective highlights the perceived benefits in terms of promoting financial accessibility, reducing costs and increasing efficiency. Variants against CBDCs were identified in 77 responses, with respondents offering as arguments that these digital currencies are vulnerable to hackers and system errors (33), that they do not want to give governments total control over the system (24), that cash offers a level of monetary security that a cashless society would not (20). Other respondents expressed more nuanced positions, neither agreeing nor disagreeing with CBDCs. Their concerns ranged from the need for security and offline functionality to issues of technological literacy and vulnerability to cyber threats and system failures.

These responses reflect the varied perspectives within the civilian community on the adoption of CBDCs as an alternative to cash. While some respondents emphasize the potential benefits, others express concerns about centralization, privacy, security, and social implications. Thorough analysis and consideration of these factors are essential before CBDCs are widely adopted.

Question 8: Do you believe replacing cash with CBDCs could help reduce money laundering crime?

Interpretation of the results while taking into account the age groups of the respondents (Figure 8) indicates varying levels of scepticism, cautious optimism and outright opposition to the idea of replacing cash with central bank digital currencies (CBDCs) as a means of reducing money laundering.

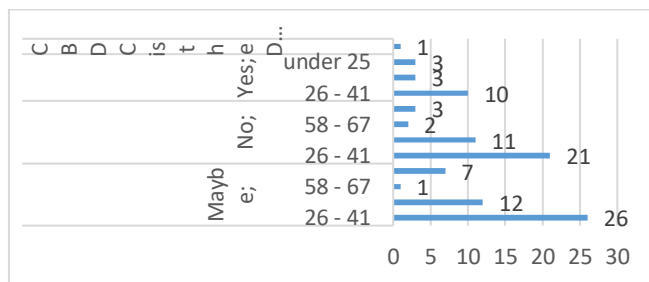


Figure 8. Answers to Question 8: could replace cash with CBDCs help reduce money laundering offences?

Across all age groups, there is a predominant sense of uncertainty, with 46 respondents expressing a ‘maybe’ position. This indicates a lack of confidence in the ability of CBDCs to effectively curb money laundering. Respondents under the age of 25 showed a higher degree of uncertainty (7 ‘Maybe’ responses and 3 ‘No’ responses) compared to those in other age groups. This could be attributed to a combination of factors, such as less familiarity with financial systems, a more cautious approach to new technologies or a lack of trust in centralised systems. The 26–41 age group showed a mix of responses, with a significant proportion leaning towards uncertainty (26 ‘Maybe’ responses and 21 ‘No’ responses), indicating a more cautious attitude towards adopting CBDCs to combat money laundering. 42 - 57 and 58–67: Relatively fewer respondents in these age groups responded, with the majority expressing uncertainty or opposition to the idea of replacing cash with CBDCs to reduce money laundering. A substantial number of respondents (37) categorically rejected the idea that CBDCs could help reduce money laundering. This suggests scepticism or concern about the effectiveness of CBDCs in tackling financial crime. A smaller number of respondents (16) expressed support for this idea, including 10 in the 26–41 age group, 3 in the under 25 age group and 3 in the 42–57 age group. This indicates a minority view in favour of CBDCs as an anti-money laundering tools. One respondent expressed strong opposition to CBDCs, characterising them as a threat to individual freedoms under the guise of protection. This view highlights concerns about potential abuses of power and loss of privacy associated with CBDCs.

Overall, the results suggest a prevailing sense of uncertainty about the effectiveness of CBDCs in reducing money laundering. Age-based analysis reveals nuanced perspectives, with younger respondents showing more uncertainty and older respondents showing varying levels of scepticism or opposition.

Question 9: *Do you believe that banks, payment institutions or other commercial entities should be involved in issuing a digital currency?*

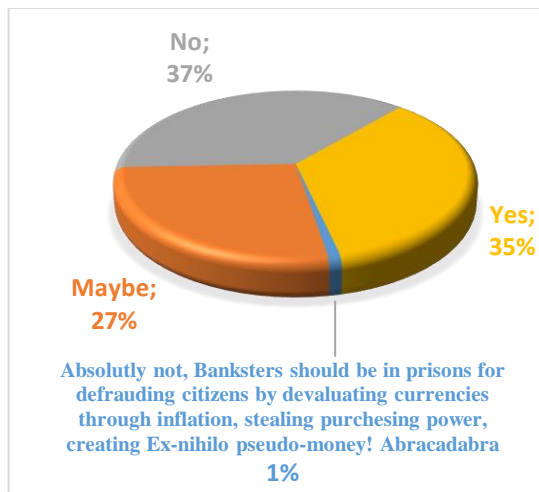


Figure 9. *Answers to Question 9: should banks, payment institutions or other commercial entities be involved in issuing a digital currency?*

Interpreting these results (Figure 9) reveals a wide range of views on the involvement of banks, payment institutions or other commercial entities in issuing digital coins. One respondent strongly opposes this idea, expressing disbelief and suggesting that banks should face legal consequences for perceived fraudulent practices linked to currency devaluation and inflation. This view reflects a deep-seated scepticism of traditional financial institutions and their role in monetary affairs.

A large group of respondents (27) express uncertainty ('Maybe') about the possibility of banks and other commercial entities being involved in issuing digital currencies. This uncertainty may stem from concerns about the potential consequences and the need for further analysis of the legal and economic implications. A significant proportion of respondents (37) categorically reject the idea, indicating a strong aversion to banks, payment institutions or other commercial entities playing a role in issuing digital money. This opposition may be motivated by concerns about centralisation, profit motives and potential abuse of power. Another group of respondents (35) express support for the involvement of banks, payment institutions or other commercial entities in the issuance of digital currencies. This view is likely to emphasise the expertise and infrastructure that these entities possess, which could facilitate the adoption and management of digital currencies.

Overall, these results highlight the complex relationship between traditional financial institutions and the emerging digital currency landscape. While some respondents advocate for the involvement of banks and commercial

entities according to their capabilities and resources, others express deep distrust and opposition, reflecting broader concerns about financial systems and their impact on society. These diverse perspectives highlight the need for careful consideration of regulatory frameworks, ethical principles and economic implications when assessing the role of banks and commercial entities in issuing digital currencies.

Question 10: *A CBDC is programmable, meaning that the government could put digital restriction rules to the point that the currency can be programmed to expire. Do you think this might threaten to save money, the consumers being forced to use it by a specific date?*

Based on the results provided, there appears to be a wide range of views on the potential impact of programmable CBDCs (central bank digital currencies) on money saving and consumer freedom (Figure 10):

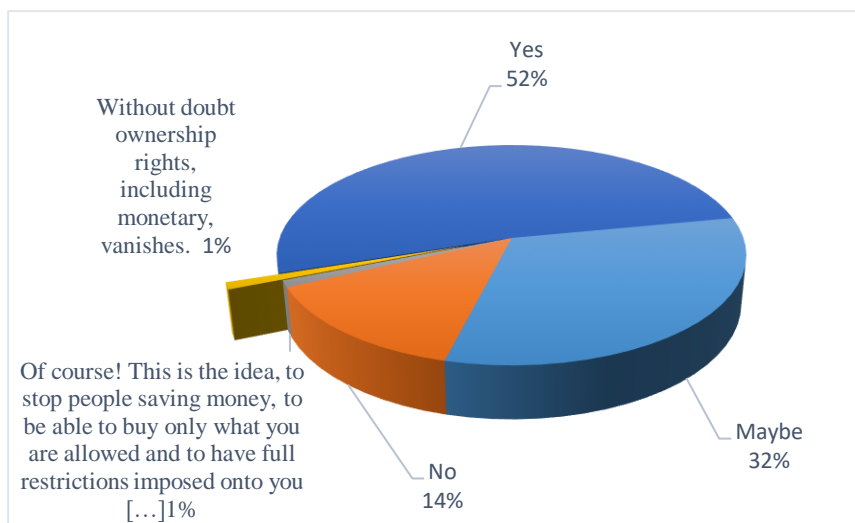


Figure 10. *Answers to Question 10: CBDC perceived threats to consumer saving habits and freedom.*

Only 14% of respondents strongly believe that programmable CBDCs will not pose a threat to saving money or force consumers to use them within a specified timeframe. It is worth noting that all respondents who do not perceive CBDCs as a threat are located in Romania, covering different areas of expertise and age groups. Of the remaining 86 respondents, 32 acknowledge that there could be a threat to saving money but are not fully convinced, and 52 strongly agree that programmable CBDCs could threaten to save money and force consumers to use them by a certain date, with a consistent theme of apprehension, particularly among those in financial services, law, and science and technology. In addition to the 52 respondents who answered ‘Yes’ to the question about the threat that CBDCs pose to saving money, two other respondents offered more

explicit perspectives on this issue. These individuals chose not to simply select the ‘Yes’ option, but provided their own detailed responses:

One respondent said: *‘Of course! That’s the idea, to stop people from saving money, to be able to buy only what you are allowed to buy and have all the restrictions imposed on you if you follow the rules [...]’* strongly indicates the belief that CBDCs are designed with the specific intention of reducing saving habits and exercising control over consumer behaviour. The other respondent expressed concern about the erosion of property rights, including money rights, in the context of programmable CBDCs. This respondent expressed this concern by stating, *‘Without a doubt, property rights, including monetary rights, are disappearing,’* underscoring broader concerns about the implications of programmable CBDCs on fundamental property rights and financial autonomy.

It is worth noting that of the 8 respondents living outside Romania who participated in the research, all of them expressed the view that they identified threats to their freedoms from CBDCs, answering this question with ‘Yes’ (3), ‘Of course’ (1), ‘No doubt’ (1) or ‘Maybe’ (3).

Question 11: *Do you think that CBDC, a centrally controlled digital currency, might mean the end of financial freedom?*

Responses to the question on perceptions of the potential ramifications of central bank digital currency (CBDC) on financial freedom, particularly in the context of centralised control of CBDC, revealed the following results:

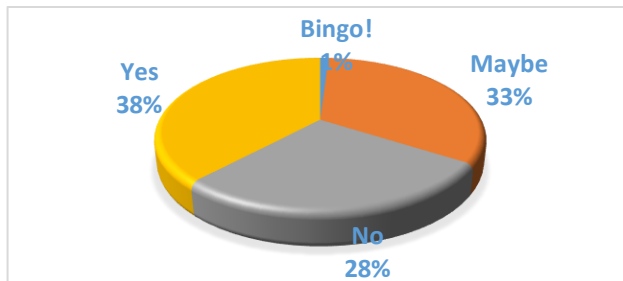


Figure 11. *Answers to Question 11: Could CBDC, a centrally controlled digital currency, mean the end of financial freedom?*

Of the survey participants, one respondent indicated unequivocal agreement (‘Bingo!’) strongly arguing that implementation of the CBDC could mean an end to financial freedom. In contrast, a considerable proportion (33%) expressed ambivalence (‘Maybe’), reflecting uncertainty or acknowledging nuanced considerations on the issue. A smaller contingent offered a divergent view (‘No’), with twenty-eight respondents expressing disagreement with the idea that implementing the CBDC would mean ending financial freedoms. In contrast, a majority of 38% said it was possible (‘Yes’) that the introduction of CBDCs could undermine financial freedom, suggesting concerns about the centralised control inherent in these digital currency systems and its potential

impact on individual financial autonomy.

This diversity of responses highlights the complexity and multidimensionality of views on the intersection between CBDCs and financial freedom. This highlights the need for more nuanced exploration and analysis to understand the factors underlying attitudes towards the potential implications of CBDC adoption on financial freedoms.

Question 12: *Do you think Cryptocurrency (a decentralised tool of people) is an unwanted competitor for the world governments?*

The responses to this question (Figure 12) show that of the 100 respondents, 37 see cryptocurrencies as a challenge to government authority, advocating decentralisation of power and financial solutions. In contrast, 30% of respondents do not see cryptocurrencies as an unwelcome competitor to world governments. This group may perceive cryptocurrencies differently, seeing them as complementary to existing systems rather than a direct competitor. The same 30% of respondents were in favour of the possibility ('Maybe') that decentralised cryptocurrencies pose a threat to world governments. Their uncertainty may stem from a variety of factors, including insufficient knowledge about the implications of cryptocurrencies or conflicting opinions about their potential impact. Three additional perspectives emerged from the study on this question. One respondent characterized cryptocurrency as similar to a Ponzi scheme. Another respondent highlighted the importance of cryptocurrency for development, particularly in terms of its role in paving the way for central bank digital currencies (CBDCs) and advancing blockchain technology, believing that all current users are developing the blockchain system for free instead of banks spending trillions of dollars on research and development. In addition, one respondent expressed ignorance and refrained from providing a definitive answer.

These responses reflect a range of perspectives on the relationship between cryptocurrencies and government authority. Most respondents see cryptocurrency as a challenge to centralised power structures, while others do not perceive it as a significant threat. There is, however, a notable share of respondents who see a possible impact of cryptocurrencies on government authority.

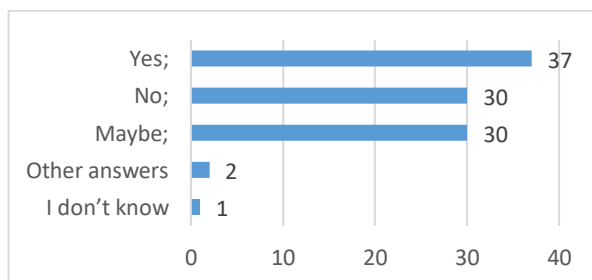


Figure 12. *Answers to question 12: Is cryptocurrency (a decentralised tool of the people) an unwanted competitor for the governments of the world?*

Overall, the responses from different areas of expertise highlight the multidimensional nature of the debate on the relationship of cryptocurrencies to government authority. Respondents from the financial services fieldIt appears that opinions vary significantly by individuals’ professional background, suggesting that perspectives on this issue are shaped by factors such as industry norms, regulatory considerations, and technological understanding.

Question 13: Cryptocurrency or CBDC as an alternative to cash?

The survey responses to the respondents preferred alternative to cash (Figure 13) show a variety of opinions, with the overall balance weighing in favour of digital currencies issued by central banks (CBDCs):

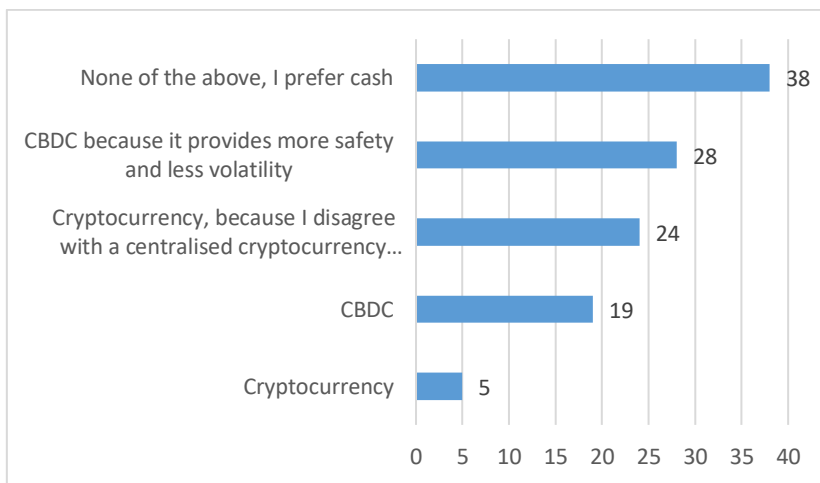


Figure 13. Answers to question 13: Cryptocurrency or CBDC as an alternative to cash?

A substantial proportion of respondents, 47%, express a preference for CBDC. Of these, 28% cite perceived advantages of CBDCs, such as increased safety and reduced volatility compared to cryptocurrencies. This preference aligns with the emphasis on stability and regulatory oversight in monetary systems, suggesting a recognition of the importance of strong governance frameworks in ensuring the integrity of digital currencies. Interestingly, a notable subset of respondents, representing 29%, support cryptocurrencies as a replacement for cash due to concerns about the potential for centralisation of CBDCs. Within this subgroup, 24% perceive centralized cryptocurrency (CBDCs) as a threat to decentralization and individual autonomy, fearing a transfer of power from people to world governments. This sentiment resonates with advocacy for inclusive economic institutions that empower citizens and distribute power more equitably. Of note, of the 100 respondents surveyed, 38% express a clear preference for traditional cash over cryptocurrencies and CBDCs. This preference suggests a desire for familiarity and trust in existing monetary

systems. It may indicate a cautious approach to innovation in monetary policy, highlighting the importance of stability and public confidence in the financial system.

Overall, the results reveal a nuanced landscape of preferences and concerns about the future of monetary systems. While some respondents advocate technological innovations such as CBDCs, others remain cautious, stressing the need to balance innovation with stability and inclusiveness in monetary policy. This nuanced perspective is critical for policymakers as they navigate the complex terrain of digital finance and strive to design effective regulatory frameworks that promote financial stability, inclusion and trust.

Question 14: *Taking into account that COVID-19 accelerated the shift of both public and private sectors to digital payments and digital finance, how do you see the future of money in ten years? (multiple choice)*

According to the 98 people who agreed to answer this question, the future of money is subject to a multifaceted dynamic, influenced by both technological advances and socio-political considerations (Figure 14).

A significant majority, representing 52% of respondents, imagine a future in which both centralised and decentralised currencies coexist in a virtual realm. This view reflects a recognition of the evolving landscape of digital finance and the emergence of innovative forms of currency. Of the 100 respondents, 28% foresee a future dominated by CBDCs. This outlook underscores the growing influence of central banks in shaping the digital financial ecosystem, with CBDCs poised to play a central role in facilitating transactions and monetary policy. Despite the trend towards digitalisation accelerated by COVID-19, 27% of respondents anticipate that cash will remain a significant component of the monetary landscape over the next decade. Recognition that cash will continue to be a significant component of the monetary landscape suggests an understanding of its enduring relevance and usefulness.

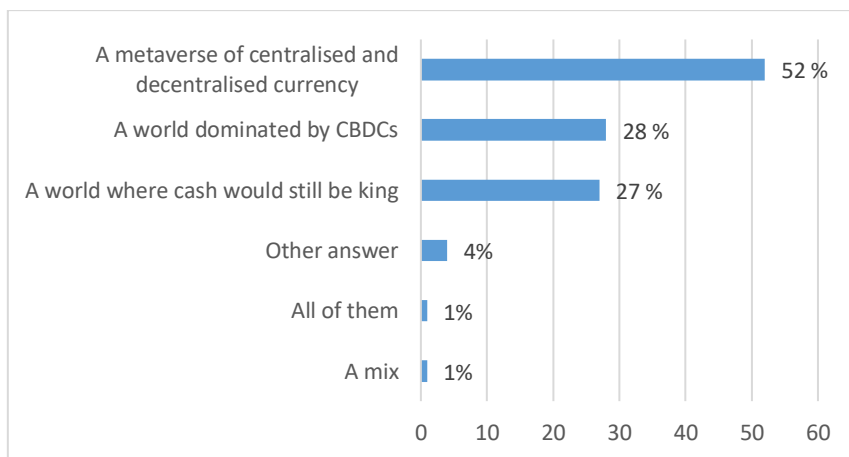


Figure 14. *Answers to Question 14: the future of money in ten years' time?*

One respondent emphasises a mixed future, indicating the complexity of the evolving monetary system. This perspective recognises the likelihood of a variety of monetary instruments co-existing in the future. Several respondents offer nuanced reflections on the interplay between technology, governance and social values. One respondent, for example, expresses scepticism about the potential for the adoption of a fully decentralised currency, citing the persistence of bureaucratic and financial interests. Another respondent highlights the role of COVID-19 in accelerating the adoption of technologies in various spheres of life, including finance. This perspective highlights the transformative impact of the pandemic on digitisation trends.

In sum, these responses reflect a rich range of perspectives on the future of money, shaped by technological innovation, regulatory dynamics and social values. Both economic and legal practitioners may find these insights valuable in navigating the complex legal and regulatory challenges inherent in the evolving digital financial landscape.

5. Conclusions

The survey results show that the majority of respondents believe that criminal organisations would adapt to limiting cash by using offshore banking, cryptocurrencies or other digital methods, suggesting that limiting cash may not fully deter money laundering. Legal and policy professionals have different views, with some believing that cash restriction could bring potential benefits, while others remain sceptical because of the adaptability of criminals. There is uncertainty about the effectiveness of traceable currencies in deterring tax evasion, with 41% of respondents expressing doubts. Scepticism about the ability of traceable currencies to deter tax evasion (34%) highlights the complexity of tackling financial crime through technology alone. However, legal and policy professionals express confidence in the potential of traceable currencies to deter tax evasion. Concerns about theft associated with large amounts of cash are prevalent among respondents, highlighting the multifaceted considerations influencing the use of cash. Overall, there is uncertainty about the effectiveness of central bank digital currencies (CBDCs) in reducing money laundering, with age-based analysis revealing nuanced perspectives. Despite some scepticism, a substantial proportion of respondents prefer CBDCs, citing perceived advantages such as increased security and reduced volatility compared to cryptocurrencies.

The recognition that both centralised and decentralised currencies will co-exist within a virtual realm highlights the importance of embracing innovation and adapting regulatory frameworks to accommodate digital currencies and emerging financial technologies. Policymakers need to consider the implications of the coexistence of centralised and decentralised currencies for regulatory frameworks governing digital finance. Policymakers may need to strike a balance between encouraging innovation and providing regulatory oversight to mitigate

the risks associated with decentralised currencies, such as potential vulnerabilities to fraud, market manipulation and illicit activities. This recognition is crucial for policy-makers as it underlines the need to maintain support for cash infrastructure and accessibility, especially in contexts where digital payment methods may not be widely adopted or accessible. Anticipating the continued importance of cash highlights its resilience as a form of payment. This resilience may stem from factors such as trust, familiarity and the ability to ensure financial privacy and anonymity, which are valued by certain individuals and communities. Policy-makers need to consider the implications of cash persistence for financial inclusion and affordability. While digital payment methods offer convenience and efficiency, policymakers need to ensure that initiatives to promote digital financial inclusion does not inadvertently exclude individuals or communities that rely on cash. This may involve implementing policies that safeguard the availability and acceptance of cash, particularly in rural or underserved areas where digital infrastructure may be lacking. Recognising the enduring value of cash also highlights the importance of balancing innovation in digital payment technologies with maintaining stability and inclusiveness in the monetary system. Policymakers must navigate the tension between promoting digital financial innovation and maintaining the resilience and accessibility of traditional payment methods.

Bibliography

1. Androulaki, Elli, Ghassan Karame, Marc Roeschlin, Tobias Scherer, and Srđjan Ćapkun. *Evaluating User Privacy in Bitcoin*. In Lecture Notes in Computer Science, 34–51, 2013. https://doi.org/10.1007/978-3-642-39884-1_4.
2. Ardizzi, Guerino, Pierpaolo De Franceschis, and Michele Giammatteo. *Cash Payment Anomalies and Money Laundering: An Econometric Analysis of Italian Municipalities*. *International Review of Law and Economics*, no. 56 © (2018): 105–121. Accessed March 4, 2024. <https://doi.org/10.1016/j.irl.2018.08.001>.
3. Butler, Simon. *Criminal Use of Cryptocurrencies: A Great New Threat or Is Cash Still King?*, *Journal of Cyber Policy* 4, no. 3 (2019): 326–345. Accessed June 4, 2022. <https://doi.org/10.1080/23738871.2019.1680720>.
4. Căpățină, Cristina & Raluca Ghețu. *Investigating Cash Replacement as a Means of Fighting Money Laundering: The Case of Digital Currency and Its Economic Impact*. *Proceedings of the 39th International Business Information Management Association (IBIMA) (2022)*: 3496–3506. Accessed March 4, 2024.
5. Centre for International Governance Innovation. *CBDC Governance: Programmability, Privacy and Policies*. Prod. Digital Policy Hub – Working Paper (2024). Accessed March 15, 2024. <https://www.cigionline.org/static/documents/DPH-paper-Freiman.pdf>.
6. Chainalysis. *The Chainalysis 2024 Crypto Crime Report*. (2024). Accessed March 9, 2024. <https://go.chainalysis.com/crypto-crime-2024.html>.
7. Committee on Payments and Market Infrastructures and Markets Committee, Bank for International Settlements. *Central Bank Digital Currencies*. (2018): 7.

- Accessed March 12, 2024. <https://www.bis.org/cpmi/publ/d174.pdf>.
8. Georgieva, Kristalina. *The Future of Money: Gearing up for Central Bank Digital Currency*. www.imf.org. International Monetary Fund, February 9, 2022. <https://www.imf.org/en/News/Articles/2022/02/09/sp020922-the-future-of-money-gearing-up-for-central-bank-digital-currency>.
 9. Gobena, Messay Asgedom & Daniel Gebreegziabher Kebede. *Cash Economy, Criminality and Cash Regulation in Ethiopia*. Journal of Money Laundering Control 25, no. 3 (2021): 645–655. Accessed March 11, 2024. <https://doi.org/10.1108/JMLC-06-2021-0065>.
 10. Riccardi, Michele & Michael Levi. 2018. *Cash, Crime and Anti-Money Laundering*. In: King C., Walker, C., Gurulé, J. (Eds) The Palgrave Handbook of Criminal and Terrorism Financing Law, Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-319-64498-1_7.
 11. Ron, Dorit & Adi Shamir. 2013. *Quantitative Analysis of the Full Bitcoin Transaction Graph*. In: Sadeghi, AR. (Ed.) *Financial Cryptography and Data Security*. FC 2013. Lecture Notes in Computer Science. 7859th ed. Berlin, Heidelberg: Springer: 6–24. https://doi.org/10.1007/978-3-642-39884-1_2.
 12. Schneider, Friedrich. *Restricting or Abolishing Cash: An Effective Instrument for Fighting the Shadow Economy, Crime and Terrorism?* Conference Paper at International Cash Conference 2017 – War on Cash: Is There a Future for Cash? 25 - 27 April 2017, Island of Mainau, Germany, April 2017.
 13. US Department of Justice, National Drug Intelligence Centre. *Money Laundering and Digital Currencies*. www.justice.gov. US Department of Justice, June 3, 2008. <https://www.justice.gov/archive/ndic/pubs28/28675/28675p.pdf>.
 14. Wright, Richard, Volkan Topalli, Chandler Mccellan & Erdal Tekin. *Less Cash, Less Crime: Evidence from the Electronic Benefit Transfer Program*. The Journal of Law and Economics, 60, no. 2 (2017): 361–383. Accessed March 15, 2024. <https://doi.org/10.1086/693745>.

**LEGAL STRATEGIES FOR TECHNOLOGICAL
INNOVATION**

Study on Digital Transformation and Algorithmic Law

Professor **Carmen Silvia PARASCHIV**¹

Abstract

The article studies the interaction between digital transformation and the legal field, analyzing the impact of digital technologies on legislation and legal practice. After outlining the basics of digital transformation, it examines how technological evolution affects the rule of law and the legal implications of digital transformation, with a focus on data protection and privacy in the digital age. Emerging legal tools such as smart contracts and blockchain technology present challenges and opportunities. Access to justice in the digital age is analyzed, noting the influence of technology on legal processes and online dispute resolution platforms. The paper also addresses the impact of digital transformation on legal education and the ethical issues associated with the use of technology in legal practice. In conclusion, the paper emphasizes the importance of adapting the legal system and educational practices to the changes generated by the digital transformation.

Keywords: digital transformation, blockchain, emerging legal instruments, algorithmic law.

JEL Classification: K24, K38

DOI: <https://doi.org/10.62768/ADJURIS/2024/1/06>

Please cite this article as:

Paraschiv, Carmen Silvia, „Study on Digital Transformation and Algorithmic Law”, in Pajuste, Tiina, Heliona Bellani (Miço) & Sejla Maslo Cerkcic (eds.), *Legal Perspectives in the Modern Era of Technological Transformations*, ADJURIS – International Academic Publisher, Bucharest, Paris, Calgary, 2024, p. 104-114.

1. Introduction. Digital transformation and the law

Digital transformation represents the adoption of digital technologies in all areas of society and the economy, including law. Digital transformation in the legal field involves the use of information technologies to streamline and improve legal processes, the provision of legal services and access to justice. The digital transformation of the legal field materializes through:

- the use of AI and automation to process legal documents, to analyze jurisprudence and to assist in the drafting of contracts;²

¹ Carmen Silvia Paraschiv - Faculty of Law, „Titu Maiorescu” University of Bucharest, Romania, paraschivcrmn@yahoo.com.

² Liane Colonna, Stanley Greenstein, *Law in the Era of Artificial Intelligence*, *Nordic Yearbook of*

- moving from paper documents to electronic documents and using document management platforms to efficiently store, organize and access legal information;
- development of online platforms that offer legal services, facilitating access to legal services and legal assistance;
- increasing the importance of cyber security in the legal field, given the large amount of sensitive and confidential information;
- the use of blockchain technology to increase the security, transparency and verifiability of legal aspects such as transactions and intellectual property;³
- the development of online justice systems (e-justice) to facilitate access to the courts and to make judicial processes more efficient;⁴
- improving data protection practices and complying with privacy regulations such as the General Data Protection Regulation (GDPR);
- adapting the legal curriculum to include notions of technology and digital skills necessary for modern legal practice.

Digital transformation in the field of law brings significant benefits, such as increased efficiency, reduced costs and improved access to justice, but is accompanied by challenges related to data security, privacy protection and the adaptation of legal professionals to new technologies.

1.1. The relationship between digital technology and individual autonomy

Digital technology provides more control over decisions in various fields such as health, finance and education. With the implementation of digital technology, the amount of personal data collected and stored also increases, with requirements to protect privacy.

At the same time, digital technology personalizes services according to individual preferences. Personalized recommendations for online shopping contribute to increasing autonomy in making consumer decisions. On the other hand, excessive dependence on technology brings risks regarding autonomy. People become vulnerable to manipulation or lose essential skills due to over-automation.

Guaranteeing digital rights, such as freedom of expression online, is essential to maintaining individual autonomy in the digital age. Appropriate legislation and regulations must protect these rights. Certain digital technologies such as monitoring and surveillance systems raise concerns about invasion of privacy

Law and Informatics 2020–2021, <https://irilaw.org/wp-content/uploads/2022/02/law-in-the-era-of-artificial-intelligence.pdf>, p. 6.

³ Primavera De Filippi, Aaron Wright, *Blockchain and the Law: The Rule of Code*, Harvard University Press, 2018, p. 74.

⁴ Richard Susskind, Daniel Susskind, *The Future of the Professions: How Technology Will Transform the Work of Human Experts*, Oxford University Press, 2016, p. 112.

and loss of individual autonomy.⁵

Regulations on the use of these technologies are essential to balance the benefits and risks.

In essence, digital technology contributes to increasing individual autonomy, but it is important to strike a balance between the benefits brought by technology and the protection of fundamental values such as privacy, freedom and human dignity.

1.2. The relationship between digital technology and protection against wrongful injury

Digital technologies such as surveillance cameras, mobile phones and online platforms can be used to monitor abusive behavior and report incidents. This helps prevent abuses and bring those responsible to justice. Blockchain technology is used to create secure and transparent systems for registering and verifying individual rights. This can provide greater protection against infringements and unfair manipulations. Digital technologies facilitate access to online legal services, providing affordable and convenient legal support for those in need of protection against wrongful injury. AI-based algorithms analyze data sets to detect and highlight patterns of discrimination and injustice in various fields, including the legal system, enabling preventive interventions.

1.3. The relationship between digital technology and the fair resolution of disputes

Digital technology plays a significant role in improving the dispute resolution process and promoting a fair approach. The relevant aspects of the relationship between digital technology and fair dispute resolution are:

- the existence of specialized digital platforms that facilitate online mediation of disputes. They connect the involved parties and mediators in the virtual environment, for conflict resolution;
- digital technology implements online arbitration systems, where arbitrators analyze evidence and arguments in digital format and issue decisions without the need for physical meetings. There are also digital platforms that offer online dispute resolution services;
- blockchain technology facilitates the creation and implementation of smart contracts;⁶
- the use of predictive analytics and AI algorithms helps to anticipate potential disputes and identify effective solutions before they become major problems.

⁵ Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, PublicAffairs, 2019, p. 78.

⁶ Primavera De Filippi, Aaron Wright, *op. cit.*, p. 75.

2. Law and ePerson

The concept of "ePerson" is not a currently established term, but there are several possible interpretations or connections between the law and such an entity. EPerson refers to the "electronic person" or how digital technology and law interact regarding digital identity or digital entities. The law must address issues related to digital identity, including ways to protect personal data online, digital authentication and identity management in the digital space. The concept of "ePerson" is associated with persons who have a significant presence in the online environment and whose identities are managed and validated electronically. In the context of ePersons, data protection becomes crucial. Legislation such as GDPR (General Data Protection Regulation) sets out rights and obligations regarding the collection, storage and processing of personal data online. The law must regulate electronic contracts and how they are validated in the digital environment. This includes things like electronic signatures and online consent. In a digital world, digital entities, be the natural or legal persons, are involved in various activities. Legislation needs to address the legal responsibility of these entities for their actions online. The law must provide effective tools to combat cybercrime and protect ePersons from illegal online activities such as identity theft and cybercrime. Where ePersons interact with automated systems or decision-making algorithms, the law must regulate issues such as transparency, accountability and potential biases.

3. The law through the algorithm

The concept of "law by algorithm" or "algorithmic laws" refers to the use of algorithmic technology and AI to influence or even make decisions in the legal and legislative process. Algorithm law materializes in the use of algorithms and AI for decision-making within the legal system, such as sentencing, parole, or even judicial decisions, which involves analyzing data to identify patterns and trends in decision-making.⁷

One controversial area is the use of algorithms to predict potential criminal activity and direct police resources to specific areas or individuals. This raises questions about discrimination and ethics in law enforcement. AI is used to analyze legislative proposals, suggest changes or even draft laws. This speeds up the legislative process, but also raises questions about transparency and representativeness. Algorithms are used to analyze massive data sets in legal processes to support arguments and decisions. They are useful in identifying precedents or patterns in jurisprudence.⁸

⁷ Dana Remus, Frank S. Levy, *Can Robots Be Lawyers? Computers, Lawyers, and the Practice of Law*, (November 27, 2016). Available at SSRN: <https://ssrn.com/abstract=2701092> or <http://dx.doi.org/10.2139/ssrn.2701092>.

⁸ Michael A. Livermore, Daniel N. Rockmore, *Law as Data: Computation, Text, and the Future of*

Technology is also used to automate repetitive legal processes, such as managing documents, researching case law or even drafting contracts.

There are concerns and criticisms associated with the concept of "law by algorithm". Algorithms reflect pre-existing biases in the data they are trained with, leading to discriminatory decisions. Algorithms are often complicated, which makes it difficult to understand how they make decisions. The use of algorithms in the legal process involves the collection and processing of massive amounts of data, which raises concerns about its privacy and security.

3.1. Digitization and customized solutions in law

Digitization in the field of law brings with it a number of opportunities for the implementation of customized solutions that improve legal services and access to justice. Digital technology automates the process of drafting legal documents, quickly generating contracts, legal documents or other documents tailored to the specific needs and circumstances of clients. There are online platforms that offer personalized legal advice, where users receive legal advice based on the information they provide. These digital solutions facilitate access to legal services for a large number of people. Digitization supports the process of mediation and conciliation, giving the parties involved the opportunity to participate in online mediation sessions and find customized solutions to resolve disputes. Lawyers and law offices benefit from digital solutions for the efficient management of legal cases. These systems provide personalized information about a case's status, deadlines and other relevant details. Using predictive analytics helps legal professionals anticipate client needs and provide personalized advice. Client profiling based on historical data helps provide legal solutions tailored to individual needs.

Digital technology is used to provide personalized legal training tailored to each individual's needs and level of knowledge. This includes online training mode and resources adapted to the specifics of each user.

Mobile app development provides quick access to personalized legal information, legislative news and other resources supports personalized legal education and legal awareness.

4. The "digital judge" and "digital instants"

The concept of "digital judge" and "digital courts" refers to the use of digital technology and artificial intelligence in the legal system to streamline and improve judicial processes. It includes the use of automated algorithms and systems for case management, evidence analysis and even judicial decision-making:

- analysis of evidence through algorithms - in simple or routine cases,

algorithms are used for rapid analysis of evidence, identification of precedents and providing recommendations for decisions;

- online conciliation platforms - digital technology facilitate the online mediation process, in which mediators and involved parties interact through digital platforms, helping to find quick and effective solutions;

- case management systems - technology is used to automate administrative processes within the courts, including document management, scheduling hearings and tracking deadlines;

- predictive analytics algorithms are used to predict the outcome of a case based on available information and judicial precedents;

- AI technology is used to extract and analyze information from jurisprudence and to provide judges with decision-making support;

- online platforms facilitate the arbitration process, offering the involved parties an efficient way to resolve disputes without resorting to traditional courts;

- in the context of digital courts, ensuring the security and confidentiality of data is crucial to maintain trust in the judicial system;

- the use of digital technology contributes to the democratization of access to justice, facilitating the participation and understanding of judicial processes for all citizens.⁹

5. Private providers of dispute resolution services

There are several private dispute resolution providers that offer online platforms and specialized services to help resolve disputes outside of traditional courts. These providers use digital technology and various approaches to facilitate the process of mediation, arbitration or negotiation between parties:

1. *Online Dispute Resolution (ODR) Platforms:*

- Modria (by Tyler Technologies)¹⁰ provides online dispute resolution solutions using ODR technologies to facilitate mediation and negotiation in various fields, including e-commerce, financial services and others.

- CyberSettle¹¹ specializes in insurance, CyberSettle provides an ODR platform for the effective resolution of insurance claims disputes.

2. *Online Arbitration:*

- the American Arbitration Association (AAA)¹² provides online arbitration services, including a digital platform for arbitration case management and dispute resolution.

⁹ Dana Remus, Frank S. Levy, *op. cit.*, p. 8 et seq.

¹⁰ <https://www.tylertech.com/products/online-dispute-resolution>, consulted on 1 March 2024.

¹¹ https://tracxn.com/d/companies/cybersettle/_K1zZahePHHGPFJmqXTPMTEJnFcaQqq-MglbHsIpYE, consulted on 1 March 2024.

¹² <https://www.adr.org/ContactUs>, consulted on 1 March 2024.

- JAMS¹³ also offers online arbitration services, allowing parties to resolve their disputes without going to court.

3. *Online Mediation:*

- Mediate.com¹⁴ is a platform that connects parties with online mediators and provides dispute resolution resources.

- Quarrel is an online mediation platform that addresses a wide range of cases, including conflicts within organizations.

4. *General Dispute Resolution Platforms:*

- FairClaims¹⁵ offers a digital platform that facilitates the online resolution of small disputes, including those related to rents, e-commerce and services.

- Rechtwijzer is a European platform that provides dispute resolution services for various types of cases, including divorce and neighbor disputes.

6. The algorithmic conciliator

The term "algorithmic conciliator" refers to the use of algorithms and technology to facilitate the process of conciliation or mediation between disputing parties. These algorithms can be used to help find efficient and fair solutions in conflict resolution.

Here are some specific characteristics of an "algorithmic conciliator":

- algorithms can analyze objective information and relevant data to assess the situation and suggest possible solutions. This analysis can provide a neutral perspective on the dispute;

- based on the data provided and the specific parameters, the algorithmic conciliator can make automatic recommendations regarding possible solutions or the direction in which the conciliation process could go;

- an algorithmic conciliator can provide transparency on how it makes decisions and can explain the reasoning behind its recommendations, which can contribute to the confidence of the parties involved in the conciliation process;

- algorithms can process information quickly and handle large volumes of data, which can lead to faster resolution of disputes compared to traditional mediation processes;

- algorithmic conciliators can be designed to adapt and learn from new information provided during the process, thus improving the ability to provide more accurate solutions as disputes evolve;

- it is essential that the platform or system using an algorithmic conciliator is built with strict security measures to protect the confidentiality of the information involved in the dispute.

¹³ <https://www.jamsadr.com/>, consulted on 1 March 2024.

¹⁴ <https://mediate.com/>, consulted on 1 March 2024.

¹⁵ <https://mediation.fairclaims.com/>, consulted on 1 March 2024.

7. The algorithmic mediator

The term "algorithmic mediator" refers to the use of algorithms and technology to facilitate the mediation process between disputing parties. Algorithmic mediation involves the use of algorithms to analyze information, suggest solutions, or facilitate communication between parties.

Thus, algorithms analyze objective information and data provided by parties to assess the situation and propose solutions. This analysis can help gain a neutral perspective on the dispute.

Based on available data and predefined settings, the algorithmic mediator provides automatic recommendations on possible solutions or the most appropriate steps to resolve the dispute.

An algorithmic mediator can facilitate communication between the parties, helping to maintain a balanced tone and encourage constructive dialogue.

They can process information quickly and handle large volumes of data, which can lead to faster resolution of disputes compared to traditional mediation processes.

Algorithmic mediators are designed to adapt and learn from new information provided throughout the process, improving the ability to provide more accurate solutions as the dispute evolves.

Protecting the privacy and security of information is crucial in algorithmic averaging, and therefore strict measures are required to prevent unauthorized access to data.

Despite the intervention of algorithms, human verification or intervention may be required in the mediation process to handle sensitive issues or to resolve conflicts that may require more complex approaches.

8. Responsibility for autonomous systems

Liability for autonomous systems, such as autonomous cars, robots, autonomous AI systems, and others, is a complex and debated issue in ethics, law, and technology.¹⁶ As these systems are capable of making decisions and acting independently, crucial questions arise as to who bears responsibility in the event of unintended consequences or accidents.¹⁷

In many jurisdictions, the primary responsibility falls on the developers and manufacturers of these systems. They are expected to implement security measures and ensure that their systems comply with applicable standards and regulations.¹⁸

¹⁶ Patrick Lin, Keith Abney, George A. Bekey, *Robot Ethics: The Ethical and Social Implications of Robotics*, MIT Press, 2012, p. 211 et seq.

¹⁷ Sheila Jasanoff, *The Ethics of Invention: Technology and the Human Future*, W. W. Norton & Company, 2016, p. 85 et seq.

¹⁸ Ryan Calo, A. Michael Froomkin, Ian Kerr, *Robot Law*, Edward Elgar, 2016, p. 315 et seq.

If an operator or user interacts with an autonomous system and there is possible human intervention, they may also be held liable under certain circumstances.

In some jurisdictions, specific regulations are being developed to define the legal responsibilities associated with autonomous systems. These regulations may impose safety, testing and liability insurance requirements.

In certain cases, it may be necessary to obtain specific insurance policies to cover possible damages caused by autonomous systems. This can help shift financial liability in the event of accidents.

Beyond the legal aspects, there is an ethical dimension to responsibility. Developers and operators are often encouraged to adopt ethical practices and prioritize safety and the common good in the development and use of autonomous systems.¹⁹

In some cases, government authorities are involved in defining the rules and accountability for autonomous systems, having a significant role in regulating and overseeing their use.

9. Conclusions

The conclusions can be summarized as follows:

a) the impact of digital transformation in the field of law:

- digital transformation makes legal processes more efficient, reduces costs and improves access to justice;
- AI, automation, blockchain and e-justice are reconfiguring traditional legal practices;
- vulnerabilities associated with data security, privacy protection and adaptation of professionals to new technologies.

b) the relationship between digital technology and individual autonomy:

- digital technology contributes to increasing individual autonomy, but excess dependence can bring risks and vulnerabilities;
- protecting digital rights, such as freedom of expression online, is essential for maintaining individual autonomy;
- appropriate regulations are needed to manage the use of technologies that may affect the autonomy and privacy of the individual.

c) the relationship between digital technology and protection against wrongful injury:

- digital technologies such as surveillance cameras and AI-based analytics help monitor and report abuse;

¹⁹ Melanie Mitchell, *Artificial Intelligence: A Guide for Thinking Humans*, Farrar, Straus and Giroux, 2019, p. 140 et seq.

- the use of blockchain technology and predictive analytics supports protection against discrimination and injustice;
- access to online legal services and dispute resolution solutions facilitates protection against unfair harm.

d) the relationship between digital technology and fair dispute resolution:

- digital platforms facilitate online mediation and arbitration, streamlining the dispute resolution process;
- digital technology, including predictive analytics and the use of blockchain, contributes to the anticipation and prevention of disputes;
- adapting technology to dispute resolution processes improves access to justice and the efficiency of judicial processes.

e) ePerson and the impact in the legal field:

- the concept of "ePerson" reveals the need for regulation regarding digital identity, data protection and legal responsibility in the online environment;
- protecting individual rights in the digital context, such as electronic signatures and online consent, becomes essential;
- legislation must take into account the responsibility of digital entities and address the challenges of cybercrime.

f) personalized solutions in law through digitization:

- digitization in law involves the implementation of customized solutions, such as the rapid generation of legal documents and online legal advice;
- client profiling and predictive analytics improve personalized legal services and anticipate client needs;
- personalized legal education and quick access to legal information through mobile apps supports legal awareness and understanding.

g) the digital judge and the digital courts:

- the use of digital technology in courts brings benefits such as rapid analysis of evidence, efficient case management and democratization of access to justice;
- data security and confidentiality are essential in the implementation of digital courts;
- the use of technology in online arbitration and mediation contributes to the quick and efficient resolution of disputes.

h) private dispute resolution service providers:

- online dispute resolution platforms offered by private providers, such as Modria, CyberSettle and others, bring efficient and specialized options for dispute resolution, and online arbitration and mediation offered by organizations such as AAA and JAMS support dispute resolution without involving traditional courts.

- specialized applications such as FairClaims and Rechtwijzer provide solutions for various types of cases and contribute to access to justice.

i) conciliator and algorithmic mediator:

- algorithmic conciliators and mediators can bring efficiency and objectivity to conciliation and mediation processes, and
- privacy protection and data security are essential in the implementation of these algorithms.
- the need for a balance between the intervention of algorithms and human intervention for the management of sensitive aspects and the resolution of complex conflicts.

j) recommendations for the future:

- the continuation of research and the development of technologies to support the digital transformation of legal systems.
- collaboration between legal professionals and technology experts to develop sustainable and ethical solutions.
- updating and adapting regulations and legislation to keep pace with technological developments and to ensure adequate protection of individual rights.
- continuing education for legal professionals and technology developers to improve mutual understanding and promote the responsible use of technology in law.

Bibliography

1. Calo, Ryan, A. Michael Froomkin & Ian Kerr, *Robot Law*, Edward Elgar, 2016.
2. Colonna, Liane & Stanley Greenstein, *Law in the Era of Artificial Intelligence, Nordic Yearbook of Law and Informatics 2020–2021*, <https://irilaw.org/wp-content/uploads/2022/02/law-in-the-era-of-artificial-intelligence.pdf>.
3. Filippi, Primavera De & Aaron Wright, *Blockchain and the Law: The Rule of Code*, Harvard University Press, 2018.
4. Jasanoff, Sheila, *The Ethics of Invention: Technology and the Human Future*, W. W. Norton & Company, 2016.
5. Lin, Patrick, Keith Abney & George A. Bekey, *Robot Ethics: The Ethical and Social Implications of Robotics*, MIT Press, 2012.
6. Livermore, Michael A. & Daniel N. Rockmore, *Law as Data: Computation, Text, and the Future of Legal Analysis*, SFI Press, 2019.
7. Mitchell, Melanie, *Artificial Intelligence: A Guide for Thinking Humans*, Farrar, Straus and Giroux, 2019.
8. Remus, Dana & Frank S. Levy, *Can Robots Be Lawyers? Computers, Lawyers, and the Practice of Law*, (November 27, 2016). Available at SSRN: <https://ssrn.com/abstract=2701092> or <http://dx.doi.org/10.2139/ssrn.2701092>.
9. Susskind, Richard & Daniel Susskind, *The Future of the Professions: How Technology Will Transform the Work of Human Experts*, Oxford University Press, 2016.
10. Zuboff, Shoshana, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, PublicAffairs, 2019.

Scenarios for the Future of the Legal Profession in the Age of Artificial Intelligence?

Professor **Verginia VEDINAȘ**¹
Lecturer **Ioan Laurențiu VEDINAȘ**²

Abstract

The present study aims to address, succinctly, aspects that concern the future. The changes that this period will bring to all professions represent a general concern. It is obvious, however, that the effects to be produced are not similar either as content, nor quantitatively. If they are professions 'prone' to be replaced, in completeness, computers, equally are professions whose content will be modified, without; however, they can be fully transferred from human to computers. Among these, we appreciate that there are also legal professions. Some of the ways in which they are exercised, it will be possible to move into the 'competence' of the computer, but man cannot ever disappear, entirely, from their exercise.

Keywords: artificial intelligence, legal professions, digitization, evolution, future, computers, professional competence, categories, reports.

JEL Classification: K10, K24

DOI: <https://doi.org/10.62768/ADJURIS/2024/1/07>

Please cite this article as:

Vedinaș, Verginia & Ioan Laurențiu Vedinaș, „Scenarios for the Future of the Legal Profession in the Age of Artificial Intelligence?”, in Pajuste, Tiina, Heliona Bellani (Miço) & Sejla Maslo Cerkić (eds.), *Legal Perspectives in the Modern Era of Technological Transformations*, ADJURIS – International Academic Publisher, Bucharest, Paris, Calgary, 2024, p. 115-125.

1. Introduction

The issue of the impact of artificial intelligence on law and the legal professions has always been a concern of ours. We are referring to those exercising judicial or executive power, but also to the liberal professions, such as lawyers, notaries and bailiffs³.

¹ Verginia Vedinaș - Corresponding member of the Academy of Romanian Scientists; President of the Institute of Administrative Sciences 'Paul Negulescu', Romania, prof.verginia.vedinas@gmail.com.

² Ioan Laurențiu Vedinaș - 'Vasile Goldiș' Western University of Arad, Romania, ioan.vedinas@gmail.com

³ See Oleksandr Shevchuk, Volodymyr Martynovskyi, Olena Volianska, Ihor Kompaniiets, Oleg Bululukov, *Problems of legal regulation of artificial intelligence in administrative judicial*

The fruit of our concerns has resulted in papers with a mixed title, in which, in addition to the academic component, there is also a metaphorical one, such as ‘from chemical pencil to computers’ or ‘from perceiver to computer programs’⁴.

Professionally, our destiny reverberates in the sphere of an essential public service to society, namely education in general and academic education in particular.

Over it lies an interest in public life in general and in administration in particular, but above all, like a comforting and protective cloak, never resting for the good of the country to which we belong⁵.

The world is not standing still, and technology is evolving at a dizzying pace. We have to cope with it both as individuals, in the privacy of our private selves, and in the professional environment in which we work.

2. The role of strategies

The Romanian State itself is concerned about its own development, the activity of its authorities and all the services through which the needs of its citizens are met, and this is the context in which the ‘national strategic framework in the field of artificial intelligence’ was developed, with financial support provided by the ‘Operational Programme for Administrative Capacity’, known by its abbreviated name of POCA.⁶

We would like to make a clarification, and we ask for your forgiveness if

procedure, Juridical Tribune - Tribuna Juridica, Volume 13, Issue 3, October 2023, pp. 346-426 and Oleksandr Shevchuk, Ihor Kompaniets, Olena Volianska, Oleksandra Shovkopljas, Vasył Baranchuk, *Electronic Administrative Judicial Procedure of Ukraine and the Right to Judicial Protection: Problems of Legal Regulation and Practical Issues*, Juridical Tribune - Review of Comparative and International Law, Volume, 14, no. 1, March 2024, p. 98-115.

⁴ See Verginia Vedinaș, *Odiseea funcției publice în România sau de la perceptor la programe pe calculator*, in Constantin Brătianu, Doina Banciu, Nicolae Dănilă (coord.), *Economia și societatea în era digitalizării*, Publishing House of the Romanian Academy of Scientists, Bucharest, 2023, p. 223-240 and Cătălin-Silviu Săraru, *Provocări contemporane în administrația publică și în dreptul administrativ* in Constantin Brătianu, Doina Banciu, Nicolae Dănilă (coord.), *op. cit.*, p. 241-260.

⁵ Lucica Tudoran, Anis Benabed, *The Informatics Integrated System for the Romanian Civil Status Documents – Practical Considerations and Applicability to the Consular Offices of Romania*, Perspectives of Law and Public Administration, Volume 11, Issue 2, June 2022, pp. 313-322. For a comparative view see Laura Hoti Statovci, *The Impact of Digitalization in Public Administration in Kosovo*, Perspectives of Law and Public Administration, Volume 10, Issue 2, June 2021, pp. 81-84 or Cristina-Elena Popa Tache, *Administrative Review and Reform Movements from the Perspective of International Investment Law*, in Julien Cazala, Velimir Zivkovic (eds.), *Administrative Law and Public Administration in the Global Social System*, ADJURIS - International Academic Publisher, Bucharest, Paris, Calgary, 2021, pp. 212-218.

⁶ See Adrian Groza, George Bara, Cristian Bella, Aurelian Ionescu, Marian Iulian, Camelia Lemnaru, Luciana Moogan, Eugen Popescu, *Elaborarea cadrului strategic național în domeniul inteligenței artificiale*, 21 December 2021, <https://www.adr.gov.ro/wp-content/uploads/2022/03/Analiza-reglementarilor-pentru-domeniul-inteligenței-artificiale.pdf>, consulted on 18 March 2024.

it is a little bitter, about the role of strategies, in general, and we refer specifically to the case of our country.

The first is that strategies, in our view, should be adopted by Parliament, not by the Government. Governments are essentially made up of politicians, and the so-called technocrats in them turn out to be – and they cannot possibly be – politicians, or people who put into practice the political commands dictated by the government.

Parliament is, as the Constitution says,⁷ the supreme representative body of the Romanian people. In Parliament we have both power and opposition, while in the Government we have only power. It is therefore possible – and this has often been proven – that in the opposition there are still some brave people who, through their voice and reactions, can stop or at least temper some of the impulses of the cowardly rulers. That is why, if we are considering drawing up a strategy that outlines the future of the country in one area and, in this way, of all of us, we believe that they should be approved by Parliament. We want to send this message because we see that the strategies that are being drawn up, in all areas, as a rule lies dusty in the drawers of the governments, who remember them when ‘the end is near’ and they have to replace them with others.

Returning to the strategies as they are currently being developed, we note that, in the meantime, a national artificial intelligence strategy has been developed covering the period 2024–2027.⁸

The adoption of this strategy has several objectives. A *first objective* is the need for Romania to develop digital technologies in the economy and society, in line with respect for human rights and the promotion of excellence and trust in artificial intelligence.

A *second objective* is the need to develop and capitalise on its positive effects, in conjunction with managing the risks posed by the evolution of artificial intelligence.

Thirdly, this national strategy proposes that Romania harmonises and integrates itself in the strategic and regulatory actions undertaken at European level in the field of digital services, as well as in the efforts to establish European and international standards in the field of management of technologies based on artificial intelligence.

Last but not least, it is important that the strategy thus developed and implemented should represent a framework for central and local public authorities in Romania to adopt measures and organise their activities in line with the accelerated development of digital infrastructure on a global scale.

⁷ The Constitution of Romania was published in the Official Gazette No. 233/21 November 1991. It was revised by Law No. 429/2003, published in the Official Gazette No. 758/29 October 2003 and republished in the Official Gazette No. 767/31 October 2003.

⁸ <https://www.mcid.gov.ro/wp-content/uploads/2024/01/Strategie-Inteligenta-Artificiala-22012024.pdf>, accessed 18 March 2024.

Underpinning the development of this strategy was the thesis that artificial intelligence must meet seven fundamental requirements, which have been summarised as: a) human oversight; b) technical robustness and security; c) privacy and data governance; d) transparency; e) diversity, non-discrimination and fairness; f) environmental and societal well-being; and g) accountability. With the exception of the first two requirements, which are specific to the field of artificial intelligence, the other five are requirements that characterise public life in general and are applicable at both national and EU level. As regards *privacy and data governance*, it is well known that with the entry into force of the Lisbon Treaty,⁹ data protection has acquired a different framework in EU law, both through the regulation of EU competences and through its enshrinement as a fundamental right.¹⁰ I mention this aspect because it poses particular problems with regard to artificial intelligence.

In this context, we refer to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016¹¹, which has been implemented in Romania, as in all EU Member States,¹² by Law no. 190/2018, as well as by Law no. 129/2018 amending and supplementing Law no. 102/2005 on the establishment, organization and functioning of the National Authority for the Supervision of Personal Data Processing.¹³

Confidentiality is analysed in the doctrine as a component of security in information systems, alongside integrity and availability.¹⁴

Complementary to these general guidelines, a series of principles underlying the development of technologies based on artificial intelligence and the adoption of these solutions in society have also been taken into account, the protection of which is carried out, to a substantial extent and determined for their destiny, by the legal professions.

A first principle is respect for human rights and democratic values.

It should be mentioned, in order to argue this principle, that the Romanian State, according to the first article para. (3) of the Constitution is proclaimed to

⁹ Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, published in OJ C-306 of 17 December 2007.

¹⁰ Irina Alexe, Daniel-Mihail Șandru, *Appointment of a single data protection officer by several public authorities or bodies*, in „Revista de Drept Public” no. 2/2019, p. 46.

¹¹ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals 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), published in OJ L 119 of 4 May 2016, pp. 1–88.

¹² In Romania, the Regulation was implemented by Law No. 190/2018 on measures implementing Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 05/46 EC (General Data Protection Regulation), published in the Official Gazette No. 651 of 26 July 2018.

¹³ Published in the Official Gazette No. 503/19 June 2019. Law No. 102/2005 was republished in the Official Gazette No. 947 of 9 November 2018.

¹⁴ Ioana VasIU, Lucian VasIU, *Crime in cyberspace*, Ed. Universul Juridic, Bucharest, 2011, p. 68.

be a *democratic and social state based on the rule of law*, in which the second supreme and guaranteed value, after human dignity, is *fundamental rights and freedoms*. And in this text, the term democratic/democratic is used twice.

These principled values must be respected both by those who create artificial intelligence and those who apply it through their work.

A *second principle* requires AI to be human-centred, inclusive, non-discriminatory and impartial. This implies and requires at the same time that the exercise of AI is under the control of human action, which is the determining factor in decision-making.

The *third principle* is that of responsibility in the management of artificial intelligence, so as to ensure respect for all fundamental rights and the principles governing their exercise, including non-discrimination in the way artificial intelligence is applied.

A *fourth principle*, which is closely linked to the previous one, is respect for diversity or otherness, as it is also called, in conjunction with gender and equal opportunities. This means that IT services must ensure that everyone has access to the use of artificial intelligence products or services.

The next principle is that of *transparency and trust*, which refers to knowledge of IT processes and their use

The principle reveals that both the data and the processes for processing it is sufficiently known so that their source can be traced and their use is correct.

At the EU level, regulation in the field of Artificial Intelligence is based, among other things, on a European strategy developed in April 2018 (COM – 2018 – 237), a White Paper on Artificial Intelligence – a European approach to excellence and trust developed in 2020, and action plans dating from 2021 with a timeframe of 2027.¹⁵

3. The effects of artificial intelligence

The effects of artificial intelligence are being felt in the legal professions. By attempting a synthesis of them, the aim is to identify the extent to which artificial intelligence could be part of the legal system. Is it possible that the human judge or prosecutor could be replaced by the robot judge or prosecutor? Another question is whether or not there will still be a need for courts in the material, objective sense, as there are at present, or will computer software lead to their disappearance?

We already know that artificial intelligence has penetrated the organisation of justice, and we need only refer to the random distribution of cases, which removes any suspicion of certain interests in their distribution.¹⁶ Or the *electronic*

¹⁵ <https://digital-strategy.ec.europa.eu/en/library/coordinated-plan-artificial-intelligence-2021-review>, accessed 18 March 2024.

¹⁶ Ciutacu Ioana, *The effects of the implementation of artificial intelligence in justice on fundamen-*

file, where all the documents making up the case file are published and can be accessed in the same way.

However, it should be noted that the use of artificial intelligence in judicial decision-making processes, by allowing for programmable and often predictable judicial outcomes, presents risks and vulnerabilities in terms of affecting the right to a fair and timely trial.

Moreover, European regulations also recognise certain vulnerabilities and risks that should be brought to the attention of European and world states.

Thus, the new EU Regulation on Artificial Intelligence states (recital/paragraph 40) that ‘*certain AI systems for the administration of justice and democratic processes should be classified as high risk in view of their potentially significant impact on democracy, the rule of law and individual freedoms, as well as on the right to an effective remedy and to a fair trial*’.¹⁷

In the amendment that has been made to this text, the content has been developed in a way that we consider important and interesting for our study, as follows: ‘(40) *Certain AI systems intended for the administration of justice and democratic processes should be classified as high risk, given their potentially significant impact on democracy, the rule of law and individual freedoms, as well as on the right to an effective remedy and a fair trial. In particular, in order to address potential risks of bias, errors and opacity, it is appropriate to classify as high-risk systems AI systems intended to be used by or on behalf of a judicial authority or administrative body to assist judicial authorities or administrative bodies in investigating and interpreting facts and the law and in applying the law to a particular set of facts, or used in a similar way in alternative dispute resolution. The use of artificial intelligence tools can support, but should not replace, the decision-making power of judges or the independence of the judiciary, as the final decision-making process must remain a human activity and decision. (...)*’.¹⁸

The European Parliament report was drafted by two MEPs, one of whom is Romanian, Dragoş Tudorache, who in a press release gave assurances that ‘*artificial intelligence systems are supervised by humans, are safe and non-discriminatory*’.¹⁹

tal and procedural rights available on https://www.unbr.ro/wp-content/uploads/2022/06/4_Ciutacu-Ioana_Efectele-implementarii-inteligentei-artificiale-in-justitie.pdf, accessed 18 March 2024.

¹⁷ This is the Proposal for a Regulation on Artificial Intelligence, adopted on 14.06.2023 in Strasbourg, on which the European Parliament adopted amendments. The proposal for a Regulation is from the European Parliament and the Council and concerns harmonised rules on artificial intelligence and amending certain Union legislation (COM – 2021 – 0206-09-01461/2021-2021/0106 – COD). See https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_RO.html, accessed 17 March 2024.

¹⁸ Cautiously, the text went on to state: ‘*However, such qualification should not extend to AI systems intended for purely ancillary administrative activities that do not affect the effective administration of justice in individual cases, such as anonymisation or pseudonymisation of court decisions, documents or data, communication between staff members, administrative tasks or resource allocation.*

¹⁹ See <https://www.starupcafe.ro>, accessed 19.11.2023.

This is an important point that artificial intelligence can support the act of justice, but it should not replace the decision-making power of judges or the independence of the judiciary, as the final decision-making process must remain a human activity and decision. We say this because it is in line with our view that there are certain areas in which man will never be replaced in the true sense of the word.

We appreciate that, in terms of the future of professions in general under the impact of artificial intelligence, we are dealing with two broad categories:

A) professions in which humans are replaced by artificial intelligence, but continue to find themselves as supervisors and performers of actions and acts that cannot be performed by them;

B) professions in which man will continue to be the main actor, but will be supported in the exercise of his role by artificial intelligence, which will take over many of the actions that he used to do, simplifying his work and increasing its quality, including by reducing the time it takes. Simply put, either man will assist the computer, or the computer will assist man. It is in this latter category, in which the human remains the principal, that we believe the legal professions fall, and the prospect of the human being totally replaced by artificial intelligence in the legal professions is, in our view, out of the question.

One idea reflected in the European Regulation is that high-risk systems are those concerned with the administration of justice and democratic processes.

The EU Regulation 2021/694 of the European Parliament and of the Council,²⁰ which establishes the Digital Europe Programme, mentions the following related challenges:

- improving access to justice for citizens, lawyers, members of the whole judicial system, through the use of interconnections, having interoperability with databases;

- facilitating an out-of-court dispute resolution²¹.

All this gives us the perspective to understand that there is an awareness among European decision-makers, who also influence national decision-makers, that legal professions have their own specificity, and that the role of artificial intelligence is to help them become more efficient, supporting the holder of such a profession, not pushing him aside. Because in law, in every case, every file has its own specificity, even if the subject matter is apparently common. It has always been said that the judge judges according to the law and his own conscience.

The Constitution states in Art. 124, para. (3) that judges are independent

²⁰ Regulation of 29 April 2021 establishing the Digital Europe Programme and repealing Decision (EU) 2015/224, published in OJEU of 11 05 2021, No. L 166.

²¹ See Maria João Mimoso, *Artificial Intelligence in International Commercial and Investment Arbitration*, International Investment Law Journal, Volume 3, Issue 2, July 2023, pp. 156-166; Cristina Elena Popa Tache, *About the Human Rights and Consumer Protection in the Digital Age of Digital Services Act 2022 or What Aspects Interested Investors Should Pay Attention To*, International Investment Law Journal, Volume 3, Issue 2, July 2023, 121-132.

and subject only to the law. Independence is total and it means that no one can impose or dictate a solution to the judge, not even intelligence other than his own.

4. A few thoughts on the legal profession

The Council of European Bars and Law Societies has produced a document²² which addresses issues of interest such as:

- A) artificial intelligence and human rights;
- B) the need for an ethical framework for the use of artificial intelligence in legal practice;
- C) artificial intelligence tools for use by lawyers.

Today, lawyers are challenged by the increasing amount of data they manage, which requires the use of artificial intelligence for the following purposes:

- a) in the analysis of legislation, case law and doctrine;
- b) in the highlighting of how contracts and all documents are carried out;
- c) the use of automated solutions in drafting documents.

The same document draws attention to the following disadvantages:

- a) the use of data and elements which have not been the subject of an adversarial debate or of conclusions which have not been reached by the judge's reasoning, which leads to the transfer of part of the decision-making power;
- b) lack of transparency of the process and a level playing field (equality of arms);
- c) violation of the principle of impartiality and reasoning, due to the existence of outcomes that are beyond human reasoning and cannot be traced, which could also lead to poorly justified and reasoned decisions.

Certain effects are likely to occur in terms of limiting the right of defence.

A first aspect is that the legal profession is usually practised in small forms of practice, as a rule, practices, which do not have the resources to record data and there are no universally accessible tools to do so.

Other issues relate to the lack of a European or global market for lawyers and the lack of sufficient data and training models in the field of artificial intelligence.

Possible ways of overcoming the above-mentioned difficulties are envisaged and can be systematised as follows:

A) A first way is considered to be the duty of competence of lawyers. This means continuous training and further training for lawyers, enabling them to keep abreast of the legislation adopted in their own country, but also of that

²² Information has been extracted from the CCBE DRAFT Considerations on the legal aspects of Artificial Intelligence, available at https://www.unbr.ro/wp-content/uploads/2020/05/RO_07a_Draft-CCBE-considerations-on-legal-aspects-of-AI.pdf, accessed November 2023 and 18 March 2024.

adopted at supranational level, and we refer in particular to that adopted at European Union level.

They must also be constantly informed about the case law, and we have in mind both the case law of the courts and the case law of the Constitutional Court.

Last but not least, the duty of competence on lawyers requires them to have skills in using the various IT tools.

B) A second obligation is to inform the client. The profession of lawyers involves a partnership with the client, who must be informed of how his case is being conducted,

C) maintaining the independence of lawyers;

D) the obligation of professional secrecy and data protection, which is specific to lawyers, is a *legal professional privilege*, must be ensured when using specific artificial intelligence tools.

5. Conclusions

We are aware that the topic is complex and cannot be ‘covered’ in a single study. What we wanted to do was to raise questions, generate concerns, launch questions and try possible answers. We believe that, from what has been presented above, we can draw some conclusions of interest for the topic we have addressed.

The first of these is that AI-specific tools will bring changes to legal services.

We should also bear in mind that their use also poses threats to the quality of our justice systems, the protection of fundamental rights and the rule of law.

Thirdly, we stress that in order to manage this change effectively, concrete principles and rules need to be established and the appropriate place and role for artificial intelligence systems in the judiciary, and the professions that underpin it, identified.

Within these principles and rules, transparency, fairness, accountability and ethical rules should be the cardinal points.

Society in general, and the legal profession in particular, need to take safeguards to ensure that AI tools work properly.

In all legal professions, including the legal profession, continuous training must be an essential condition for entering and remaining in the profession. The paper presented²³ even discusses *the setting up of IT/IA law labs or workshops in law faculties*, which may also be eligible for EU funding and could lead to the creation of new specialisations for lawyers or even the emergence of new professions.

Fundamental rights and respect for ethical rules cannot be subordinated

²³ We refer to the CCBE DRAFT, Considerations on the legal aspects of Artificial Intelligence, available at https://www.unbr.ro/wp-content/uploads/2020/05/RO_07a_Draft-CCBE-considerations-on-legal-aspects-of-AI.pdf, accessed November 2023 and 18 March 2024.

to mere efficiency gains or cost-saving benefits whether for court users or judicial authorities²⁴. Increasing access to justice by reducing the costs of court proceedings may seem a desirable outcome, but it is less important to improve access to justice when the quality of justice is compromised in the process. Justice is one of the most important activities in a society, and its quality cannot be compromised by claiming savings for the state or for the litigants.

Bibliography

1. Alexe, Irina & Daniel-Mihail Șandru, *Appointment of a single data protection officer by several public authorities or bodies*, in „Revista de Drept Public” no. 2/2019.
2. CCBE Draft, Considerations on the legal aspects of Artificial Intelligence, available at https://www.unbr.ro/wp-content/uploads/2020/05/RO_07a_Draft-CCBE-considerations-on-legal-aspects-of-AI.pdf, accessed November 2023 and 18 March 2024.
3. Ciutacu, Ioana, *The effects of the implementation of artificial intelligence in justice on fundamental and procedural rights* available on https://www.unbr.ro/wp-content/uploads/2022/06/4_Ciutacu-Ioana_Efectele-implementarii-inteligentei-artificiale-in-justitie.pdf, accessed 18 March 2024.
4. Constitution of Romania was published in the Official Gazette No. 233/21 November 1991, it was revised by Law No. 429/2003, published in the Official Gazette No. 758/29 October 2003 and republished in the Official Gazette No. 767/31 October 2003.
5. Groza, Adrian, George Bara, Cristian Bella, Aurelian Ionescu, Marian Iulian, Camelia Lemnaru, Luciana Moogan & Eugen Popescu, *Elaborarea cadrului strategic național în domeniul inteligenței artificiale*, 21 December 2021, <https://www.adr.gov.ro/wp-content/uploads/2022/03/Analiza-reglementarilor-pentru-domeniul-inteligenței-artificiale.pdf>, consulted on 18 March 2024.
6. Mimoso, Maria João, *Artificial Intelligence in International Commercial and Investment Arbitration*, International Investment Law Journal, Volume 3, Issue 2, July 2023, pp. 156-166.
7. Popa Tache, Cristina Elena, *About the Human Rights and Consumer Protection in the Digital Age of Digital Services Act 2022 or What Aspects Interested Investors Should Pay Attention To*, International Investment Law Journal, Volume 3, Issue 2, July 2023, 121-132.
8. Popa Tache, Cristina-Elena, *Administrative Review and Reform Movements from the Perspective of International Investment Law*, in Julien Cazala, Velimir Zivkovic (eds.), *Administrative Law and Public Administration in the Global Social System*, ADJURIS - International Academic Publisher, Bucharest, Paris, Calgary, 2021, pp. 212-218.
9. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27

²⁴ See Cătălin-Silviu Săraru, *Drept administrativ. Curs universitar*, vol. II, Ed. Universul Juridic, Bucharest, 2024, p. 194; Cătălin-Silviu Săraru, *Tratat de contencios administrativ*, Ed. Universul Juridic, Bucharest, 2022, p. 40-50.

- April 2016 on the protection of individuals 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), published in OJ L 119 of 4 May 2016, pp. 1–88.
10. Regulation of 29 April 2021 establishing the Digital Europe Programme and repealing Decision (EU) 2015/224Slide0, published in OJEU of 11 05 2021, No. L 166.
 11. Săraru, Cătălin-Silviu, *Drept administrativ. Curs universitar*, vol. II, Ed. Universul Juridic, Bucharest, 2024.
 12. Săraru, Cătălin-Silviu, *Provocări contemporane în administrația publică și în dreptul administrativ* in Brătianu, Constantin, Doina Banciu & Nicolae Dănilă (coord.), *Economia și societatea în era digitalizării*, Publishing House of the Romanian Academy of Scientists, Bucharest, 2023, p. 241-260.
 13. Săraru, Cătălin-Silviu, *Tratat de contencios administrativ*, Ed. Universul Juridic, Bucharest, 2022.
 14. Shevchuk, Oleksandr, Ihor Kompaniets, Olena Volianska, Oleksandra Shovkopljas & Vasyl Baranchuk, *Electronic Administrative Judicial Procedure of Ukraine and the Right to Judicial Protection: Problems of Legal Regulation and Practical Issues*, Juridical Tribune - Review of Comparative and International Law, Volume, 14, no. 1, March 2024, p. 98-115.
 15. Shevchuk, Oleksandr, Volodymyr Martynovskyi, Olena Volianska, Ihor Kompaniets & Oleg Bululukov, *Problems of legal regulation of artificial intelligence in administrative judicial procedure*, Juridical Tribune - Tribuna Juridica, Volume 13, Issue 3, October 2023, pp. 346-426.
 16. Statovci, Laura Hoti, *The Impact of Digitalization in Public Administration in Kosovo*, Perspectives of Law and Public Administration, Volume 10, Issue 2, June 2021, pp. 81-84.
 17. Tudoran, Lucica & Anis Benabed, *The Informatics Integrated System for the Romanian Civil Status Documents – Practical Considerations and Applicability to the Consular Offices of Romania*, Perspectives of Law and Public Administration, Volume 11, Issue 2, June 2022, pp. 313-322.
 18. Vasiu, Ioana & Lucian Vasiu, *Crime in cyberspace*, Ed. Universul Juridic, Bucharest, 2011.
 19. Vedinaș, Verginia, *Odiseea funcției publice în România sau de la perceptor la programe pe calculator*, in Brătianu, Constantin, Doina Banciu & Nicolae Dănilă (coord.), *Economia și societatea în era digitalizării*, Publishing House of the Romanian Academy of Scientists, Bucharest, 2023, p. 223-240.

Liability of News Platforms under the Digital Services Act

Teaching assistant **Sorin-Alexandru VERNEA**¹

Abstract

This article analyzes the conditions under which news platforms can be held liable under European Regulation (EU) 2022/2065 of the Parliament and of the Council (Digital Services Act). The first part concerns the object of the DSA regulation, by reference to news platforms, and the second part regards the notion of illegal content and its specific nature in the case of news platforms. The third and fourth parts concern the liability of the online platform both for posted articles and for advertising, in which the author has identified a distinct regime depending on the type of uploaded material. The conclusion of the paper concerns the importance of the European Regulation (EU) 2022/2065 of the Parliament and of the Council for the activity of journalists and news platforms.

Keywords: news platforms, Digital Services Act, public communication law, journalist's responsibility, press freedom.

JEL Classification: K24, K33

DOI: <https://doi.org/10.62768/ADJURIS/2024/1/08>

Please cite this article as:

Vernea, Sorin-Alexandru, „Liability of News Platforms under the Digital Services Act”, in Pajuste, Tiina, Heliona Bellani (Miço) & Sejla Maslo Cerkić (eds.), *Legal Perspectives in the Modern Era of Technological Transformations*, ADJURIS – International Academic Publisher, Bucharest, Paris, Calgary, 2024, p. 126-137.

1. Introduction

Freedom of the press implies carrying out the activities of collecting and transmitting information to the public through media channels, without the intervention of authorities on the content of the communicated message.

Since the French Revolution of 1789, freedom of speech has been consistently recognized as a fundamental right², celebrated both nationally and internationally, especially in the second part of the 20th century.

¹ Sorin-Alexandru Vernea - Faculty of Law, University of Bucharest, Romania, vernea.sorin-alexandru@drept.unibuc.ro.

² Art. 11 of the Declaration of the Rights of Man and Citizen adopted in 1789 provided: "The free communication of thoughts and opinions is one of the most precious human rights; every citizen can therefore speak, write and print freely, except in the cases provided by law, in which he will have to answer for the abusive use of this freedom."

In most international regulations, freedom of expression includes both the right to send and the right to receive information transmitted by others to the public. The enforcement of these rights was achieved both by art. 19 of the Universal Declaration of Human Rights³, as well as by art. 10 of the European Convention on Human Rights⁴. The latter regulation was imported, in a similar manner, by art. 11, paragraph 1 of the Charter of Fundamental Rights of the European Union.

Undeniably, freedom of expression is a fundamental right, recognized, at least formally, in any modern society. Freedom of the press is a component of this right, having a complex content, which includes both the freedom of speech and the freedom to organize the journalist's activity.

With the development of information technology, public communication has entered a new stage of development, and traditional means such as newspapers, radio channels and television have been overtaken by online media, both in written and audio-video formats.

The Internet is an important part of life in contemporary society, and for the younger generations it represents a natural element known since birth.

Unlike the traditional press, which has benefited from a heterogeneous regulatory framework for the last decades in European states, the online press has, with few exceptions, been exempted from any attempt of regulation.

In reality, the accelerated development of a new, innovative communication system could not be achieved without almost total freedom of action. Under these conditions, at the level of the European Union, in the first decade of the 2000s, there were no mechanisms to restrict the content of information posted online, only messages of an obviously illegal nature, such as those with terrorist content, or inciting hatred and discrimination, were prohibited. Otherwise, the authorities had a passive role⁵ and allowed the existence of some self-regulatory mechanisms, most of them dependent on the editorial policy of each individual online publication.

The doctrine of the passive role of the authorities, both at national and European level, limited the possibility of applying the principle of responsibility, as a general principle of communication law⁶, since beyond the responsibility of the author of a material posted online, there is no form of liability for the provider

³ Adopted in 1948, by the General Assembly of the United Nations Organization - according to art. 19: " Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers."

⁴ Adopted at the level of the Council of Europe in 1950 - according to art. 10, paragraph 1: "Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers."

⁵ E. Lazăr, N. D. Costescu, *Dreptul european al internetului*, Hamangiu Publishing House, Bucharest, 2021, p. 46.

⁶ S.-Al. Vernea, *Dreptul Comunicării*, Hamangiu Publishing House, Bucharest, 2021, p. 12.

of the hosting service of that material.

This regulatory omission has been corrected by the European legislator through multiple measures taken in recent years⁷.

On October 19, 2022, Regulation (EU) 2022/2065 of the European Parliament and of the Council on a single market for digital services and amending Directive 2000/31/EC (Digital Services Regulation), was adopted; hereinafter referred to as "DSA".

We are of the opinion that taking concrete measures, homogeneous at European level in this matter, constitutes the foundation for regulating liability of online platforms, which by their nature are not dependent on borders or national specifics.

Precisely for these reasons, the European legislator opted for the enforcement of a Regulation, an act with direct applicability in the internal law of member states⁸, which, unlike directives, does not require implementation⁹. Some authors have rightly pointed out that the standard imposed by the regulation is a minimal one¹⁰, each member state being free to improve by national legislation.

2. The object of the DSA Regulation regarding news platforms

Beyond the purpose of the act, expressly revealed by art. 1, paragraph 1, the object of regulation is provided in the following paragraph. According to it: "This Regulation lays down harmonised rules on the provision of intermediary services in the internal market. In particular, it establishes: (a) a framework for the conditional exemption from liability of providers of intermediary services; (b) rules on specific due diligence obligations tailored to certain specific categories of providers of intermediary services; (c) rules on the implementation and enforcement of this Regulation, including as regards the cooperation and coordination between the competent authorities."

From the content of the rendered text, we note that the regulation aims to establish uniform conditions for providing services on the internal market. The most important regulated areas are aimed at establishing a common framework for holding intermediate service providers liable and implicitly determining the cases of exonerating them from liability for the existence of illegal content. From

⁷ J. P. Quintais, S. F. Schwemer, *The Interplay between the Digital Services Act and Sector Regulation: How Special Is Copyright?*, European Journal of Risk Regulation, vol. 13, No. 2/2022, p. 192.

⁸ P. Church, C. N. Pehlivan, *The Digital Services Act (DSA): A New Era for Online Harms and Intermediary Liability*, Global Privacy Law Review, vol. 4, No. 1/2023, p. 53.

⁹ M. A. Dumitraşcu, *Dreptul Uniunii Europene I*, Universul Juridic Publishing House, Bucharest, 2021, p. 318.

¹⁰ A. Savin, *The EU Digital Services Act: Towards a More Responsible Internet*, Copenhagen Business School Law Research Paper Series No. 21-04, 2021, p. 5, available online at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3786792, accessed on 16.03.2024.

the wording of art.1, par.2, letter an of the Regulation, we note that the rule consists in holding intermediate service providers liable for illegal content, and, exceptionally, they can be exempted from liability under certain restrictive conditions.

Equally, the Regulation establishes preventive obligations of certain categories of suppliers, these being limited to due diligence obligations. In order to effectively apply the regulation at the level of the European Union, given the fact that the transmission of information does not depend on the existence of borders, common rules of cooperation between the authorities of the member states have been established.

In the matter of online media, the regulation is particularly relevant for determining the conditions of liability for news platforms, respectively of their exoneration from liability. We note that the DSA Regulation does not regulate an editorial policy, this being essentially left to the discretion of each publication, respectively platform, however, in the event of posting material with illegal content, the responsibility does not fall solely on the author¹¹, but also on the platform that provided the hosting services and implicitly, made the information public.

By art. 2, par. 1 and 2 of the DSA Regulation, the fields in which it produces effects are expressly stipulated, respectively: "1. This Regulation shall apply to intermediary services offered to recipients of the service that have their place of the establishment or are located in the Union, irrespective of where the providers of those intermediary services have their place of the establishment. 2. This Regulation shall not apply to any service that is not an intermediary service or to any requirements imposed in respect of such a service, irrespective of whether the service is provided through the use of an intermediary service."

The sequence of the two previously reproduced paragraphs clearly shows that the regulation is not intended to be applied directly to the authors of online materials or the producer of an audio-video material, but only to the intermediary that provides the public communication service, called "intermediate service". This notion is defined by art. 3, letter g of the Regulation: "one of the following information society services: (i) a 'mere conduit' service, consisting of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network; (ii) a 'caching' service, consisting of the transmission in a communication network of information provided by a recipient of the service, involving the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients upon their request; (iii) a 'hosting' service, consisting of the storage of information provided by, and at the request of, a recipient of the service".

The activity of simple transmission (mere conduit) is carried out by the

¹¹Who will be liable for his own deed under the conditions of tortious or contractual civil liability, depending on the content of the message and the obligations violated by making it available to the intermediary service provider?

provider of the internet service. This does not involve an analysis, of any kind, of the information communicated, thus not being relevant for the responsibility of the news platforms.

Equally, the caching service involves the automatic, temporary storage of some information to make it much more quickly accessible to end users, without any control of the storage service provider over the content of the stored data. Thus, this category of intermediate services is also not relevant for the liability of news platforms.

In terms of the hosting service, it involves storing information provided by one person, followed by communicating that information upon access by another person. In general, this service is provided through online platforms, defined by art. 3, letter I of the Regulation as "a hosting service that, at the request of a recipient of the service, stores and disseminates information to the public, unless that activity is a minor and purely ancillary feature of another service or a minor functionality of the principal service and, for objective and technical reasons, cannot be used without that other service, and the integration of the feature or functionality into the other service is not a means to circumvent the applicability of this Regulation".

Regarding news platforms, this term is an equivalent to specialized sites, online publications, blogs, sites that provide audio-video files, including news feed on social networks or social media applications, etc. Any form of organization through which an electronic platform makes available to the public information produced by other persons, performs, in concrete terms, a hosting activity within the meaning of the Regulation. For the purpose of this article, by news platforms we will designate the specialized sites that have an editorial policy and collaborate with professional journalists. The rest of the platforms will be designated by indicating their typology.

3. Illegal content in news platforms – concept and importance

The role of the DSA Regulation is to establish the conditions under which an intermediary service provider, in this case a news platform, is responsible for the material found within it. As a rule, platforms will be liable for posting "illegal content". The definition of the notion is made by art. 3, letter h of the Regulation, as "any information that, in itself or in relation to an activity, including the sale of products or the provision of services, is not in compliance with Union law or the law of any Member State which is in compliance with Union law, irrespective of the precise subject matter or nature of that law".

Under these conditions, by illegal content we do not mean only messages expressly prohibited by the legal provisions of the European Union, but also information that does not comply with the law of the Union or of any member state, regardless of the object or nature of that law. In our opinion, everything that exceeds the limits of freedom of expression, regulated by art. 10 of the European

Convention on Human Rights or by art. 11 of the Charter of Fundamental Rights of the European Union, will be qualified as illegal content.

For this purpose, we note that freedom of expression can be limited, according to art. 10, paragraph 2 of the European Convention on Human Rights, through measures provided by law, necessary in a democratic society and proportionally used to protect the following values: (i) national security (ii) territorial integrity or public safety (iii) defense of public order and crime prevention (iv) protection of health or morals, (v) protection of reputation or rights of others (vi) to prevent disclosure of confidential information or (vii) to guarantee the authority and impartiality of the judiciary.

Although art. 11 of the Charter of Fundamental Rights of the European Union does not contain an equivalent of art. 10, paragraph 2 of the ECHR Convention, we note that the scope and meaning of the freedom of expression, as a fundamental right, are the same, as expressly stipulated by art. 52, paragraph 3, sentence I of the Charter¹².

Under these conditions, the violation of any limit of freedom of expression, as provided for by the ECHR Convention, automatically implies a violation of freedom of expression under the terms of the Charter, which leads to the classification of the content as illegal.

In addition, depending on the national law of each member state, what exceeds the limits of freedom of expression recognized in domestic law, to the extent that it does not contradict Union law, constitutes illegal content.

In our opinion, the platform is responsible for an act of its own, that of not having limited the spread of illegal content, although it had the opportunity to know the nature of this material, either by setting up an automatic content filtering system or by analyzing notifications sent by users.

Determining the illegal content is essential for triggering the liability mechanism according to the Regulation or for identifying the conditions for exemption from liability.

4. Particular rules regarding the liability of news platforms

Since news platforms are a species of online platforms, the provisions of the Common Regulation for online platforms will be applied to them, customized according to the defining elements of a news platform: (i) gathering materials on a multitude of subjects (ii) the existence of an editorial policy (iii) the elaboration of materials by persons either in a relationship of subordination to the platform, or in a contractual relationship of collaboration (professionals).

As a rule, to the extent that there is illegal, publicly accessible content on

¹² According to art. 52, paragraph 3, sentence I of the Charter of Fundamental Rights of the European Union: "to the extent that this charter contains rights that correspond to rights guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms, their meaning and extent are the same as those provided by the mentioned convention".

the platform, its civil liability will be incurred. The Regulation introduced, in art. 6, paragraph 1 an exemption clause, according to which: "Where an information society service is provided that consists of the storage of information provided by a recipient of the service, the service provider shall not be liable for the information stored at the request of a recipient of the service, on condition that the provider: (a) does not have actual knowledge of illegal activity or illegal content and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or illegal content is apparent; or (b) upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the illegal content."

Legal literature¹³ referred to this provision as a "liability shield", which we think is an appropriate terminology.

The text imposes two alternative conditions for exonerating the platform from liability: (a) not to know the illegal content or data or facts from which the illegal content results or (b) to promptly remove the illegal content. The removal can be done both *ex officio*, through a preventive measure, and at the express request of at least one user, who sent a notification for this purpose.

Although the previously exposed rules can be used in blog posts or in the news feed on social media platforms, they do not apply in the case of news platforms with editorial control. We bear in mind that news platforms have the nature of specialized sites, with their own editorial policy, a fact that attracts the incidence of art. 6, paragraph 2 of the Regulation, according to which: "paragraph 1 shall not apply where the recipient of the service is acting under the authority or the control of the provider". Subjecting the posted materials (press articles, audio-video reports) to an editorial policy, which is equivalent to exercising a form of control over the content posted on the platform. It is extremely important to make a distinction between the exercise of an editorial control prior to publication, which aims at both the form and substance of the respective material, according to the editorial policy of the platform, and the exercise of a technical, automated control to identify any illegal content (nudity, words specific to licentious language or messages of a terrorist nature or that incite hatred, etc.).

In this regard, art.7 of the Regulation uses this distinction, even if the legislator did not expressly regulate it, stipulating: "Providers of intermediary services shall not be deemed ineligible for the exemptions from liability referred to in Articles 4, 5 and 6 solely because they, in good faith and in a diligent manner, carry out voluntary own-initiative investigations into, or take other measures aimed at detecting, identifying and removing, or disabling access to, illegal content, or take the necessary measures to comply with the requirements of Union law and national law in compliance with Union law, including the requirements set out in this Regulation." This article was inspired by section 230 of the US

¹³A. Turillazzi, M. Taddeo, L. Floridi, F. Casolari, *The digital services act: an analysis of its ethical, legal, and social implications*, Law, Innovation and Technology, vol. 15, No. 1/2023, p. 95.

Communications Decency Act, as amended by the Telecommunications Act of 1996¹⁴ and acts as a reward for the efforts of the platform operator, who in good faith tried to remove the illegal content.

By applying this rule to news platforms, we observe that intermediate service providers can benefit from the protection conferred by art.6 even if they carry out in good faith, investigations and checks capable of leading to the identification, removal or blocking of illegal content. In reality, the legislator notes that conducting investigations on its own initiative and in good faith does not equate to editorial control, which is why the platform can be exonerated from liability.

Under these conditions, we appreciate that regarding the news platforms, for the posted materials (press articles, audio-video reports, images) the exemption from liability cannot occur either according to art. 6 or according to art. 7 of the Regulation, since, in both situations, the editorial control disqualifies the platform from liability exemption, as expressly stipulated in art.6, paragraph 2 of the Regulation.

The situation is different with regard to comments posted by users, to the extent that they are allowed by the platform. We appreciate that it is not possible to apply the editorial policy for comments, as they result from the freedom of expression of the readers. Regarding them, there is no control from the intermediary service provider, and the simple application of content-based filters (licensed words, nudity, words specific to terrorist messages, etc.), does not disqualify the news platform from the exemption from liability provided of art. 6, par. One and art. 7 of the Regulation, strictly in what concerns the content of the comments.

Therefore, the DSA Regulation does not exempt news platforms from liability regarding the content subject to editorial control, but allows the removal of liability, under the restrictive conditions stipulated in arts. 6 and 7 regarding the content of comments or other information posted by users and not subjected to editorial control.

To the extent that we will refer to a news blog, or a page on a social network or a channel on an audio-video content-sharing sites, we will not be in the presence of a publication, with its own editorial policy, but of a personal page, a fact that will allow the intermediary service provider to be exempted from liability under the conditions of fulfilling one of the assumptions provided by art.6, paragraph 1 letter "a" or "b" of the Regulation. Equally, if the service provider has its own policy of automatic verification or investigation of the content, followed by its deactivation for preventive purposes, we consider that the provisions of art. 7 of the Regulation may apply, and thus the provider will benefit from the exemption from liability in the basis of the Good Samaritan clause.

¹⁴ Available online at <https://www.fcc.gov/general/telecommunications-act-1996>, accessed on 16.03.2024.

As noted in literature, the DSA Regulation not only encourages the detection of illegal content, but also the removal or disabling of access to it, without the prior permission of a judicial or administrative authority¹⁵. In the field of online platforms, another, much more subtle, way of reducing the visibility of a material consists of "shadow banning", a procedure that makes it no longer accessible in the main flow of the platform for users¹⁶. Either way, concretely, the task of protecting the public against illegal content is outsourced to private individuals, respectively to intermediate service providers, who have the opportunity to act by limiting, at least temporarily, the freedom of expression of the authors of censored materials.

In our opinion, we are not in the presence of an impermissible limitation of the exercise of a fundamental right, since, on the one hand, such measures can be taken to prevent the dissemination of illegal content, and after taking such a measure, the author will be notified, having the possibility to appeal the decision of the intermediate service provider in a summary and fast solving procedures.

Another provision of the Regulation, applicable in a particular way in for news platforms, is found in art. 8 of the DSA: 'No general obligation to monitor the information which providers of intermediary services transmit or store, nor actively to seek facts or circumstances indicating illegal activity shall be imposed on those providers.'

The provision indicates that the news platform does not have a general obligation to monitor information communicated to the public. This regulation is only relevant for posted content for which there was no previous editorial control, which would be equivalent to information monitoring, but it is also relevant for comments and any information posted without having been subjected to control. For news blogs, pages on a social network or channels for sharing audio-video content, the provisions of art. 8 of the DSA have the nature of a guarantee that prohibits unjustified censorship, for preventive reasons.

Legal literature¹⁷ considered that the role of this article is to balance the risk that the service provider, by exercising a control obligation, could plausibly know the illegal nature of the content and thus be held liable.

5. Rules regarding advertising on a news platform

The relationship between the press and advertising implies an obvious interdependence, as long as advertising constitutes an essential source of income

¹⁵ C. Cauffman, C. Goanta, *A New Order: The Digital Services Act and Consumer Protection*, European Journal of Risk Regulation, vol. 12, No. 4/2021, p. 769.

¹⁶ P. Leerssen, *An end to shadow banning? Transparency rights in the Digital Services Act between content moderation and curation*, Computer Law & Security Review, vol. 48, 2023, p. 3.

¹⁷ I. Buri, J. van Hoboken, *The Digital Services Act (DSA) proposal: a critical overview*, in Digital Services Act (DSA) Observatory Institute for Information Law (IViR), University of Amsterdam, 2021, p. 16, available online at: https://dsa-observatory.eu/wp-content/uploads/2021/11/Buri-Van-Hoboken-DSA-discussion-paper-Version-28_10_21.pdf, last accessed on 16.03.2024.

for any publication. Under these conditions, any news platform benefits from a space allocated to advertising.

In advance, we note that the provisions relating to it are not applicable to the services of online platform providers that qualify as micro-enterprises or small enterprises, within the meaning of the definition in Recommendation 2003/361/EC, as stipulated in art. 19, paragraph 1 of Regulations. Exceptions are made by platform providers that qualify as VLOP, i.e. very large online platforms in accordance with art. 33 of the Regulation, i.e. have an average monthly number of active service recipients in the Union greater than or equal to 45 million and that are designated as very large online platforms.

The substantial regulation regarding advertising on online platforms can be found in art. 26, paragraph 1 of the DSA Regulation, according to which: ‘Providers of online platforms that present advertisements on their online interfaces shall ensure that, for each specific advertisement presented to each individual recipient, the recipients of the service are able to identify, in a clear, concise and unambiguous manner and in real time, the following: (a) that the information is an advertisement, including through prominent markings, which might follow standards pursuant to Article 44; (b) the natural or legal person on whose behalf the advertisement is presented; (c) the natural or legal person who paid for the advertisement if that person is different from the natural or legal person referred to in points (b); (d) meaningful information directly and easily accessible from the advertisement about the main parameters used to determine the recipient to whom the advertisement is presented and, where applicable, about how to change those parameters.’

As it follows from the previous text, the European legislator imposed four transparency conditions: (i) identification of the material as advertising (ii) identification of the beneficiary of the advertising activity (iii) identification of the entity that paid for the advertising activity, if it is distinct from the beneficiary and (iv) easy identification of the recipient of the advertising activity.

The purpose of the regulation aims, on the one hand, to make a clear distinction between informative materials posted on the platform and materials intended to promote products or services. In this way, the degree of fidelity of the assessments made by the author of the advertising materials are subjected to a specific level of tolerance, intended for commercial promotion. This rule constitutes an application of the principle of objectivity, as a specific principle of public communication law.

As for the beneficiary of the activity, we note that it is presumed to be the entity that paid for the advertising activity, and if the latter is different, the public is entitled to know, precisely because negative, deceptive or comparative advertising can easily go unnoticed.

In our view, the rules on advertising are elementary and specific to the purpose of the regulation, which is to increase transparency in the use of online platforms.

6. Conclusions

The adoption of the DSA Regulation represents an important landmark in the European Union's activity of unitary regulating digital platforms. With the emergence of online media and communication technology, new means of rapid and exceptionally efficient communication have appeared, such as vlogs, live broadcasts through social networks and a multitude of channels for sharing audio-video content.

These changes led to a reconfiguration of modern journalism, by simplifying both the information transmitted and the way of receiving it.

Currently, a considerable part of the press predominantly operates in the sphere of online publications, either by using a news platform, with a constant audience, loyal through the publications' editorial policy, or by freelancing.

With the entry into force of the DSA Regulation, rules were established to moderate communications, by preventing the dissemination to the public of any information that, according to European law and the national law of the member states, can be classified as illegal content.

Although, at first glance, such a regulation appears as a form of censorship, we note that it pursues a legitimate goal, and constitutes a beginning for the establishment of a legal framework for online platforms, including those in the media.

In agreement with some recent literature,¹⁸ we appreciate that the Regulation incorporates the values of the Charter of Fundamental Rights of the European Union, which gives it a long perspective in the regulated field.

As we have observed, its application involves many particularities when the provider of intermediate services is a news platform, its responsibility being difficult to remove, as long as there is an editorial control over the published materials. In these conditions, the regulation has, however, an encouraging nature for journalists, on the one hand, because it reduces the risk of exposing the public to misinformation, and, on the other hand, because it transfers the burden of responsibility to the publisher, thus preventing a risk of retaliation through judicial action of the person mentioned in the press material, against the journalist.

In essence, we can say that the Regulation contributes to increasing the degree of safety of public communications carried out online, both through its regulatory object and its effects.

¹⁸ A. P. Heldt, *EU Digital Services Act: The White Hope of Intermediary Regulation*, in T. Flew, F. R. Martin, *Digital platform regulation, Global Perspectives on Internet Governance*, Palgrave Macmillan, Cham, 2022, p. 76.

Bibliography

1. Buri, I & J. van Hoboken, *The Digital Services Act (DSA) proposal: a critical overview*, Digital Services Act (DSA) Observatory Institute for Information Law (IViR), University of Amsterdam, 2021.
2. Cauffman, C. & C. Goanta, *A New Order: The Digital Services Act and Consumer Protection*, European Journal of Risk Regulation, vol. 12, No. 4, 2021.
3. Church, P. & C. N. Pehlivan, *The Digital Services Act (DSA): A New Era for Online Harms and Intermediary Liability*, Global Privacy Law Review, vol. 4, No. 1/2023.
4. Dumitrașcu, M. A., *Dreptul Uniunii Europene I*, Universul Juridic Publishing House, Bucharest, 2021.
5. Heldt, A.P., *EU Digital Services Act: The White Hope of Intermediary Regulation*, in Flew, T. & F. R. Martin, *Digital Platform Regulation, Global Perspectives on Internet Governance*, Plagrave Macmillan, Cham, 2022.
6. Lazăr, E. & Costescu, N. D., *Dreptul european al internetului*, Hamangiu Publishing House, Bucharest, 2021.
7. Leerssen, P., *An end to shadow banning? Transparency rights in the Digital Services Act between content moderation and curation*, Computer Law & Security Review, vol. 48, 2023.
8. Quintais, J. P. & S. F. Schwemer, *The Interplay between the Digital Services Act and Sector Regulation: How Special Is Copyright?*, European Journal of Risk Regulation, vol. 13, No. 2/2022.
9. Savin, A., *The EU Digital Services Act: Towards a More Responsible Internet*, Copenhagen Business School Law Research Paper Series No. 21-04, 2021.
10. Turillazzi, A., M. Taddeo, L. Floridi & F. Casolari, *The digital services act: an analysis of its ethical, legal, and social implications*, Law Innovation and Technology, vol. 15, No. 1/2023.
11. Vernea, S.-Al., *Dreptul comunicării*, Hamangiu Publishing House, Bucharest, 2021.

The Processing of Personal Data in Contracts for the Supply of Digital Content and Services

PhD. student **Sorana BRISC**¹

Abstract

This paper highlights the impact of personal data processing in contracts for the supply of digital content and services. The primary aim of this study is to clarify the role played by the consent given by the data subject to the processing of personal data within the framework of these new-wave digital contracts. In particular, our focus lies on discerning the consequences of the withdrawal of consent on the contract itself. This subject requires a multidisciplinary approach. By using the historical, theoretical and descriptive method of scientific inquiry, we hope to provide a more precise understanding of the complex regulatory framework governing electronic commerce. The paper commences by explaining the socio-economic and regulatory context in which the processing of personal data influences contract law. In the first section of the paper, we underline the distinction between two manifestations of will: the contractual consent, understood as a prerequisite for the validity of a contract, and the GDPR consent, representing an agreement to the processing of personal data. Subsequently, we emphasize the role of GDPR consent in synallagmatic contracts for the supply of digital content and services whereas the third section deals with the effects of GDPR consent withdrawal on the digital contract. Following our research, we concluded that there is a symbiotic relationship between the two legal forms of consent, despite their different nature. It is certain that the extensive processing of data, often referred to as 'Big Data', which has been prevalent for at least a decade, claims the need to protect the consumer of digital content and services beyond the non-patrimonial nature of the fundamental rights regulated by Regulation (EU) 2016/679.

Keywords: *supply of digital content, supply of digital services, Directive (EU) 2019/770, Regulation (EU) 2016/679, consent, processing of personal data.*

JEL Classification: K15, K24

DOI: <https://doi.org/10.62768/ADJURIS/2024/1/09>

Please cite this article as:

Brisic, Sorana, „The Processing of Personal Data in Contracts for the Supply of Digital Content and Services”, in Pajuste, Tiina, Heliona Bellani (Miço) & Sejla Maslo Cerkić (eds.), *Legal Perspectives in the Modern Era of Technological Transformations*, ADJURIS – International Academic Publisher, Bucharest, Paris, Calgary, 2024, p. 138-153.

¹ Sorana Brisc - Doctoral School of Law, Faculty of Law, Babeş-Bolyai University of Cluj, Romania, sorana.suciu@gmail.com.

1. Introductory remarks

The economical context in which consent given to the processing of personal data influences contract law already has a history of at least a decade. The emergence of new disruptive technologies enhanced by data production has given rise to contractual figures never seen in the past. We are referring to the contracts for the supply of digital content and services that nowadays benefit from a unified normative act at the European Union level: Directive (EU) 2019/770², further referred to as ‘DCD’.

The DCD governs two primary obligations of the supplier of digital content and services: the obligation to supply and the conformity obligation³. However, no definition of the term ‘supply’ is provided⁴. No less true is that the DCD’s source of inspiration is the abandoned Proposal for a European Regulation on a Common European Sales Law [CESL]⁵. CESL was intended to establish the legislative framework for sale contracts while also regulating the contracts for the supply of digital content⁶.

The inclusion of the contract for the supply of digital content within a regulatory instrument that aimed to create a common sales law proves the European interest in regulating the supplying of digital content in alignment with the consumer’s sales law. The choice of the European legislator is unsurprising, given that the civil law is structured in a way that places the synallagmatic sales contract at its core⁷.

² Directive (EU) 2019/770 Of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services, OJ L 136 of 22 May 2019, pp. 1–27. Romania transposed the DCD by O.U.G. no. 141/2021, M. Of. Number 1248 of 30 December 2021.

³ Alongside the DCD, the European legislator adopted the corresponding regulatory instrument regulating the sale of goods, including goods with embedded software. Directive (UE) 2019/771 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the sale of goods, amending Regulation (EU) 2017/2394 and Directive 2009/22/EC, and repealing Directive 1999/44/EC, OJ L 136 of 22nd of May 2019. Romania transposed the Directive by O.U.G. no. 140/2021, M. Of. Number 1245 of 30 December 2021.

⁴ In the draft stage of the regulatory act, it was discussed about defining the act of supply as granting access to digital content or making digital content available, but it was abandoned because by defining the act of supply, future performances could fall outside its scope of application. See the Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content, 9 December 2015, COM (2015) 634 final.

⁵ See Proposal for a Regulation of the European Parliament and of the Council on a Common European Sales Law, 11th of October 2011, COM (2011) 635 final.

⁶ Andrej Savin, *Harmonising Private Law in Cyberspace: The New Directives in the Digital Single Market Context*, Copenhagen Business School Law Research Paper Series no. 19–35/2019. The document is available online at the address: <https://ssrn.com/abstract=3474289>, date of last access: 1st of Mars 2024. For the same conclusion, see Sorana Suciuc, *Reflecții asupra contractului digital*, Revista Română de Drept Privat No. 2/2022, p. 393.

⁷ François Terré, Philippe Simler, Yves Lequette, François Chénéde, *Droit civil. Les obligations*, 13^e édition, Dalloz, Paris, 2022, p. 38. However, the synallagmatic nature of the sale emerged later, under the influence of canonists. In this regard, see Philippe Malaurie, Laurent Aynès, Pierre Yves

But currently, economic reality sheds light on contract models that increasingly diverge from traditional sales contract. This pertains to the transfer of digital assets, such as digital financial instruments or computer programs, where the conventional sale, primary involving the transfer of ownership, is incompatible with the virtual nature of these new digital assets⁸. However, sales law, tied to the physical aspect of the goods, continues to serve as the main framework for all other contracts.

Thus, the contract for the supply of digital content and services addressed by the DCD (further referred to as the *digital contract*)⁹ is not a sale of digital content, but rather an unnamed contract¹⁰. The act of qualifying for the type of binding legal agreement falls within the scope of the national law, which determines it in accordance with otherwise flexible private law rules.

However, this mission is challenging. At the European Union level, the legislation concerning the new technologies is fragmented among regulatory acts with varying degrees of force and applicability. We take as an example the General Data Protection Regulation [GDPR]¹¹, the Directive on intellectual rights upon computer programs [Software Directive]¹², the Directive on the Supply of Digital Content and Services [DCD], the European Data Regulation [Data Act]¹³, and more recently, proposals such as the Regulation on Horizontal Cybersecurity

Gautier, *Droit des Contrats Spéciaux*, LGDJ, 11^e édition, Paris, 2020, p. 56.

⁸ Regarding the incompatibility of the right of ownership (in its traditional sense) with digital values, see Andreas Rahmatian, *Debts, Money, Intellectual Property, Data and the Concept of Dematerialised Property*, in *Journal of Intellectual Property, Information Technology, and Electronic Commerce Law* no. 11/2020, p. 186 and following. See also Johan David Michels, Christopher Millard, *Mind the Gap: The Status of Digital Files Under Property Law*, Legal Studies Research Paper no. 317/2019, the document is available online at the address: <https://ssrn.com/abstract=3387400>, date of last access: 1st of Mars 2024.

⁹ For more details regarding the notion of ‘digital content’ and that of ‘digital services], see Ionuț Florin Popa, *Furnizarea și conformitatea conținutului digital sau serviciului digital*, in *Revista Română de Drept privat* nr. 1/2022, pp. 229–271; Sorana Suci, *Conformitatea conținutului digital. Noi instrumente legislative europene*, in *Revista Română de Drept Privat* nr. 1/2021, pp. 704–728.

¹⁰ Reiner Schulze, Dirk Staudenmayer, *EU Digital Law. Article-by-Article Commentary*, Hart Publishing-C.H. Beck-Nomos, Oxford-New York-Baden-Baden-München, 2020, p. 100; The same idea in Sorana Suci, *op. cit. (Conformitatea conținutului digital. Noi instrumente legislative europene)*, pp. 721–722.

¹¹ 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), JO L 119 of 4th of May 2016, pp. 1–88, further referred to as ‘GDPR’.

¹² Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs, OJ L 111 of 5th of May 2009, p. 16–22 (The Software Directive).

¹³ Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act), JO L of 22nd of December 2023.

Requirements for Products with Digital Elements [EU Cyber Resilience Act]¹⁴ and the Regulation on Artificial Intelligence [EU Artificial Intelligence Act]¹⁵. All of these directly impact the digital contract. The challenge lies precisely in the patchwork application of the law in the realm of the supply of digital content and services.

Among the numerous facets of the digitalization of contract law, equally captivating, we focus on one in particular: the effects of personal data processing upon the digital contract.

The subject holds particular interest because the DCD expressly recognizes that the digital content and services are supplied in exchange for the processing of personal data [art. 3 para. (1) 2nd provision DCD]. While the contract for supply of digital content may not be considered a sales contract, it nonetheless adheres to its structure, essentially functioning as a synallagmatic contract. In this case, the price is not necessarily the payment of money but rather the supplier's ability to process the personal data of the consumer.

Although DCD provides that it shall be without prejudice to GDPR [art. 3 para. (8) Second provision DCD], the contractual effects of the data subject's consent remain unclear. As we will see in the following sections, the will of the consumer plays a dual role: firstly, the *contractual consent*, necessary for the validity of the contractual agreement, and secondly, the *GDPR consent*, necessary to authorize the processing of personal data [section I].

We pose a predictable question: what role does the *GDPR-consent* play in the digital contract? [Section II]. Having formulated a potential answer, we are equally interested in what happens to the digital contract when the *GDPR consent* is withdrawn under the terms of art. 7 para. (3) of the Regulation, particularly when personal data serves as the sole consideration for the supply for digital content or service [section III].

We address the given hypotheses by trying to coherently apply civil and European law principles, aiming to elucidate the complex e-commerce legislation. However, despite the flexibility of private law, we assert that the digital market requires to enhance consumer protection mechanisms that should extend beyond the non-patrimonial-oriented protection provided by the GDPR Regulation¹⁶.

¹⁴ Proposals for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020, of 15th of September 2022, COM (2022) 454 final.

¹⁵ Proposals for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act), of 21st of April 2021, COM (2021) 206 final.

¹⁶ The need to protect the consumer through two layers, one of personal data protection and the other of contractual obligations, was illustrated in Carmen Langhanke, Martin Schmidt-Kessel, *Consumer Data as Consideration*, in Journal of European Consumer and Market Law no. 6/2015, p. 218 and following.

2. Data subject's consent: between authorization of personal data processing and *ad validitatem* condition

1. *Contractual-consent*. The consent of the parties lies at the heart of the contract, defined as a meeting of the minds [1,166 Civil Code] or as a mutual assent¹⁷. The meeting of the minds is recognized as the central point of the contract in comparative law¹⁸, in European codifications without legal force¹⁹ and in positive European law²⁰.

The internal will, crucial in forming the contract, consists of a fusion of consent and contractual cause. In this framework, the absence of either component results in a lack of an agreement. Thus, the serious, free, and informed consent generates obligations and leads to the primary effect: the binding force of the contract [art. 1,270 para. (1) C. civ.]. This implies that neither party can unilaterally withdraw his or her consent, as embodied in the principle of contractual symmetry [art. 1,270 para. (2) C. civ.] or in the principle of irrevocability of the unilateral legal act. Civil law recognizes this as a fundamental condition for the validity of a contract; thus we refer to it as *contractual consent*.

2. *GDPR consent*: On the other hand, the consent granted by the data subject for the processing of personal data [art. 6 para. (1) lit. a) and art. 7 GDPR] differs from what we qualified as contractual consent.

In private law, beyond its primary definition as codified information²¹, the concept of 'data'²² is used to denote a good or commodity that serves as the subject of legally binding relationships²³. Indeed, data has been characterized as alienable and appropriable intangible assets²⁴. The possession of data involves

¹⁷ See Liviu Pop, Ionuț-Florin Popa, Stelian Ioan Vidu, *Drept civil. Obligațiile*, 2nd ed., Universul Juridic, Bucharest, 2020, pp. 31-32.

¹⁸ See Reiner Schulze, Fryderyk Zoll, *European Contract Law. Second Edition*, C. H. Beck-Hart-Nomos, Baden-Baden, 2018, pp. 25-29.

¹⁹ Art. II. -1:101 DCFR. See Reiner Schulze, Fryderyk Zoll, *op. cit.*, p. 40.

²⁰ The contract as a concordant agreement of wills is illustrated by the Court of Justice of the European Union in the case of Rudolf Gabriel C-96/00, ECLI:EU:C:2002:436, para. 49. See Reiner Schulze, Fryderyk Zoll, *op. cit.*, p. 26. Also see Sorana Suci, *op. cit. (Reflecții asupra contractului digital)*, p. 392.

²¹ About data understood as encoded information, see Sorana Suci, *op. cit. (Reflecții asupra contractului digital)*, p. 396 and following.

²² Recently, the notion of 'data' received its first definition in European Private Law. According to art. 2 (1) of Regulation (EU) 2023/2854 [Data Act], they represent, '*any digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audio-visual recording*'.

²³ Herbert Zech, *Data as a tradeable commodity* in Alberto de Franceschi (ed.), *European Contract Law and the Digital Single Market*, Intersentia, Cambridge-Antwerp-Portland, 2016, p. 53.

²⁴ From a technical perspective, 'Big Data' refers to databases, meaning collections of information processed in such a way that the result becomes a 'product' or a 'commodity' with economic value. See Alberto de Franceschi, Michael Lehmann, *Data as Tradeable Commodity and New Measures for their Protection*, in Italian Law Journal no. 1/2016, Vol. 1. The document is available online at the address: https://www.theitalianlawjournal.it/data/uploads/pdf/1_2014/data-as-tradeable.pdf.

access to information (*usus*), the utilization involves processing (*fructus*), and disposal implies the right to erase them (*abusus*)²⁵. The economic value of data processing stems from its utility; thus, we distinguish between raw data and the information it carries. In the context, the purpose of data use is to process raw data in order to extract economically exploitable information.

Personal data constitute a special category of data, since their protection was given the status of a fundamental right [as outlined in art. 8 para. (1) of the Charter of Fundamental Rights of the European Union and art. 16 of the Treaty on the Functioning of the European Union (TFEU)]²⁶. Indeed, precisely this need for non-patrimonial protection urged the adoption of the GDPR. Given that the non-monetary aspect of personal data is the sole focus of this regulatory instrument, the consent of the data subject plays a central role in the processing of their personal data²⁷.

Thus, consent holds the power to legitimize data processing, a significant force which stems from the broad language of art. 6 para. (1) a) GDPR²⁸, which grants individuals the authority to allow the usage of their data, ‘for any specific purpose’²⁹. The person’s ability to dispose of their own personal data derives from the subjective and discretionary nature of the right to data protection, derivative of the non-patrimonial personality rights. As an expression of the personality right, approving the processing of personal data has a protective function, the act of authorization being essentially revocable [art. 7 para. (3) GDPR]³⁰. However, since consent for data processing constitutes a unilateral and independent legal

date of last access: 29th of February 2024.

²⁵ Herbert Zech, *op. cit.*, p. 56.

²⁶ It has been argued that this protection is rather allocated to the individual, and not to personal data. In reality, the person is the one protected against violations through the exploitation of personal data. See Herbert Zech, *op. cit.*, p. 66.

²⁷ Art. 4 points 11 GDPR: ‘“consent” of the data subject means any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her’.

²⁸ Art. 6 para. (1) a) GDPR: ‘Processing shall be lawful only if and to the extent that at least one of the following applies a) the data subject has given consent to the processing of his or her personal data for one or more specific purpose.’

²⁹ However, data processing must remain within the limits imposed by public order and good morals. In this regard, art. 5 para. (1) (b) GDPR stipulates the requirement that the purpose of the processing must be specific, explicit, and legitimate, while recital [39] establishes that ‘Any processing of personal data should be lawful and fair’.

³⁰ This non-patrimonial right is found in domestic law provisions such as art. 58 Civil Code referring to the respect owed to the human being and its inherent rights. Debates regarding the legal nature of personal data and correlative rights are numerous, ranging from their qualification as derivatives of the non-patrimonial right of personality to their qualification as proprietary rights, similar to intellectual property rights. See Martin Schmidt-Kessel, *The Processing of Personal Data. Consent for the Processing of Personal Data and its Relationship to Contract*, in Alberto De Franceschi, Reiner Schulze, ‘Digital Revolution – New Challenges for Law’, C. H. Beck-Nomos, München, 2019, p. 79. For the same idea, see Herbert Zech, *op. cit.*, p. 66.

act, it must adhere to the general conditions for the validity of a legal act: capacity, consent, object, and cause³¹.

In the context of digital contracts, we witness the transgression of the person's right to dispose of their own personal data from the plan of non-patrimonial rights that enjoy protection to that of patrimonial rights³². This transition introduces uncertainties concerning the role of the data subject's consent in the performance of contractual obligations.

3. *The distinction*: The confusion between *contractual consent* and *GDPR consent* arises from the external manifestation of will because both declarations of the consumer (the actual data subject) occur simultaneously and through the same means. In electronic contracts, the formation of the contract typically occurs through actions such as ticking boxes just by clicking them³³. However, the GDPR, in art. 7 para. (2), stipulates that the consent for the processing of personal data must be given in a written form and separated from other potential aspects for which the data subject is required to give consent.

From the perspective of the internal will, it is certain that the two serve different purposes: while GDPR consent legitimizes data processing, contractual consent legally binds the data subject³⁴. Thus, GDPR-consent alone does not establish the agreement that caused the processing of personal data.

Due to the separation of these two, the consumer, being both a data subject and a contractual party, should not face any contractual consequences when GDPR consent is absent, invalid or withdrawn. It has even been argued that the consent for personal data processing, unlike contractual consent, binds the consumer through a natural obligation derived from the right to dispose of their personal data as there is no enforcement of this obligation³⁵.

However, despite its optional and non-patrimonial nature, GDPR consent is meant to fulfil the legal requirements for data processing without which the provider cannot process personal data. As we will explore, although they serve different functions, these two forms of consent are in a symbiotic relationship, hence the absence or withdrawal of the consent to process personal data significantly impacts the fate of the contract.

³¹ In the sense that the data processing agreement is just apparently a unilateral legal act, see Lucian Bercea, *Standardul 'consumatorului mediu' și consimțământul pentru prelucrarea datelor cu caracter personal*, in *Revista Română de Drept Privat* No. 1/2018, p. 41.

³² See Rolf H. Weber, *Data Protection in the Termination of Contract*, in Reiner Schulze, Dirk Staudenmayer, Sebastian Lohsse (eds.), 'Contracts for the Supply of Digital Content: Regulatory Challenges and Gaps. Münster Colloquia on EU Law and the Digital Economy II,' Nomos-Hart Publishing, Baden-Baden, 2017, p. 194.

³³ Known as '*click-wrap contracts*'. See Rodrigo Momberg, *Standard Terms and Transparency in Online Contracts*, in Alberto De Franceschi (ed.), 'European Contract Law and the Digital Single Market. The Implications of the Digital Revolution,' Intersentia, Cambridge-Antwerp-Portland, 2017, pp. 189–207.

³⁴ Martin Schmidt-Kessel, *op. cit.*, p. 77.

³⁵ In this context, it has been argued that the disposal right upon personal data is 'almost perfect'. See Martin Schmidt-Kessel, *op. cit.*, p. 78.

3. The role of the consent given to personal data processing in synallagmatic digital contracts

We therefore admit that the consent for the processing of personal data, as outlined in art. 6 para. (1) a) GDPR, exerts influence on the digital contract. Since GDPR consent is a legal act, distinct from the contract, it follows its own autonomous legal regime, through its own conditions of validity³⁶. For example, according to art. 8 para. (1) GDPR, individuals under the age of 16 cannot provide consent for personal data processing; thus, consent must be given by the holder of parental responsibility³⁷. Also, GDPR consent is deemed freely given only when the individual is adequately informed in advance on the scope of personal data processing, as prescribed by arts. 12–14GDPR³⁸.

As it differs from contractual consent, the absence of GDPR consent should not affect the fate of the contract. Thus, the invalidity of GDPR consent should not impact the validity of the contract. The contract should remain valid and the obligations stemming from its binding nature remain enforceable. Following this logic, the supplier must continue to perform its obligation to supply, even though the consumer has not validly given his consent to the processing of his personal data.

The conclusion may be theoretically correct but pragmatically the separation of the two does not work. Therefore, we must distinguish between two models of personal data processing: essential processing of personal data (1); non-essential processing of personal data (2).

(1) *Essential processing of personal data*. When the processing of personal data is essential for the performance of a contract, the informed consent of the data subject is not required [art. 6 para. (1) b) GDPR]. Therefore, the provider does not need to seek or obtain consent to process personal data.

In the case of a supplier of an e-book, he must collect personal data in order to deliver the e-book, such as the e-mail address of the consumer. Without this information, the provider does not know the party's address and, thus, cannot fulfil its obligation to provide the electronic copy of the book. This exemplifies

³⁶ In the sense that the consumer's declaration of consent is based on a contractual mechanism, see Lucian Bercea, *op. cit.*, p. 42.

³⁷ Art. 8 para. (3) GDPR provides that this rule 'shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child'. It is worth noting that under Romanian civil law, the contract itself will be valid even when consent is given by a minor under 16 years old, having limited capacity to exercise rights, if the act is authorized by the parents or the custodian (tutor) [art. 41 para. (2) C. civ.].

³⁸ See recital [42] GDPR: 'Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.' See also recital [32] GDPR: 'Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her' and 'when the processing has multiple purposes, consent should be given for all of them'.

the *essential processing of personal data*.

It is sufficient for the data subject to express consent to the formation of the contract to legitimate the personal data processing³⁹. The absence of explicit consent for data processing is irrelevant and any refusal to process them does not invalidate the contract. Of course, failure to provide these personal data at the contract formation stage means that the legal agreement will not be established. This is because the digital architecture of the IT systems is designed in such a way that failure to give these personal data prevents the user from pressing the subscription button, which would otherwise signify acceptance of the contractual offer.

(2) *Non-essential processing of personal data*. The reality shows us that, most common, the supplier of digital content and services also processes personal data that is not necessary for the supply of the digital content or digital service.

In the example from point (1), the supplier of the e-book, acting both as a contractual party and a personal data controller, collects personal data from the buyer for purposes beyond the actual performance of the contract. These purposes may include gathering information about the buyer's literary preferences, about the spoken languages, or geographical location. The collection of this information is not necessary for providing the e-book, as it can be delivered without such details. In this case we are dealing with non-essential processing of personal data.

When the supplier processes personal data that is not necessary for the performance of the contract, according to art. 6 para. (1) a) GDPR, the supplier has the obligation to obtain informed consent for the processing of personal data.

Almost without exception, the suppliers of digital content and services reserve their right to process personal data beyond what is strictly necessary. This applies to various services such as online streaming, cloud storage, social platforms, user-generated content services and finally, all applications that offer *software-as-a-service* solutions⁴⁰. In practice, suppliers' contractual terms often condition the supply of digital content and services on the consent to the processing of personal data.

The European Union has accepted data trading as a new business model and acknowledged the inherent patrimonial value of personal data. Art. 3 par (1) 2nd provision DCD⁴¹ confirms the empirical reality of contracts where an individual's consent for data processing constitutes the very object of the obligation, or

³⁹ This is also the case of supply by downloading of free open-source software, when any data collected and processed is strictly for the purpose of performing the supply (i.e. Adobe Acrobat Reader). Art. 3 para. (1) DCD expressly excludes it from its scope. See also recital [32] DCD.

⁴⁰ For example, Google, Facebook, Twitter, YouTube, Spotify, Netflix, and others. They apparently offer free digital services for which the consumer pays by giving their consent for personal data processing for various purposes, ranging from simple service optimizations to personalized advertising, profiling, or transferring data to other entities.

⁴¹ Art. 3 para. (1) DCD: *'This Directive shall also apply where the trader supplies or undertakes to supply digital content or a digital service to the consumer, and the consumer provides or undertakes to provide personal data to the trader, except where the personal data provided by the consumer*

more precisely, the consideration for digital supply.

Therefore, the European legislator distinguishes between contracts in which personal data processing constitutes the consideration for the supply of digital content or service and those that are supplied free of charge, wherein data processing is strictly necessary for the supply of the digital content or service. The latter are excluded from the scope of DCD⁴².

In fact, the DCD regulates only the onerous contracts, as indicated by art. 3 para. (1) and para. (5) f) DCD, which excludes from its scope the operating systems offered by the supplier under a free open-source license. Therefore, it is unsurprising that the DCD exclusively regulates the supply of digital content or digital services in exchange for money or for the right to process personal data that are not essential for the performance of the contract⁴³. In the latter case, data processing effectively serves as the price of the supply of digital content or service, thereby conferring an onerous character upon the contract.

The provisions of the DCD are in line with what was already recognized by the GDPR. Art. 6 para. (1) (b) GDPR exempts from the rule of explicit consent those contracts also exempted by art. 3 par (1) 2nd DCD from its scope, namely that in which data processing is strictly necessary for the performance of the contract⁴⁴. In addition, art. 7 para. (4) GDPR also distinguishes between essential and non-essential personal data processing. The differentiation is significant in evaluating the voluntary and informed nature of GDPR consent⁴⁵.

Let us consider an example: an application offering navigation and traffic warning services based on crowdsourcing. Because this service relies on real-time information provided by users, the supplier processes personal data including names, email addresses, device locations, reasons for traffic stops, and commonly travelled routes. Given the digital service's nature, the application could not function without user-provided information that often represents personal data. However, data collection extends beyond contract performance as the supplier reserves the right to process collected data for other purposes such as marketing profiling. These additional processing purposes, exceeding what's strictly

are exclusively processed by the trader for the purpose of supplying the digital content or digital service in accordance with this Directive or for allowing the trader to comply with legal requirements to which the trader is subject, and the trader does not process that data for any other purpose.'

⁴² See also Sorana Suciuc, *op. cit.* (*Conformitatea conținutului digital. Noi instrumente legislative europene*), pp. 724-725.

⁴³ Fryderyk Zoll, *Personal Data as Remuneration in the Proposal for a Directive on Supply of Digital Content*, in Reiner Schulze, Dirk Staudenmayer, Sebastian Lohsse (eds.), 'Contracts for the Supply of Digital Content: Regulatory Challenges and Gaps. Münster Colloquia on EU Law and the Digital Economy II', Nomos-Hart Publishing, Baden-Baden, 2017, p. 181.

⁴⁴ *Ibidem*, p. 183.

⁴⁵ Art. 7 para. (4) GDPR: '*When assessing whether consent is freely given, the utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.*'

necessary for contract performance, require express consent for data processing under art. 6 para. (1) a) GDPR.

We can assert that, most of the time, when data processing is not essential to fulfil the contract's function, it constitutes genuine consideration for the digital content or services. In this scenario, the individual's consent for data processing aligns with that expressed in the contractual agreements⁴⁶ and is akin to the notion of 'cause' used in civil law legal systems or the notion of 'consideration' used in Anglo-Saxon legal systems⁴⁷.

Therefore, while the general rule is the independence between the consent for personal data processing and the consent for the formation of the contract, they establish a dependency relationship when the digital content or service is supplied in exchange of personal data.

Consequently, the person's consent not only satisfies the legal requirements imposed by the GDPR but also signifies the internal will which is necessary for the conclusion of the contract.

4. Contractual effects of the withdrawal of consent for the processing of personal data

We explained that, as a rule, contractual consent and GDPR consent are distinct. However, in digital contracts where personal data processing constitutes the supplier's remuneration, the two are interdependent. What happens if the consent for data processing is withdrawn during the performance of the contract?

Art. 7 para. (3) GDPR provides consumers with the optional right to withdraw their consent for the processing of their personal data at any time. In the silence of the European legislator, there could be a potential conflict between the discretionary right to withdraw consent for data processing and the general principle of the binding force of contracts, which is present in most legal systems in Europe⁴⁸. This issue requires further preliminary observations.

The first observation is that the DCD acknowledges its subsidiary nature in relation to the GDPR⁴⁹. This means that the provision outlined in art. 7 para. (3) GDPR takes precedence over any rule within the DCD.

The second observation is that the potential conflict arises primarily in synallagmatic contracts, where the consumer's consent to personal data processing is in exchange for the specific contractual performance. In other situations, as mentioned in Section II, the distinction between the binding consent and data processing consent is clearly defined.

Finally, the third observation is that the mutual and interdependent obligation to process personal data lies, not so much in the provision of the personal

⁴⁶ This idea was also emphasized in Lucian Bercea, *op. cit.*, p. 20.

⁴⁷ Reiner Schulze, Dirk Staudenmayer, *op. cit.*, p. 73.

⁴⁸ Herbert Zech, *op. cit.*, p. 68.

⁴⁹ Recital [37] DCD.

data itself, but rather in the consumer's tolerance of data processing. This aspect qualifies the agreement as one with successive performance, although not from the perspective of the action to supply digital content or services, but rather from that of accepting the data processing in return⁵⁰. Additionally, art. 7 para. (3) GDPR stipulates that data processing conducted during the period of consent validity remains in effect. This underscores the future-only effects of consent withdrawal and the validity of data processing carried out during the contract's active period.

Based on these three observations, different opinions were expressed regarding the effect of consent withdrawal on contracts. Some argue that withdrawal of consent leads to the termination of synallagmatic contracts where data processing serves as consideration, as the interdependent obligation disappears, making the supplier find no interest in performing the digital contract⁵¹. Others suggest that withdrawal of consent under art. 7 para. (3) GDPR may not necessarily terminate the contract, due to the separation of the two declarations⁵². According to the latter, exerting the optional right to withdraw consent should justify non-performance⁵³.

We believe that the discretionary nature of the right to withdraw consent should be interpreted in light of the regulation's primary goal: the protection of personal data. It is essential to consider art. 7 para. (3) GDPR from the perspective of safeguarding personal data, rather than focusing on the contractual position of the consumer. Therefore, when a consumer successfully withdraws his consent in accordance with art. 7 para. (3) to protect their personal data, the Regulation's objective is achieved, irrespective of whether the contractual agreement continues.

The withdrawal of consent for personal data processing under art. 7 para. (3) GDPR constitutes a failure to perform the main obligation of the consumer, that of consenting to his personal data being processed. This failure is significant enough for the supplier to lose interest in performing his own obligation, that of supplying digital content or services. While withdrawal of GDPR consent is an optional right from the perspective of personal data protection, it nonetheless represents a failure to perform an obligation, from the contractual standpoint. This failure should be considered unjustified in civil law terms and therefore justifies the supplier to terminate the contract.

In conclusion, we argue that withdrawing consent for personal data processing gives the supplier the right to terminate the digital contract. As data processing transforms the contract from a one-off contract (*uno actu*) to a contract with successive performance, withdrawing GDPR-consent leads to *ex nunc* ter-

⁵⁰ Fryderyk Zoll, *op. cit.*, p. 184.

⁵¹ *Ibidem*.

⁵² Carmen Langhanke, Martin Schmidt-Kessel, *op. cit.*, p. 222.

⁵³ Also see Fryderyk Zoll, *op. cit.*, footnote 17, p. 184.

mination of the contract, only by affecting future personal data processing as otherwise is provided by art. 7 para. (3) GDPR.

On the other hand, although this conclusion is natural from the supplier's perspective, the consumer expects the digital service to be supplied even though they express their intention to withdraw consent for the processing of their data. This expectation is precisely determined by the behaviour of the major companies that provide digital services which, for a long time, have not been transparent about the commercial purpose of their virtual platforms. Through their acts, providers have led consumers to believe that the services are supplied free of charge.

Why is it important? Over time, the use of personal data in marketing profiling purpose has become increasingly aggressive, to the point where, due to the accuracy of the advertisements displayed on virtual platforms, consumers wonder if they are being tracked by major companies, even in the privacy of their own homes⁵⁴. Meanwhile, consumers have become aware of their subjective rights over personal data, especially after the adoption of the GDPR. On the other hand, social or user-generated content platforms have managed to create dependency. As a result, the consumer is no longer willing to give up digital services, but at the same time they expect their personal data not to be used.

For instance, the behaviour of Meta Platforms Inc., which at the beginning of November 2023 decided to condition the supply of its service, either on agreeing to the processing of data for marketing profiling, or on paying a fee of \$251.88 per year, for the access to the platform without personalized advertisements, has sparked widespread outrage⁵⁵. Meta's decision came in response to the Judgment of the Court of Justice of the European Union in the case of Meta Platforms and others, C-252/21⁵⁶, in which the Court ruled, among other things, that the dominant position in the market is an important factor in determining whether consent has indeed been validly freely given⁵⁷. Indeed, Facebook users, accustomed to the illusion of a free digital service, considered to be abusive the act of conditioning the service on consent to processing personal data.

It is precisely the consumer expectation of having the service supplied free of charge that has led some authors to consider that the supplier would not be entitled to terminate the contract when the consumer withdraws his GDPR

⁵⁴ See for example, <https://www.thesun.co.uk/tech/21005595/facebook-listening-conversation-microphone-truth/>, date of last access: 10th of March 2024.

⁵⁵ Known as 'pay or okay' method. NOYB [European Center for Digital Tights] accused Meta of abusive behaviour, even formulating a legal action against the operator for this, considering it illegal under the GDPR. See <https://noyb.eu/en/meta-ignores-users-right-easily-withdraw-consent>, date of last access: 10th of March 2024. See also, <https://www.dataguidance.com/news/austria-noyb-files-complaint-against-meta-over-pay-or>, date of last access: 10th of March 2024.

⁵⁶ Case C-252/21 Meta Platforms and others, EU:C:2023:537.

⁵⁷ However, ECJ argued that art. 6 par. (1) a) and art. 9 par. (2) a) of the GDPR do not prevent the operator of an online social network, which holds a dominant position in the market, from contractual stipulating that users may consent to the processing of personal data. See Case C-252/21 Meta Platforms and others, EU:C:2023:537, par. 154.

consent, arguing that the unilateral right over the data constitutes an excusable event for non-performance for the consumer⁵⁸.

Certainly, neither the GDPR nor the DCD meet the real expectation of the consumer, which is to access free digital services, as we have concluded that the withdrawal of GDPR consent justifies the supplier's decision to terminate the contract. On the other hand, it is evident that the common expectation for major providers to provide digital services for free is unreasonable.

We believe that the protection provided by art. 7 par. (3) GDPR should be understood in conjunction with the supplier's duty to transparently and coherently inform the consumer regarding the limits of this subjective right over their personal data, especially regarding the purpose and means of processing personal data. Indeed, The Court of Justice of the European Union explained in Case *Meta Platforms and others* that users of digital services must have the freedom to refuse the processing of personal data, even to opt to withdraw consent only for specific data processing purposes, without being obliged to give up to the digital service itself. However, the Court has not recognized a consumer's right to free services⁵⁹. According to the Court, it is sufficient for the supplier to offer the consumer, in case of withdrawal of GDPR consent, an equivalent alternative digital service, that is not accompanied by such processing of personal data, but is provided in exchange for compensation⁶⁰.

If the consumer is unwilling to allow the use of data and also unwilling to pay the price, the supplier's decision to terminate the contract is justified. Ultimately, the market for digital assets and services is governed by the rule of contractual freedom whereas consumer protection norms are intended to maintain balance in the contract between parties and not to inhibit the market of these fabulous new emerging technologies.

5. Concluding remarks

When discussing the processing of personal data, interference with contract law is inevitable. However, neither GDPR nor DCD address directly the effects of personal data processing on the digital contract. The connection between the two commence from the consent of the natural person which, in contract law, provides the contract with a binding force, whereas in personal data protection law, authorize the processing of personal data.

While the external manifestation of suggests a similarity between them, consent for personal data processing is distinct from consent as a condition for the validity of a contract. Generally, failure to comply with data protection regulations or withdrawal of consent does not affect the contract's binding force. However, there's a notable exception: the digital contracts where personal data

⁵⁸ *Supra*, footnote 51.

⁵⁹ Case C-252/21 *Meta Platforms and others*, EU:C:2023:537, par. 150.

⁶⁰ Case C-252/21 *Meta Platforms and others*, EU:C:2023:537, par. 150.

processing constitutes the mere consideration of the contract. In such cases, the agreement for data processing serves as the consideration for the supplier's obligation, making it indispensable for the contract enforceability. Consequently, withdrawing consent for personal data processing, as permitted under art. 7 para. (3) GDPR can implicitly influence the contract for the supply of digital content or services and potentially lead to its termination.

Bibliography

1. Bercea, Lucian: *Standardul 'consumatorului mediu' și consimțământul pentru prelucrarea datelor cu caracter personal*, in *Revista Română de Drept Privat* no. 1/2018.
2. De Franceschi, Alberto & Michael Lehmann: *Data as Tradeable Commodity and New Measures for Their Protection*, in *Italian Law Journal* no. 1/2016, Vol. 1. The document is available online at the address: https://www.theitalian-lawjournal.it/data/uploads/pdf/1_2014/data-as-tradeable.pdf.
3. Langhanke, Carmen & Martin Schmidt-Kessel: *Consumer Data as Consideration*, in *Journal of European Consumer and Market Law* no. 6/2015.
4. Malaurie, Philippe, Laurent Aynès & Pierre-Yves Gautier: *Droit des Contrats Spéciaux*, LGDJ, 11^e édition, Paris, 2020.
5. Michels, Johan David & Christopher Millard: *Mind the Gap: The Status of Digital Files Under Property Law*, *Legal Studies Research Paper* no. 317/2019. The document is available online at the address: <https://ssrn.com/abstract=3387400>.
6. Momberg, Rodrigo: *Standard Terms and Transparency in Online Contracts*, in Alberto De Franceschi (ed.), „European Contract Law and the Digital Single Market. The Implications of the Digital Revolution,” Intersentia, Cambridge-Antwerp-Portland, 2017.
7. Pop, Liviu, Ionuț-Florin Popa & Stelian Ioan Vidu: *Drept civil. Obligațiile*, 2nd ed., Universul Juridic, Bucharest, 2020.
8. Popa, Ionuț Florin: *Furnizarea și conformitatea conținutului digital sau serviciului digital*, in *Revista Română de Drept privat* no. 1/2022.
9. Rahmatian, Andreas: *Debts, Money, Intellectual Property, Data and the Concept of Dematerialised Property*, in *Journal of Intellectual Property, Information Technology, and Electronic Commerce Law* no. 11/2020.
10. Savin, Andrej: *Harmonising Private Law in Cyberspace: The New Directives in the Digital Single Market Context*, *Copenhagen Business School Law Research Paper Series* no. 19–35/2019. The document is available online at the address: <https://ssrn.com/abstract=3474289>.
11. Schmidt-Kessel, Martin: *The Processing of Personal Data. Consent for the Processing of Personal Data and its Relationship to Contract*, in Alberto De Franceschi, Reiner Schulze, „Digital Revolution – New Challenges for Law”, C.H. Beck-Nomos, München, 2019.
12. Schulze, Reiner & Dirk Staudenmayer: *EU Digital Law. Article-by-Article Commentary*, Hart Publishing-C.H. Beck-Nomos, Oxford-New York-Baden-Baden-München, 2020.
13. Schulze, Reiner & Fryderyk Zoll: *European Contract Law. Second Edition*, C. H. Beck-Hart-Nomos, Baden-Baden, 2018.

14. Suciu, Sorana: *Conformitatea conținutului digital. Noi instrumente legislative europene*, in Revista Română de Drept privat no. 1/2021.
15. Suciu, Sorana: *Reflecții asupra contractului digital*, in Revista Română de Drept Privat no. 2/2022.
16. Terré, François, Philippe Simler, Yves Lequette & Chénéde François: *Droit civil. Les obligations*, 13^e édition, Dalloz, Paris, 2022.
17. Weber, Rolf H: *Data Protection in the Termination of Contract*, in Reiner Schulze, Dirk Staudenmayer, Sebastian Lohsse (eds.), 'Contracts for the Supply of Digital Content: Regulatory Challenges and Gaps. Münster Colloquia on EU Law and the Digital Economy II', Nomos-Hart Publishing, Baden-Baden, 2017.
18. Zech, Herbert: *Data as a tradeable commodity* in Alberto de Franceschi (ed.), *European Contract Law and the Digital Single Market*, Intersentia, Cambridge-Antwerp-Portland, 2016.
19. Zoll, Fryderyk: *Personal Data as Remuneration in the Proposal for a Directive on Supply of Digital Content*, in Reiner Schulze, Dirk Staudenmayer, Sebastian Lohsse (eds.), 'Contracts for the Supply of Digital Content: Regulatory Challenges and Gaps. Münster Colloquia on EU Law and the Digital Economy II', Nomos-Hart Publishing, Baden-Baden, 2017.

Artificial Intelligence Regulation: Approaches and Implications

PhD. student **Gabriel NIȚĂ**¹

Abstract

The complexity of technological risks and cyber security risks with a major significant impact on fundamental rights and freedoms arising from the adoption of new artificial intelligence technologies calls for the implementation of specific regulations adapted to the rapid pace of technological innovation and the continuous evolution of threats in this area. The proposed study will focus both on the critical analysis of the regulatory and institutional instruments for regulating artificial intelligence as one of the so-called disruptive technologies and on the challenges faced by regulators. Methodologically, the research will involve the identification and analysis of the risks associated with AI technology, followed by a systematic assessment of the mandatory (hard law) and non-mandatory (soft law) legal instruments applicable to the field, as well as proposed governance system proposals, in order to identify similarities and juxtapositions. In addition, synthesising the views expressed in legal doctrine will make an important contribution to analyse and understand the challenges to regulation and governance posed by new digital technology. By analysing from different perspectives, the proposed regulations to prevent risks associated with artificial intelligence, the scientific contribution brings into question possible directions for the future regulatory framework.

Keywords: artificial intelligence, risk, regulation, ethics, governance.

JEL Classification: K24, K33

DOI: <https://doi.org/10.62768/ADJURIS/2024/1/10>

Please cite this article as:

Gabriel Niță, „Artificial Intelligence Regulation: Approaches and Implications”, in Pajuste, Tiina, Heliona Bellani (Miço) & Sejla Maslo Cerkic (eds.), *Legal Perspectives in the Modern Era of Technological Transformations*, ADJURIS – International Academic Publisher, Bucharest, Paris, Calgary, 2024, p. 154-176.

1. Introduction

Artificial intelligence technology is a catalyst for the ‘*fourth industrial revolution*’², as the digital revolution has been called, being a central element of the digital transformation of society, representing a cultural change as much as a

¹ Gabriel Niță - Faculty of Law, „Babeș-Bolyai” University of Cluj-Napoca, Romania, gabriel.nita@law.ubbcluj.ro.

² The concept introduced by Klaus Schwab in *The Fourth Industrial Revolution*, World Economic Forum, 2016, the document is available online at https://law.unimelb.edu.au/__data/assets/pdf_file/0005/3385454/Schwab-The_Fourth_Industrial_Revolution_Klaus_S.pdf, accessed on 27.02.2024.

technical one³. Recent studies⁴ note the potential of artificial intelligence technology to grow the global economy, with an estimated total economic impact by 2030 of \$15.7 trillion (representing a 14% increase in global GDP), but this will require strategic investment in different types of artificial intelligence technologies.

The main feature of artificial intelligence technology is to solve tasks typical of human behaviour by applying algorithmic programs (analytical, predictive, classification) to large volumes of computer data (including both personal and non-personal data). Artificial intelligence applications are designed to operate with different levels of autonomy. In practice, they improve the speed, accuracy and effectiveness of human efforts and are used in most fields. Artificial intelligence systems can be software only, operating in the virtual world (e.g. voice assistants, image analysis software, search engines, voice or facial recognition systems) or artificial intelligence can be embedded in hardware devices (e.g. advanced robots, autonomous vehicles, drones or the Internet of Things/IoT applications)⁵.

As a computing environment, artificial intelligence is both technically and legally complex. From a technical point of view, the architecture of artificial intelligence involves a set of technologies combining IT infrastructure, data, algorithms and computing power. The performance of artificial intelligence is dependent on interaction with other emerging technologies such as Big Data, Cloud Computing or Quantum Computing. From a legal perspective, artificial intelligence is a computing environment that brings new types of threats to the cybersecurity landscape by extending existing threats or introducing new ones⁶. The artificial intelligence environment has allowed cyber actors to expand their attack surface, targeting cyber attacks on artificial intelligence models by exploiting their vulnerabilities affecting the confidentiality, integrity and availability of the data and information systems they interact with. In addition, technological risks related to potential opacity, possible errors, algorithmic discrimination and lack of explainability increase the threat to fundamental rights and freedoms.

³ Ryan Calo, Kate Crawford, *There is a blind spot in AI research*, 'Nature' 538, 2016, pp. 311–313, the document is available online at <https://www.nature.com/articles/538311a>, accessed on 27.02.2024.

⁴ PwC, *Sizing de prize. What's the real value of AI for your business and how can you capitalise?*, 2017, the document is available online at <https://www.pwc.com/gx/en/issues/data-and-analytics/publications/artificial-intelligence-study.html>, accessed on 27.02.2024.

⁵ European Commission, *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, COM (2018) 237 final*, Bruxelles, 25.04.2018, p. 2, the document is available online at <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018DC0237>, accessed on 27.02.2024.

⁶ Pupillo Lorenzo, Fantin Stefano, Ferreira Afonso, Polito Carolina, *Artificial Intelligence and Cybersecurity. Technology, Governance and Policy Challenges*, Centre for European Policy Studies (CEPS), Brussels, 2021, the document is available online at <https://www.ceps.eu/ceps-publications/artificial-intelligence-and-cybersecurity-2/>, accessed on 27.02.2024.

The AI Incident Database⁷ now identifies over 500 cases globally where recently deployed artificial intelligence systems have produced unexpected results in the real world, affecting fundamental rights and freedoms.

Technological and cybersecurity risks arising from the use of artificial intelligence systems have led to an upsurge in the adoption of preventive regulatory frameworks at global, regional, national or sectoral level.

This new technology represents a major advance in the field of technology and is the focus of legal scholarship exploring its legal implications, with previous scholarly approaches generally focusing on a particular study of ethical frameworks or legal mechanisms or the impact on fundamental rights and freedoms, without an integrated approach to the landscape of regulatory and governance frameworks for artificial intelligence, which is absolutely necessary to identify possible overlaps and juxtapositions. This interdisciplinary study takes a comprehensive look at the adequacy and limitations of existing ethical and legal frameworks related to artificial intelligence technology, with the aim of evaluating and improving its associated practices and regulations. The article is further organised as follows: Section 2 examines the regulatory landscape of artificial intelligence, Section 3 will be oriented towards the analysis of the main proposed governance systems with respect to the environment and artificial intelligence technology, in the perspective of preventing risks associated with them, and in the last section we will cover the conclusions of the study.

2. Regulating artificial intelligence

As in the past, uncertainty about the potential impact of new technologies and an existing legal framework not adapted to new socio-technical scenarios has been the main reason for legislative bodies to regulate⁸. The debate on the regulation of artificial intelligence is still fluid globally and legislative initiatives are at an early stage and fragmented.

As a result of technological progress and the growing impact of artificial intelligence on fundamental rights and freedoms, governments and international organisations have begun to focus on establishing ethical and legal frameworks for the use and development of this technology. These initiatives are criticised, on the one hand, for being premature given the early stage of development of the new technology⁹, and, on the other hand, for the unknown and difficult to control

⁷ Sean McGregor, *Preventing Repeated Real World AI Failures by Cataloging Incidents: The AI Incident Database*, the data are available online at <https://incidentdatabase.ai/apps/incidents/>, accessed on 29.02.2024.

⁸ Gary E. Merchant, Braden R. Allenby, Joseph R. Herkert, *The Growing Gap Between Emerging Technologies and Legal-Ethical Oversight*, The International Library of Ethics, Law and Technology, 2011, volume 7, the document is available online at <https://link.springer.com/book/10.1007/978-94-007-1356-7>, accessed on 02.06.2023.

⁹ Calo Ryan, *Peeping HALs: Making Sense of Artificial Intelligence and Privacy*, *European Journal of Legal Studies*, 2010, 2, 3, the document is available online at <https://hdl.handle.net/1814/15123>,

risks¹⁰.

The instruments adopted at the level of international bodies have focused initially on establishing principled ethical standards in the design, development and use of artificial intelligence, and more recently on regulatory and standardisation initiatives based on risk assessment.

Since 2016, there has been a real effervescence in the adoption of ethical frameworks on artificial intelligence from intergovernmental agencies (OECD¹¹, Council of Europe¹², European Union¹³, UNESCO¹⁴, G20¹⁵), government bodies¹⁶,

accessed on 08.06.2023; Gary Marchant, Lucille Tournas, Carlos Ignacio Gutierrez, *Governing emerging technologies through Soft Law: Lessons for Artificial Intelligence*, 07.12.2020, 'Jurimetrics', vol. 61, Issue no. 1 (Fall 2020), the document is available online at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3761871, accessed on 16.01.2023; Ryan Hageman, Jennifer Hudleston, Adam Thierer, *Soft Law for Hard Problems: The Governance of Emerging Technologies in an Uncertain Future*, 'Colorado Technology Law Journal', 05.02.2018, the document is available online at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3118539, accessed on 08.06.2023.

¹⁰ Buiten Miriam, *Towards Intelligent Regulation of Artificial Intelligence*, 29.04.2019, 'European Journal of Risk Regulation' 10(1), 2019, pp. 41–59, the document is available online at <https://www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/towards-intelligent-regulation-of-artificial-intelligence/AF1AD1>, accessed on 13.12.2022.

¹¹ OECD, *Recommendation 0449 of the Council on Artificial Intelligence*, 22.05.2019, the document is available online at <https://oecd.ai/en/assets/files/OECD-LEGAL-0449-en.pdf>, accessed on 06.06.2023.

¹² The Council of Europe, European Commission for the Efficiency of Justice (CEPEJ), *European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment*, the document is available online at <https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c>, accessed on 06.06.2023.

¹³ European Commission, High-Level Expert Group on Artificial Intelligence, *Ethics Guidelines for Trustworthy AI*, 08.04.2019, the document is available online at <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai>, accessed on 29.02.2024.

¹⁴ UNESCO, *Recommendation on the Ethics of Artificial Intelligence*, 23.11.2021, the document is available online at <https://unesdoc.unesco.org/ark:/48223/pf0000381137>, accessed on 06.06.2023.

¹⁵ G20, *G20 AI Principles*, 2019, the document is available online at <https://wp.oecd.ai/app/uploads/2021/06/G20-AI-Principles.pdf>, accessed on 06.06.2023.

¹⁶ UK: House of Lords – Select Committee on Artificial Intelligence, *AI in the UK: ready, willing and able?*, 16.04.2018, the document is available online at <https://publications.parliament.uk/pa/ld201719/ldselect/ldai/100/100.pdf>; Japan: *Social Principles of Human-Centric AI*, 2019, the document is available online at <https://www.cas.go.jp/jp/seisaku/jinkouchinou/pdf/humancentricai.pdf>; China: National Governance Committee for the New Generation Artificial Intelligence, *Governance Principles for the New Generation Artificial Intelligence*, 2019, the document is available online at <http://www.chinadaily.com.cn/a/201906/17/WS5d07486ba3103dbf14328ab7.html>; Australia: Department of Industry, Science and Resources, *Australia's Artificial Intelligence Ethics Framework*, 07.11.2019, the document is available online at <https://www.industry.gov.au/publications/australias-artificial-intelligence-ethics-framework>; The United States: Executive Office of the President, *Executive Order 13960 on Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government*, 03.12.2020, the document is available online at <https://www.federalregister.gov/documents/2020/12/08/2020-27065/promoting-the-use-of-trustworthy-artificial-intelligence-in-the-federal-government>, all accessed on 06.06.2023.

private organisations (IBM¹⁷, Google¹⁸, Microsoft¹⁹, Tencent Institute²⁰), NGOs (Access Now and Amnesty International²¹, UNI Global Union²²) or with the participation of all stakeholders (Asilomar Principles²³, Montreal Declaration²⁴, IEEE²⁵, Beijing Principles²⁶). The vast majority of initiatives come from economically developed countries (the USA, the UK, Japan, Germany, China), with an under-representation of the Global South²⁷.

The report by the UN Secretary-General for Digital Cooperation²⁸ and Algorithm Watch²⁹ cites the existence of more than 160 instruments or mechanisms to regulate the ethics of artificial intelligence globally as the most effective proactive strategy to mitigate the risks posed by new disruptive technology. The plethora of proposed ethical initiatives on artificial intelligence runs the risk of unnecessary repetition and duplication if the different sets of principles are similar, or confusion and ambiguity if they differ³⁰. The landscape of ethical principles

¹⁷ IBM, *Everyday Ethics for Artificial Intelligence*, the document is available online at <https://www.ibm.com/downloads/cas/VDO5W3JK>, accessed on 06.06.2023.

¹⁸ Google, *AI at Google: Our Principles*, 2019, the document is available online at <https://www.blog.google/technology/ai/ai-principles/>, accessed on 06.06.2023.

¹⁹ Microsoft, *Microsoft AI Principles*, 2018, the document is available online at <https://www.microsoft.com/en-us/ai/our-approach?activetab=pivot1%3aprimar5>, accessed on 06.06.2023.

²⁰ Tencent Institute, *Technological ethics at intelligent era – reshape trustworthiness in digital society*, 08.07.2019, the document is available online at <https://tisi.org/10890>, accessed on 06.06.2023.

²¹ Access now, Amnesty International, *The Toronto Declaration*, 16.05.2018, the document is available online at <https://www.amnesty.org/en/documents/pol30/8447/2018/en/>, accessed on 06.06.2023.

²² UNI Global Union, *Top 10 Principles for Ethical Artificial Intelligence*, 2017, the document is available online at http://www.thefutureworldofwork.org/media/35420/uni_ethical_ai.pdf, accessed on 06.06.2023.

²³ The Future of Life Institute, *AI Principles*, 11.08.2017, the document is available online at <https://futureoflife.org/open-letter/ai-principles/>, accessed on 06.06.2023.

²⁴ *Montreal Declaration for a Responsible Development of Artificial Intelligence*, 2018, the document is available online at https://www.montrealdeclaration-responsibleai.com/_files/ugd/ebc3a3_5c89e007e0de440097cef36dcd69c7b0.pdf, accessed on 06.06.2023.

²⁵ The Institute of Electrical and Electronics Engineers, *Ethically Aligned Design*, 2019, the document is available online at <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=93986> 13, accessed on 06.06.2023.

²⁶ Beijing Academy of Artificial Intelligence, *Beijing AI Principles*, 28.05.2019, the document is available online at <https://link.springer.com/content/pdf/10.1007/s11623-019-1183-6.pdf>, accessed on 06.06.2023.

²⁷ Schiff Daniel, *What's Next for AI Ethics, Policy, and Governance? A Global Overview*, the document is available online at <https://aies-conference.com/2020/wp-content/papers/030.pdf>, accessed on 29.02.2024.

²⁸ United Nations, *Report of the Secretary-General' Roadmap for Digital Cooperation'*, 2020, the document is available online at https://www.un.org/en/content/digital-cooperation-roadmap/assets/pdf/Roadmap_for_Digital_Cooperation_EN.pdf, p. 18, accessed on 06.06.2023.

²⁹ AlgorithmWatch, *AI Ethics Guidelines Global Inventory*, 2020, the document is available online at <https://inventory.algorithmwatch.org>, accessed on 06.06.2023.

³⁰ Floridi Luciano, Cows Josh, *A Unified Framework of Five Principles for AI in Society*, 29.04.2021, the document is available online at <https://papers.ssrn.com/sol3/papers.cfm?abstract>

is vast, but recent studies³¹ show global convergence around the following: transparency, fairness, non-abuse of artificial intelligence, accountability, privacy.

However, the ethical guidelines on artificial intelligence have some limitations in mitigating and preventing the risks associated with the new technology, mainly due to the formulation of sets of principles in too broad terms which may contribute to divergent interpretations³², the lack of balanced participation in their elaboration which may contribute to ‘ethics washing’³³, the lack of legal force to enforce compliance and legal consequences in case of violation³⁴, and the lack of enforcement mechanisms³⁵.

Due to the fact that ethical guidelines cannot provide full legal protection

_id=3831321, accessed on 01.12.2023; Rees Connor, Muller Berndt, *All that glitters is not gold: trustworthy and ethical AI principles*, *AI and Ethics*, 16.11.2022, the document is available online at <https://link.springer.com/article/10.1007/s43681-022-00232-x>, accessed on 30.11.2023.

³¹ Fjeld Jessica, Nele Achten, Hannah Hilligoss, Adam Nagy, Madhulika Srikumar, *Principled Artificial Intelligence: Mapping Consensus in Ethical and Right-based Approaches to Principles of AI*, Berkman Klein Center, Research Publication no. 2020-1, the document is available online at <https://ssrn.com/abstract=3518482>, accessed on 02.12.2023; Jobin Anna, Ienca Marcelo, Vayena Effy, *Artificial Intelligence: the global landscape of ethics guidelines*, 2019, the document is available online at <https://arxiv.org/abs/1906.11668>, accessed on 01.12.2022; Zeng Yi, Enmeng Lu, Cunqing Huangfu, *Linking Artificial Intelligence Principles*, the document is available online at <https://arxiv.org/abs/1812.04814>, accessed on 02.12.2023; Niels van Berkel, Eleftherios Papachristos, Anastasia Giachanou, Simo Hosio, *A systematic Assessment of National Artificial Intelligence Policies: Perspectives from the Nordics and Beyond*, the document is available online at <https://www.researchgate.net/publication/344320861>, accessed on 02.12.2023; Hagendorff Thilo, *The Ethics of AI Ethics. An Evaluation of Guidelines*, 11.10.2019, the document is available online at <https://arxiv.org/abs/1903.03425>, accessed on 30.11.2023; PwC, *Responsible AI – Maturing from theory to practice*, 2021, the document is available online at <https://www.pwc.com/gx/en/issues/data-and-analytics/artificial-intelligence/what-is-responsible-ai/pwc-responsible-ai-maturing-from-theory-to-practice.pdf>, accessed on 06.06.2023.

³² Whittlestone Jess, Rune Nyrup, Anna Alexandrova, Stephen Cave, *The Role and Limits of Principles in AI Ethics: Towards a Focus on Tensions*, AIES '19: Proceedings of the 2019 AAAI/ACM Conference on AI, Ethics, and Society, 2019, pp. 195–200, the document is available online at <https://dl.acm.org/doi/10.1145/3306618.3314289>, accessed on 29.02.2024.

³³ Stix Charlotte, *Actionable Principles for Artificial Intelligence Policy: Three Pathways*, *Science and Engineering Ethics*, 2021, Volume 27, the document is available online at <https://link.springer.com/article/10.1007/s11948-020-00277-3>, accessed on 02.02.2024.

³⁴ Bruschi Danilo, Diomede Nicla, *A framework for assessing AI ethics with applications to cybersecurity*, *AI and Ethics*, 2022, Volume 3, pp. 65–72, the document is available online at <https://link.springer.com/article/10.1007/s43681-022-00162-8>, accessed on 02.01.2022; Stahl Bernd Carsten, Rowena Rodrigues, Nicole Santiago, Kevin Macnish, *A European Agency for Artificial Intelligence: Protecting fundamental rights and ethical values*, *Computer Law & Security Review*, 2022, Volume 45, the document is available online at <https://sciencedirect.com/science/article/pii/S0267364922000097>, accessed on 09.12.2023.

³⁵ Fukuda-Parr Sakito, Gibbons Elisabeth, *Emerging Consensus on 'Ethical AI': Human Rights Critique of Stakeholders Guidelines*, *Global Policy*, 2021, Volume 12, Supplement 6, the document is available online at <https://onlinelibrary.wiley.com/doi/full/10.1111/1758-5899.12965>, accessed on 13.12.2022; Eileen Donahoe, Megan MacDuffee Metzger, *Artificial Intelligence and Human Rights*, *Journal of Democracy*, 2019, Volume 30(2), pp. 115–126, the document is available online at <https://www.proquest.com/docview/2295528777>, accessed on 07.06.2023.

of individual rights and interests against the risks associated with the new technology, there has been an increase in policy-makers' interest in adopting legislation on artificial intelligence. Ethical guidelines and legal regulation are not mutually exclusive but complementary. Legal regulation can provide clarity and a binding legal framework for the implementation of ethical principles.

The Ad hoc Committee on Artificial Intelligence of the Council of Europe, in its studies '*Towards Regulation of AI Systems*' (2020)³⁶ and '*A Legal Framework of AI Systems*' (2021)³⁷, considers that a comprehensive legal framework based on the Council of Europe's human rights standards is needed to fill the substantive and procedural gaps in ethical frameworks. The European Commission, through the *White Paper on Artificial Intelligence – A European Approach to Excellence and Trust, COM(2020) 65 Final*³⁸, proposes a European legal framework for trusted artificial intelligence. In the same vein, there are approaches to the need for federal legislation in the US or primary legislation in the UK.

There are, however, opinions that legal regulation in the field of artificial intelligence is inappropriate given that the law, in general, cannot keep up with technology³⁹, is not precise enough to regulate complex technology and is too inflexible to take into account all possible future developments⁴⁰, as well as due to the lack of expertise in the public sector to coordinate policies aimed at new technology in the industrial sector⁴¹. On the contrary, others⁴² consider that regulation by law is necessary in view of the intensity of the threats posed by artificial intelligence technology and its impact on the rule of law, democracy and human rights.

Many countries globally are developing or adopting specific laws to address the risks associated with artificial intelligence. The overarching theme of

³⁶ The document is available online at <https://edoc.coe.int/fr/intelligence-artificielle/9656-towards-regulation-of-ai-systems.html#>, accessed on 08.06.2023.

³⁷ The document is available online at <https://edoc.coe.int/fr/intelligence-artificielle/9648-a-legal-framework-for-ai-systems.html>, accessed on 08.06.2023.

³⁸ The document is available online at <https://eur-lex.europa.eu/legal-content/RO/TXT/HTML/?uri=CELEX:52020DC0065>, accessed on 08.06.2023.

³⁹ Taihagh Arez, *Assessing the regulatory challenges of emerging disruptive technologies*, 'Regulation & Governance', 2021, Volume 15, pp. 1009–1019, the document is available online at <https://onlinelibrary.wiley.com/doi/epdf/10.1111/rego.12392>, accessed on 16.12.2023.

⁴⁰ Nemitz Paul, *Constitutional democracy and technology in the age of artificial intelligence*, 15.10.2018, 'Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences', Volume 376, Issue 2133 the document is available online at <https://royal.societypublishing.org/doi/epdf/10.1098/rsta.2018.0089>, accessed on 28.02.2024.

⁴¹ Calo Ryan, *Artificial Intelligence Policy: A Primer and Roadmap*, "University of Bologna Law Review", 2018, Volume 3(2), pp. 180–218, the document is available online at <https://doaj.org/article/cc06b2b47fbc4e3d9b6d6835b7fc6bca>, accessed on 23.02.2024.

⁴² Nemitz Paul, *op. cit.*; Clarke Roger, *Regulatory alternatives for AI*, "Computer Law & Security Review", 2019, Volume 35, pp. 398–409, the document is available online at <https://www.science-direct.com/science/article/abs/pii/S0267364919301281>, accessed on 27.12.2023.

the regulations adopted or being adopted globally is to maintain the accountability, transparency and fairness of artificial intelligence. According to the *'2023 AI Index Report'*⁴³ there will be 37 such legislative initiatives in 2022, compared to 2016 when only one legislative proposal was registered.

At the national level, the United States, through the Algorithmic Accountability Act of 2022⁴⁴, requires companies to assess the impact of artificial intelligence. During 2022, the UK has put forward proposals for the future regulation of artificial intelligence⁴⁵ that address future risks and opportunities. In the same year, a regulatory instrument⁴⁶ came into force in China regulating companies' use of algorithms in online recommender systems, requiring such services to be moral, ethical, accountable and transparent. In Romania, a legislative project on the responsible use of technology in the context of the deepfake phenomenon was initiated in 2023, aimed at limiting the use of artificial intelligence in connection with the creation, distribution and storage of digital content⁴⁷.

At European level, the European Commission has published a general proposal for a regulatory framework called the Artificial Intelligence Act⁴⁸. The proposed regulation aims to create a harmonised legal framework in the European Union on the operation and use of artificial intelligence and follows a risk prevention approach: unacceptable risk (new technology poses a clear threat to safety, livelihoods and human rights: artificial intelligence systems that manipulate human behaviour to prevent users from exercising their free will, i.e. those that allow governments to conduct social scoring); high risk (technology is used in areas such as critical infrastructure, educational or vocational training, product safety components, employment, essential public and private services, law enforcement, migration, asylum and border control management, administration of justice and democratic processes), limited risk (applications are subject to specific transparency obligations – e.g. in the case of chatbot users must be aware

⁴³ Stanford Institute for Human-Centered Artificial Intelligence, *2023 AI Index Report*, the data is available online at <https://aiindex.stanford.edu/report/>, accessed on 06.06.2023.

⁴⁴ The document is available online at <https://www.congress.gov/bill/117th-congress/house-bill/6580/text>, accessed on 08.06.2023.

⁴⁵ Department for Science, Innovation and Technology, Office for Artificial Intelligence, *Establishing a pro-innovation approach to regulating AI*, the document is available online at <https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach/white-paper>, accessed on 08.08.2023.

⁴⁶ The Cyberspace Administration of China, *Internet Information Service Algorithmic Recommendation Management Provisions*, the document is available online at <https://digichina.stanford.edu/work/translation-internet-information-service-algorithmic-recommendation-management-provisions-effective-march-1-2022>, accessed on 08.08.2023.

⁴⁷ The document is available online at https://www.cdep.ro/pls/proiecte/upl_pck.proiect?cam=2&idp=20853, accessed on 24.07.2023.

⁴⁸ European Commission, *Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts*, 21.04.2021, the document is available online at <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206>, accessed on 29.02.2024.

that they are interacting with software), minimal risk (rules do not intervene in this case). The proposed Regulation also provides for the creation of a framework for conformity assessment and supervision of compliance with the obligations and requirements imposed on developers and users of artificial intelligence systems.

The proposed new EU regulatory framework for artificial intelligence has been the subject of criticism and debate in the technological and legal community. Some critics⁴⁹ argue that the proposed Regulation could limit innovation and progress of the new technology by placing strict rules and requirements on developers and users. The proposed Regulation focuses on compliance assessment and less on fundamental rights impact assessment⁵⁰, overlaps with Regulation (EU) 2019/881 on cybersecurity⁵¹ in relation to the certification process which may undermine the objectives of the certification mechanisms⁵², i.e. it is not synchronised with the provisions of other EU legislation (such as the GDPR legislation – it does not provide rights for data subjects and authorities were complaints can be lodged). The provisions of the future Regulation only offer providers the possibility to assess risks, there are no provisions for sanctions in case of non-compliance and no authorities to supervise this process⁵³, while compliance of artificial intelligence products with private standards presents risks⁵⁴.

⁴⁹ Mariarosaria Taddeo, *On the Risks of Trusting Artificial Intelligence: The Case of Cybersecurity*, Josh Cowls, Jessica Morley (editors), *The 2020 Yearbook of the Digital Ethics Lab.*, Springer, 2020, pp. 97–108, the document is available online at https://link.springer.com/chapter/10.1007/978-3-030-80083-3_10, accessed on 29.02.2024.

⁵⁰ Smuha Nathalie, Ahmed-Rengers Emma, Harkens Adam, Li Wenlong, MacLaren James, Piselli Riccardo, Yeung Karen, *How the EU can achieve legally trustworthy AI: a response to the European Commission's proposal for an Artificial Intelligence Act*, 05.08.2021, "Artificial Intelligence – Law, Policy & Ethics eJournal", SSRN Network, the document is available online at <https://ssrn.com/abstract=389991>, accessed on 29.12.2023; Lane Lottie, *Clarifying Human Rights Standards through Artificial Intelligence Initiatives*, "International & Comparative Law Quarterly", 2022, Volume 71(4), pp. 915–944, the document is available online at <https://www.cambridge.org/core/journals/international-and-comparative-law-quarterly/article/clarifying-human-rights-standards-through-artificial-intelligence-initiatives/52D69ACE49CE1E0B5D9E69E51CA14690>, accessed on 07.12.2023.

⁵¹ The European Parliament and the Council of the European Union, *Regulation (EU) 2019/881 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)*, the document is available online at <https://eur-lex.europa.eu/eli/reg/2019/881/oj>, accessed on 01.03.2024.

⁵² Federica Casarosa, *Cybersecurity certification of Artificial Intelligence: a missed opportunity to coordinate between Artificial Intelligence Act and the Cybersecurity Act*, "International Cybersecurity Law Review", 2022, Volume 3, pp. 115–130, the document is available online at <https://link.springer.com/article/10.1365/s43439-021-00043-6>, accessed on 09.06.2023.

⁵³ Smuha Nathalie, Ahmed-Rengers Emma, Harkens Adam, Li Wenlong, MacLaren James, Piselli Riccardo, Yeung Karen, *op. cit.*

⁵⁴ Martin Ebers, Veronica R.S. Hoch, Frank Rosenkranz, Hannah Ruschemeier, Björn Steinrötter, *The European Commission's Proposal for an Artificial Intelligence Act – A Critical Assessment by*

As artificial intelligence achieves its goals by processing a large amount of personal data, there is a collision with all the fundamental data protection principles that are laid down in the European General Data Protection Regulation (GDPR) 2016/679⁵⁵, considered to be the first legal instrument applicable to artificial intelligence. At the same time, Directive (EU) 2016/680⁵⁶ and Regulation (EU) 2018/1725⁵⁷ should be mentioned.

Unlike the proposed Regulation establishing harmonised rules on artificial intelligence, the GDPR proposes a framework based on rights rather than risk prevention. Although it does not explicitly refer to artificial intelligence, the GDPR Regulation aims to impose a high standard of personal data protection that may limit the free flow of data that lies at the heart of the development of the new technology⁵⁸.

There are, however, opinions⁵⁹ that GDPR would be incompatible with

members of the Robotics and AI Law Society, "Multidisciplinary Scientific Journal", 2021, Volume 4(4), pp. 589–603, the document is available online at <https://www.mdpi.com/2571-8800/4/4/43>, accessed on 25.11.2023.

⁵⁵ The European Parliament and the Council of the European Union, *Regulation (EU) 2016/679 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 document is available online at <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679>, accessed on 29.02.2024.

⁵⁶ The European Parliament and the Council of the European Union, *Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA*, the document is available online at <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L0680>, accessed on 29.02.2024.

⁵⁷ The European Parliament and the Council of the European Union, *Regulation (EU) 2018/1725 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC*, the document is available online at <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32018R1725>, accessed on 29.02.2024.

⁵⁸ Herve Allan, *Data Protection and Artificial Intelligence*, Shin-Yi Peng, Ching-Fu Lin, Thomas Streinz (editors), Artificial Intelligence and International Economic Law, Cambridge University Press, 2021, pp. 193–214, the document is available online at <https://www.cambridge.org/core/books/artificial-intelligence-and-international-economic-law/data-protection-and-artificial-intelligence/B98076D59C2B75892D58CC11518E2217>, accessed on 19.12.2023.

⁵⁹ Sartor Giovanni, *The impact of the General Data Protection Regulation (GDPR) on artificial intelligence*, the document is available online at [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU\(2020\)641530_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf), accessed on 20.12.2022; Cate Fred, Kuner Christopher, Orla Lynskey, Christopher Millard, Nora Ni Loideain, Dan Jerker B. Svantesson, *Expanding the Artificial Intelligence – Data Protection Debate*, "International Data Privacy Law", 2018, Volume 8, No. 4, pp. 289–292, the document is available online at <https://www.academic.oup.com/idpl/article/8/4/289/5299551>, accessed on 19.12.2023; Paal Boris, *Artificial Intelligence as a Challenge for Data Protection Law*, Silja Voienky, Philipp Kellmeyer, Oliver Mueller, Wolfgang Burgard (editors), *The Cambridge Handbook of Responsible Artificial Intelligence*, Cambridge University Press, 2022, pp. 290–308, the document is available online at <https://www.cambridge.org/core/books/cambridge-handbook-of-responsible-artificial-intelligence/artificial-intelligence->

artificial intelligence, as the EU Regulation is based on principles such as purpose limitations, data minimisation, special treatment of sensitive data, limitation of automated decisions, thus forcing the EU to abandon the application of GDPR. In addition, the GDPR provisions contain specific rules for certain types of automated individual decision-making, but not for collective decisions⁶⁰. From another perspective, the GDPR does not provide for the right to explain all algorithmic decisions, but only those that have a legal or significant effect⁶¹. On the other hand, there are views⁶² that it is possible to implement an interpretation of the GDPR in the case of technologies using artificial intelligence, so as to reconcile both needs: the protection of subjective data, on the one hand, and the development of useful applications on the other.

Standardisation documents are also part of the efforts associated with the challenge of regulating artificial intelligence. At the level of standards development bodies, there is a real effervescence in the preparation of more or less consistent and early-stage guidelines and standards for artificial intelligence. The StandICT report⁶³ identified more than 250 documents in this regard, with the

as-a-challenge-for-data-protection-law/84B9874F94043E8AFC81616A60 BA69CC, accessed on 27.12.2023; Wallace Nick, Castro Daniel, *The Impact of the EU's New Data Protection Regulation on AI*, Centre for Data Innovation, 27.03.2018, the document is available online at <https://www2.datainnovation.org/2018-impact-gdpr-ai.pdf>, accessed on 27.12.2022.

⁶⁰ Zuiderveen Borgesius Frederik, *Strengthening legal protection against discrimination by algorithms and artificial intelligence*, "International Journal of Human Rights", 2020, pp. 1–22, the document is available online at <https://ssrn.com/abstract=3561441>, accessed on 22.12.2023; Castets-Renard Celine, *Accountability of Algorithms in the GDPR and Beyond: A European Legal Framework on Automated Decision-Making*, "Fordham Intellectual Property, Media & Entertainment Law Journal, Futurecoming", 20.05.2019, the document is available online at <https://ssrn.com/abstract=3391266>, accessed on 28.12.2023.

⁶¹ Brkan Maja, Bonner Gregory, *Legal and Technical Feasibility of the GDPR's Quest for Explanation of Algorithmic Decisions: of Black Boxes, White Boxes and Fata Morganas*, "European Journal of Risk Regulation", Volume 11, Issue 1, 2020, pp. 18–50, the document is available online at <https://www.cambridge.com/core/journals/european-journal-of-risk-regulation/article/legal-and-technical-feasibility-of-the-gdprs-quest-for-explanation-of-algorithmic-decision-s-of-black-boxes-white-boxes-and-fata-morganas/7324CDE80A300179C170C5BA8CA7E851>, accessed on 27.12.2023; Sava Ruxandra, *Când decizia o ia mașina ... Despre profilare, drepturi și echilibru într-un univers digital*, "Revista Română pentru Protecția și Securitatea Datelor cu Caracter Personal" NR. 3/2020, the document is available online at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3721413, accessed on 28.12.2023; Wachter Sandra, Mittelstadt Brent, Floridi Luciano, *Why a Right to Explanation of Automated Decision-Making Does Not Exist in General Data Protection Regulation*, "International Data Privacy Law", 2017, the document is available online at <https://ssrn.com/abstract=2903469>, accessed on 23.12.2023; Wachter Sandra, Brent Mittelstadt, Russel Chris, *Counterfactual explanations without opening the black box: automated decisions and the GDPR*, "Harvard Journal of Law and Technology", 2018, Volume 31(2), the document is available online at <https://ssrn.com/abstract=3063289>, accessed on 30.12.2023.

⁶² Mantelero Alessandro, *Artificial Intelligence and Data Protection: Challenges and Possible Remedies*, 25.01.2019, the document is available online at <https://rm.coe.int/artificial-intelligence-and-data-protection-challenges-and-possible-re/168091f8a6>, accessed on 12.12.2023.

⁶³ Lindsay Frost, Ray Walshe, Silvana Muscella, *Report of TWG AI: Landscape of AI Standards*,

International Organisation for Standardisation (ISO), the International Electrotechnical Commission (IEC), the European Telecommunications Standards Institute (ETSI), the Institute of Electrical and Electronics Engineers (IEEE), the International Telecommunication Union (ITU) and SAE International⁶⁴ being very active in this regard and in various stages of development.

The landscape of artificial intelligence regulation is very diverse and still in formation. The global nature of the impact of artificial intelligence requires interstate cooperation and the involvement of all stakeholders, especially as the Global South is underrepresented at this time. Although many policies and governance recommendations have been made, instead of strong government regulation, no concrete set of mechanisms to mitigate the risks of artificial intelligence has emerged and legislation needs to be adapted⁶⁵. There is both a lack of regulation and considerable gaps in what we know and can hope to know about the risks posed by artificial intelligence⁶⁶. On the other hand, over-regulation or excessive regulation can hamper innovation and progress of new technology⁶⁷.

3. Governance of artificial intelligence

Due to the complexity, the accelerated pace of development, the risks to which users are exposed as a result of interaction with artificial intelligence applications, the possibility of use for criminal purposes (fake news, deep fakes, cyber-attacks, terrorism, warfare, manipulation of the population)⁶⁸ and the cross-border nature of cybercrime, it is necessary to ensure an adequate system of governance⁶⁹ of this information environment at the global level.

The challenges of artificial intelligence can only be effectively addressed

20.05.2021, the data is available online at <https://zenodo.org/record/5011179#.YhvgLOjMK5c>, accessed on 19.06.2023.

⁶⁴ For details see ENISA, *Cybersecurity of AI and Standardisation*, 14.03.2023, the document is available online at <https://www.enisa.europa.eu/publications/cybersecurity-of-ai-and-standardisation>, accessed on 15.01.2024.

⁶⁵ Gerard's Janneke, *The fundamental rights challenges of algorithms*, "Netherlands Quarterly of Human Rights", 2019, Volume 37(3), pp. 205–209, the document is available online at <https://journals.sagepub.com/doi/full/10.1177/0924051919861773>, accessed on 07.12.2023.

⁶⁶ James M. White, Rolf Lidskog, *Ignorance and the regulation of artificial intelligence*, "Journal of Risk Research", 2022, Volume 25, Issue 4, pp. 488–500, the document is available online at <https://www.tandfonline.com/doi/full/10.1080/13669877.2021.1957985>, accessed on 03.02.2024.

⁶⁷ Mariarosaria Taddeo, *op.cit.*

⁶⁸ Gomez Rego de Almeida Patricia, Denner dos Santos Carlos, Silva Farias Josivania, *Artificial Intelligence Regulation: a framework for governance*, "Ethics and Information Technology", 2021, Volume 23, pp. 505–525, the document is available online at <https://link.springer.com/article/10.1007/s10676-021-09593-z>, accessed on 13.12.2023.

⁶⁹ For more on the concept of "governance" see Edward (Ted) A. Parson, Richard M. Re, Alicia Solow-Niederman, Elana Zeide, *Artificial Intelligence in Strategic Context: An Introduction*, "UCLA School of Law, Public Law Research Paper", 2019, No. 19–45, the document is available online at <https://ssrn.com/abstract=3476384>, accessed on 18.02.2024.

through international coordination, as its regulation has externalities that go beyond national borders⁷⁰. New governance frameworks can be adapted to approaches taken to regulate previous emerging technologies⁷¹. Given that artificial intelligence is a transformative technology that offers both great benefits and poses a number of challenges, effective governance is important to ensure that ethical concerns and fundamental rights are met.

Artificial intelligence governance is at an early stage⁷², with research results showing a predominance of ethics-oriented systems rather than rule-based systems⁷³.

Soft law is insufficient for reasons such as lack of efficiency (voluntary nature of initiatives cannot ensure that established principles will always be adhered to), not subject to uniform application standards, governments will face the challenge of ensuring consistent application of these guidelines in designing the same AI technologies in different sectors if the principles differ in several guidelines and are not well coordinated with regulations, inability to ensure inclusiveness and representation of different stakeholders, and not subject to public scrutiny⁷⁴. By taking advantage of soft law, leading technology companies can attempt to set the ‘ethical AI’ narrative on their own terms and serve as a shield against regulation (avoiding the introduction of binding legal rules)⁷⁵, concentrating digital power in the hands of a few players (‘Big Five’ — Google, Facebook, Microsoft, Apple, Amazon)⁷⁶.

On the other hand, it is considered necessary to adopt a centralised framework for the governance of artificial intelligence through the adoption of specific

⁷⁰ Olivia Erdelyi, Judy Goldsmith, *Regulating artificial intelligence: Proposal for a global solution*, “Government Information Quarterly”, 2022, Volume 39, Issue 4, the document is available online at <https://www.sciencedirect.com/science/article/abs/pii/S0740624X22000843>, accessed on 27.11.2023.

⁷¹ Gasser Urs, Virgilio A.F. Almeida, *A layered model for AI governance*, “IEEE Internet Computing”, 2017, Volume 21, Issue 6, pp. 58–62, the document is available online at <https://ieeexplore.ieee.org/document/8114684>, accessed on 14.12.2023.

⁷² Butcher James, Beridze Irakli, *What is the State of Artificial Intelligence Governance Globally*, “RUSI Journal”, 2019, Volume 164, Nos 5/6, pp. 88–96, the document is available online at <https://www.researchgate.net/publication/337640603>, accessed on 16.12.2023.

⁷³ Radu Roxana, *Steering the governance of artificial intelligence: national strategies in perspective*, “Policy and Society”, 2021, Volume 40, Issue 2, pp. 178–193, the document is available online at <https://www.tandfonline.com/doi/full/10.1080/14494035.2021.1929728>, accessed on 13.02.2024.

⁷⁴ Taeihagh Arez, *Governance of artificial intelligence*, “Policy and Society”, 2021, Volume 40, Issue 2, pp. 137–157, the document is available online at <https://academic.oup.com/policyandsociety/article/40/2/137/6509315>, accessed on 14.12.2023.

⁷⁵ Vasiliki Koniaku, *From the “rush to ethics” to “race for governance” in Artificial Intelligence*, “Information Systems Frontiers”, 2022, Volume 25, pp. 71–102, the document is available online at <https://link.springer.com/article/10.1007/s10796-022-10300-6>, accessed on 27.02.2024.

⁷⁶ Muller Catelijne, *The impact of Artificial Intelligence on Human Rights, Democracy and the Rule of Law*, 24.06.2020, the document is available online at <https://rm.coe.int/cahai-2020-06-fin-c-muller-the-impact-of-ai-on-human-rights-democracy-16809ed6da>, accessed on 17.12.2023.

legislative instruments⁷⁷ (binding legal rules) and governmental institutions⁷⁸, or by adapting existing ones (Global Partnership for Artificial Intelligence, ONE-AI Working Groups adjacent to the OECD Policy Observatory, European Commission – International Alliance for a Human-Centred Approach to Artificial Intelligence), or by creating new ones (creation of a G20 coordination committee⁷⁹, international governance coordination committee for artificial intelligence⁸⁰, international regulatory agency for artificial intelligence⁸¹, institutional alternative of a new ‘Ombudperson’⁸²), to avoid conflicts of jurisdiction, ensure rules on cooperation and accountability or coordination and control institutions.

In the face of concerns generated by the use of artificial intelligence, data governance frameworks⁸³ or forms of ‘hybrid’ governance⁸⁴ (considering the increasing role played by non-state actors) have also been proposed.

Possibly human rights will also serve to guide the development and governance of the new technology⁸⁵. Human rights can complement existing ethics initiatives⁸⁶. International human rights law provides a universally accepted

⁷⁷ Dixon Red Bin Lee, *A principled governance for emerging AI regimes: lessons from China, the European Union, and the United States*, "AI and Ethics", 2023, Volume 3, pp. 793–810, the document is available online at <https://link.springer.com/article/10.1007/s43681-022-00205-0>, accessed on 29.11.2023.

⁷⁸ Stix Charlotte, *Foundations for the future: institution building for the purpose of artificial intelligence governance*, "AI & Ethics", 2022, Volume 2, pp. 463–476, the document is available online at <https://link.springer.com/article/10.1007/s43681-021-00093-w>, accessed on 29.11.2023.

⁷⁹ Thorsten Jelinek, Wendell Wallach, Danil Kerimi, *Policy brief: the creation of a G20 coordinating committee for the governance of AI*, "AI and Ethics", 2021, Volume 1, pp. 141–150, the document is available online at <https://link.springer.com/article/10.1007/s43681-020-00019-y>, accessed on 29.11.2023.

⁸⁰ Wallach Marchant, *An agile ethical/legal model for the international and national governance of AI and robotics*, 2018, the document is available online at https://www.aies-conference.com/2018/contents/papers/main/AIES_2018_paper_77.pdf, accessed on 21.02.2024.

⁸¹ Olivia Erdelyi, Judy Goldsmith, *op. cit.*, p. 9.

⁸² Simon Chesterman, *Weapons of Mass Disruption: Artificial Intelligence and International Law*, "Cambridge International Law Journal", 2021, Volume 10, pp. 181–203, the document is available online at <https://ssrn.com/abstract=3832563>, accessed on 30.11.2023.

⁸³ Janssen Marjin, Brous Paul, Estevez Elsa, Barbosa S. Luis, Janowski Tomasz, *Data governance: Organizing data for trustworthy Artificial Intelligence*, "Government Information Quarterly", 2020, Volume 37, Issue 3, the document is available online at <https://www.sciencedirect.com/science/article/pii/S0740624X20302719>, accessed on 16.12.2023.

⁸⁴ Radu Roxana, *op. cit.*, Taeihagh Arez, *op. cit.*

⁸⁵ Latonero Mark, *Governing Artificial Intelligence: Upholding Human Rights & Dignity*, Data & Society, 2018, the document is available online at <https://datasociety.net/library/governing-artificial-intelligence/>, accessed on 04.12.2023; Smuha Natalie, *Beyond a Human Rights-based to AI Governance: Promise, Pitfalls, Plea*, "Philosophy & Technology", 2021, Volume 34, pp. 91–104, the document is available online at <https://link.springer.com/article/10.1007/s13347-020-00403-w>, accessed on 29.02.2024; Risse Matthias, *Human Rights and Artificial Intelligence: An Urgently Needed Agenda*, "HKS Faculty Research Working Paper Series RWP18-015", 2018, the document is available online at <https://www.hks.harvard.edu/publications/human-rights-and-artificial-intelligence-urgently-needed-agenda>, accessed on 17.12.2023.

⁸⁶ Access now, *Human Rights in the Age of Artificial Intelligence*, 2018, the document is available

framework for analysing, assessing and ultimately remedying the impact of artificial intelligence on individuals and society⁸⁷. A number of arguments⁸⁸ are put forward in support of this governance framework: a) human rights law sets global standards and accountability mechanisms that specify how individuals are entitled to be treated; b) the EU legal order is rooted in constitutional and human rights commitments; c) the well-developed institutional framework through which human rights norms are systematically monitored, promoted and enforced around the world can support/ensure the ethical governance of AI; d) resolution of ethical conflicts can be carried out by judicial institutions (at national or international level) responsible for adjudicating cases involving complaints of human rights violations; e) recognition of human rights law in all national jurisdictions.

4. Conclusions

The technological advance brought about by the emergence and evolution of new digital technologies brings a number of opportunities to society, but also challenges related to certain risks to fundamental rights and freedoms, artificial intelligence being no exception in this respect. Technological and cybersecurity risks arising from the use of artificial intelligence technology require proactive and convergent measures by policy-makers and organisations developing such systems, by adopting specific prevention mechanisms. The current regulatory landscape for artificial intelligence, while complex and dynamic, is highly fragmented and non-harmonised, which can lead to legal uncertainty and confusion. For these reasons, in order to prevent the risks associated with the use of artificial intelligence systems, there must be a global consensus to adopt a specific legal framework, with balanced participation and representation of all stakeholders, given the ubiquity of the digital space. However, we must bear in mind that such an initiative is currently difficult to achieve, given the continuous evolution of this new technology, the dynamics and lack of knowledge of all the associated

online at <https://www.accesnow.org/cms/assets/uploads/2018/11/AI-and-Human-Rights.pdf>, accessed on 08.12.2023.

⁸⁷ Raso Fillippo, Hannah Hilligoss, Vivek Krishnamurthy, Christopher Bavitz, Levin Kim, *Artificial Intelligence & Human Rights: Opportunities & Risks*, Berkman Klein Center for Internet & Society Research Publication, 2018, the document is available online at <https://dash.harvard.edu/handle/1/38021439>, accessed on 07.12.2022.

⁸⁸ Yeung Karen, Andrew Howes, Ganna Pogrebna, *AI Governance by Human Rights-Centred Designed, Deliberation and Oversight: An End to Ethics Washing*, Markus D. Dubber (editor), The Oxford Handbook of Ethics of AI, 2020, pp. 76–106, the document is available online at <https://academic.oup.com/edited-volume/34287/chapter-abstract/290657408?redirectedFrom=full-text>, accessed on 28.02.2024; Pielemeier Jason, *The Advantages and Limitation of Applying the International Human Rights Framework to Artificial Intelligence*, 26.02.2019, the document is available online at <https://cpr.unu.edu/publications/articles/ai-global-governance-the-advantages-of-applying-the-international-human-rights-framework-to-artificial-intelligence.html>, accessed on 08.12.2022.

threats and the lack of consensus in defining the concept of ‘artificial intelligence’. It is particularly important that the future framework incorporates a number of principles already introduced by ethical standards and legal mechanisms adopted or proposed, such as transparency, fairness, accountability, privacy and non-abuse, but ensuring a full balance between respect for fundamental rights and technological progress.

Bibliography

I. Books and articles

1. Brkan, Maja & Bonner Gregory, *Legal and Technical Feasibility of the GDPR’s Quest for Explanation of Algorithmic Decisions: of Black Boxes, White Boxes and Fata Morganas*, ‘European Journal of Risk Regulation’, Volume 11, Issue 1, 2020, pp. 18-50, <https://www.cambridge.com/core/journals/european-journal-of-risk-regulation/article/legal-and-technical-feasibility-of-the-gdprs-quest-for-explanation-of-algorithmic-decisions-of-black-boxes-white-boxes-and-fata-morganas/7324CDE80A300179C170C5BA8CA7E851>.
2. Bruschi, Danilo & Diomede Nicla, *A framework for assessing AI ethics with applications to cybersecurity*, ‘AI and Ethics’, 2022, Volume 3, pp. 65–72, <https://link.springer.com/article/10.1007/s43681-022-00162-8>.
3. Buiten, Miriam, *Towards Intelligent Regulation of Artificial Intelligence*, 29.04.2019, ‘European Journal of Risk Regulation’ 10(1), 2019, pp. 41–59, <https://www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/towards-intelligent-regulation-of-artificial-intelligence/AF1AD1>.
4. Butcher, James & Beridze Irakli, *What is the State of Artificial Intelligence Governance Globally*, ‘RUSI Journal’, 2019, Volume 164, Nos 5/6, pp. 88–96, <https://www.researchgate.net/publication/337640603>.
5. Carsten, Stahl Bernd, Rowena Rodrigues, Nicole Santiago & Kevin Macnish, *A European Agency for Artificial Intelligence: Protecting fundamental rights and ethical values*, ‘Computer Law & Security Review’, 2022, Volume 45, <https://sciencedirect.com/science/article/pii/S0267364922000097>.
6. Casarosa, Federica, *Cybersecurity Certification of Artificial Intelligence: a missed opportunity to coordinate between Artificial Intelligence Act and the Cybersecurity Act*, ‘International Cybersecurity Law Review’, 2022, Volume 3, pp. 115–130, <https://link.springer.com/article/10.1365/s43439-021-00043-6>.
7. Castets-Renard, Celine, *Accountability of Algorithms in the GDPR and Beyond: A European Legal Framework on Automated Decision-Making*, ‘Fordham Intellectual Property, Media & Entertainment Law Journal, Futurecoming’, 20.05.2019, <https://ssrn.com/abstract=3391266>.
8. Cate, Fred, Kuner Christopher, Orla Lynskey, Christopher Millard, Nora Ni Loideain & Dan Jerker B. Svantesson, *Expanding the Artificial Intelligence – Data Protection Debate*, ‘International Data Privacy Law’, 2018, Volume 8, No. 4, pp. 289–292, <https://www.academic.oup.com/idpl/article/8/4/289/5299551>.
9. Chesterman, Simon, *Weapons of Mass Disruption: Artificial Intelligence and International Law*, ‘Cambridge International Law Journal’, 2021, Volume 10, pp. 181–203, <https://ssrn.com/abstract=3832563>.

10. Clarke, Roger, *Regulatory alternatives for AI*, 'Computer Law & Security Review', 2019, Volume 35, pp. 398-409, <https://www.sciencedirect.com/science/article/abs/pii/S0267364919301281>.
11. Connor, Rees & Muller Berndt, *All that glitters is not gold: trustworthy and ethical AI principles*, 'AI and Ethics', 16.11.2022, <https://link.springer.com/article/10.1007/s43681-022-00232-x>.
12. Dixon, Red Bin Lee, *A principled governance for emerging AI regimes: lessons from China, the European Union, and the United States*, 'AI and Ethics', 2023, Volume 3, pp. 793–810, <https://link.springer.com/article/10.1007/s43681-022-00205-0>.
13. Donahoe, Eileen & Megan MacDuffee Metzger, *Artificial Intelligence and Human Rights*, 'Journal of Democracy', 2019, Volume 30(2), pp. 115-126, <https://www.proquest.com/docview/2295528777>.
14. Ebers, Martin, Veronica R.S. Hoch, Frank Rosenkranz, Hannah Ruschemeier & Björn Steinrötter, *The European Commission's Proposal for an Artificial Intelligence Act – A Critical Assessment by members of the Robotics and AI Law Society*, 'Multidisciplinary Scientific Journal's', 2021, Volume 4(4), pp. 589–603, <https://www.mdpi.com/2571-8800/4/4/43>.
15. Erdelyi, Olivia & Judy Goldsmith, *Regulating artificial intelligence: Proposal for a global solution*, 'Government Information Quarterly', 2022, Volume 39, Issue 4, <https://www.sciencedirect.com/science/article/abs/pii/S0740624X22000843>.
16. Fjeld, Jessica, Nele Achten, Hannah Hilligoss, Adam Nagy & Madhulika Sriku-mar, *Principled Artificial Intelligence: Mapping Consensus in Ethical and Right-Based Approaches to Principles of AI*, Berkman Klein Center, Research Publication no. 2020-1, <https://ssrn.com/abstract=3518482>.
17. Floridi, Luciano & Cowl Josh, *A Unified Framework of Five Principles for AI in Society*, 29.04.2021, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3831321.
18. Fukuda-Parr, Sakito & Gibbons Elisabeth, *Emerging Consensus on 'Ethical AI': Human Rights Critique of Stakeholders Guidelines*, 'Global Policy', 2021, Volume 12, Supplement 6, <https://onlinelibrary.wiley.com/doi/full/10.1111/1758-5899.12965>.
19. Gomez Rego, de Almeida Patricia, Denner dos Santos Carlos & Silva Farias Jovivania, *Artificial Intelligence Regulation: a framework for governance*, 'Ethics and Information Technology', 2021, Volume 23, pp. 505-525, <https://link.springer.com/article/10.1007/s10676-021-09593-z>.
20. Hageman, Ryan, Jennifer Hudleston & Adam Thierer, *Soft Law for Hard Problems: The Governance of Emerging Technologies in an Uncertain Future*, 'Colorado Technology Law Journal', 05.02.2018, https://papers.ssrn.com/sol3/papers.cfm?abstract_id3118539.
21. Hagendorff, Thilo, *The Ethics of AI Ethics. An Evaluation of Guidelines*, 11.10.2019, <https://arxiv.org/abs/1903.03425>.
22. Herve, Allan, *Data Protection and Artificial Intelligence*, in Peng Shin-Yi, Ching-Fu Lin, Thomas Streinz (editors), *Artificial Intelligence and International Economic Law*, Cambridge University Press, 2021, pp. 193–214, <https://www.cambridge.org/core/books/artificial-intelligence-and-international-economic-law/data-protection-and-artificial-intelligence/B98076D59C2B75892D58CC115>

- 18E2217.
23. Janneke, Gerards, *The fundamental rights challenges of algorithms*, 'Netherlands Quarterly of Human Rights', 2019, Volume 37(3), pp. 205–209, <https://journals.sagepub.com/doi/full/10.1177/0924051919861773>.
 24. Jelinek, Thorsten, Wendell Wallach & Danil Kerimi, *Policy brief: the creation of a G20 coordinating committee for the governance of AI*, 'AI and Ethics', 2021, Volume 1, pp. 141–150, <https://link.springer.com/article/10.1007/s43681-020-00019-y>.
 25. Jobin, Anna, Ienca Marcelo & Vayena Effy, *Artificial Intelligence: the global landscape of ethics guidelines*, 2019, <https://arxiv.org/abs/1906.11668>.
 26. Latonero, Mark, *Governing Artificial Intelligence: Upholding Human Rights & Dignity*, Data & Society, 2018, <https://datasociety.net/library/governing-artificial-intelligence/>.
 27. Lottie, Lane, *Clarifying Human Rights Standards through Artificial Intelligence Initiatives*, 'International & Comparative Law Quarterly', 2022, Volume 71(4), pp. 915–944, <https://www.cambridge.org/core/journals/international-and-comparative-law-quarterly/article/clarifying-human-rights-standards-through-artificial-intelligence-initiatives/52D69ACE49CE1E0B5D9E69E51CA14690>.
 28. Marchant, Gary, Lucille Tournas & Carlos Ignacio Gutierrez, *Governing emerging technologies through Soft Law: Lessons for Artificial Intelligence*, 07.12.2020, » Jurimetrics', vol. 61, Issue 1, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3761871.
 29. Marjin, Janssen, Brous Paul, Estevez Elsa, Barbosa S. Luis & Janowski Tomasz, *Data governance: Organizing data for trustworthy Artificial Intelligence*, 'Government Information Quarterly', 2020, Volume 37, Issue 3, <https://www.sciencedirect.com/science/article/pii/S0740624X20302719>.
 30. Merchant, Gary E., Braden R. Allenby & Joseph R. Herkert, *The Growing Gap Between Emerging Technologies and Legal-Ethical Oversight*, The International Library of Ethics, Law and Technology, 2011, volume 7, <https://link.springer.com/book/10.1007/978-94-007-1356-7>.
 31. Nemitz, Paul, *Constitutional democracy and technology in the age of artificial intelligence*, 15.10.2018, 'Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences', Volume 376, Issue 2133, <https://royalsocietypublishing.org/doi/epdf/10.1098/rsta.2018.0089>.
 32. Niels, Berkel van, Eleftherios Papachristos, Anastasia Giachanou, Simo Hosio, *A systematic Assessment of National Artificial Intelligence Policies: Perspectives from the Nordics and Beyond*, <https://www.researchgate.net/publication/344320861>.
 33. Paal, Boris, *Artificial Intelligence as a Challenge for Data Protection Law*, in Voenekey, Silja, Philipp Kellmeyer, Oliver Mueller & Wolfram Burgard (editors), *The Cambridge Handbook of Responsible Artificial Intelligence*, Cambridge University Press, 2022, pp. 290–308, <https://www.cambridge.org/core/books/cambridge-handbook-of-responsible-artificial-intelligence/artificial-intelligence-as-a-challenge-for-data-protection-law/84B9874F94043E8AFC81616A60BA69CC>.
 34. Parson, Edward (Ted) A., Richard M. Re, Alicia Solow-Niederman & Elana Zeide, *Artificial Intelligence in Strategic Context: An Introduction*, UCLA

- School of Law, Public Law Research Paper's, 2019, No. 19–45, <https://ssrn.com/abstract=3476384>.
35. Pielemeier, Jason, *The Advantages and Limitation of Applying the International Human Rights Framework to Artificial Intelligence*, 26.02.2019, <https://cpr.unu.edu/publications/articles/ai-global-governance-the-advantages-of-applying-the-international-human-rights-framework-to-artificial-intelligence.html>.
 36. Radu, Roxana, *Steering the governance of artificial intelligence: national strategies in perspective*, 'Policy and Society', 2021, Volume 40, Issue 2, pp. 178–193, <https://www.tandfonline.com/doi/full/10.1080/14494035.2021.1929728>.
 37. Raso, Fillippo, Hannah Hilligoss, Vivek Krishnamurthy, Christopher Bavitz & Levin Kim, *Artificial Intelligence & Human Rights: Opportunities & Risks*, Berkman Klein Center for Internet & Society Research Publication, 2018, <https://dash.harvard.edu/handle/1/38021439>.
 38. Risse, Matthias, *Human Rights and Artificial Intelligence: An Urgently Needed Agenda*, » HKS Faculty Research Working Paper Series RWP18-015,' 2018, <https://www.hks.harvard.edu/publications/human-rights-and-artificial-intelligence-urgently-needed-agenda>.
 39. Ryan, Calo & Kate Crawford, *There is a blind spot in AI research*, 'Nature' 538, 2016, pp. 311–313, <https://www.nature.com/articles/538311a>.
 40. Ryan, Calo, *Artificial Intelligence Policy: A Primer and Roadmap*, » University of Bologna Law Review', 2018, Volume 3(2), pp. 180–218, <https://doaj.org/article/cc06b2b47fbc4e3d9b6d6835b7fccbca>.
 41. Ryan, Calo, *Peeping HALs: Making Sense of Artificial Intelligence and Privacy*, » European Journal of Legal Studies', 2010, 2, 3, <https://hdl.handle.net/1814/15123>.
 42. Sava, Ruxandra, *Când decizia o ia mașina ... Despre profilare, drepturi și echilibru într-un univers digital*, „Revista Română pentru Protecția și Securitatea Datelor cu Caracter Personal” No. 3/2020, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3721413.
 43. Schiff, Daniel, *What's Next for AI Ethics, Policy, and Governance? A Global Overview*, <https://aies-conference.com/2020/wp-content/papers/030.pdf>.
 44. Schwab, Klaus, *The Fourth Industrial Revolution*, World Economic Forum, 2016, https://law.unimelb.edu.au/_data/assets/pdf_file/0005/3385454/Schwab-The_Fourth_Industrial_Revolution_Klaus_S.pdf.
 45. Smuha, Natalie, *Beyond a Human Rights-based to AI Governance: Promise, Pitfalls, Plea*, 'Philosophy & Technology', 2021, Volume 34, pp. 91–104, <https://link.springer.com/article/10.1007/s13347-020-00403-w>.
 46. Smuha, Nathalie, Ahmed-Rengers Emma, Harkens Adam, Li Wenlong, MacLaren James, Piselli Riccardo & Yeung Karen, *How the EU can achieve legally trustworthy AI: a response to the European Commission's proposal for an Artificial Intelligence Act*, 05.08.2021,' Artificial Intelligence – Law, Policy & Ethics eJournal', SSRN Network, <https://ssrn.com/abstract=389991>.
 47. Stix, Charlotte, *Actionable Principles for Artificial Intelligence Policy: Three Pathways*, 'Science and Engineering Ethics', 2021, Volume 27, <https://link.springer.com/article/10.1007/s11948-020-00277-3>.
 48. Stix, Charlotte, *Foundations for the future: institution building for the purpose of artificial intelligence governance*, 'AI & Ethics', 2022, Volume 2, pp. 463–476, <https://link.springer.com/article/10.1007/s43681-021-00093-w>.

49. Taddeo, Mariarosaria, *On the Risks of Trusting Artificial Intelligence: The Case of Cybersecurity*, in Cows, Josh & Jessica Morley (editors), *The 2020 Yearbook of the Digital Ethics Lab.*, Springer, 2020, pp. 97–108, https://link.springer.com/chapter/10.1007/978-3-030-80083-3_10.
50. Taeihagh, Arez, *Assessing the regulatory challenges of emerging disruptive technologies*, "Regulation & Governance", 2021, Volume 15, pp. 1009–1019, <https://onlinelibrary.wiley.com/doi/epdf/10.1111/rego.12392>.
51. Taeihagh, Arez, *Governance of artificial intelligence*, 'Policy and Society', 2021, Volume 40, Issue 2, pp. 137-157, <https://academic.oup.com/policyandsociety/article/40/2/137/6509315>.
52. Urs, Gasser & Virgilio A. F. Almeida, *A layered model for AI governance*, 'IEEE Internet Computing', 2017, Volume 21, Issue 6, pp. 58–62, <https://ieeexplore.ieee.org/document/8114684>.
53. Vasiliki, Koniaku, *From the rush to ethics' to race for governance' in Artificial Intelligence*, 'Information Systems Frontiers', 2022, Volume 25, pp. 71–102, <https://link.springer.com/article/10.1007/s10796-022-10300-6>.
54. Wachter, Sandra, Brent Mittelstadt & Russel Chris, *Counterfactual explanations without opening the black box: automated decisions and the GDPR*, 'Harvard Journal of Law and Technology', 2018, Volume 31(2), <https://ssrn.com/abstract=3063289>.
55. Wachter, Sandra, Mittelstadt Brent & Floridi Luciano, *Why a Right to Explanation of Automated Decision-Making Does Not Exist in General Data Protection Regulation*, 'International Data Privacy Law', 2017, <https://ssrn.com/abstract=2903469>.
56. Wallace, Nick & Castro Daniel, *The Impact of the EU's New Data Protection Regulation on AI*, Centre for Data Innovation, 27.03.2018, <https://www2.datainnovation.org/2018-impact-gdpr-ai.pdf>.
57. Wallach, Marchant, *An agile ethical/legal model for the international and national governance of AI and robotics*, 2018, https://www.aies-conference.com/2018/contents/papers/main/AIES_2018_paper_77.pdf.
58. White, James M. & Rolf Lidskog, *Ignorance and the regulation of artificial intelligence*, 'Journal of Risk Research', 2022, Volume 25, Issue 4, pp. 488–500, <https://www.tandfonline.com/doi/full/10.1080/13669877.2021.1957985>.
59. Whittlestone, Jess, Rune Nyrup, Anna Alexandrova & Stephen Cave, *The Role and Limits of Principles in AI Ethics: Towards a Focus on Tensions*, AIES '19: Proceedings of the 2019 AAAI/ACM Conference on AI, Ethics, and Society, 2019, pp. 195–200, <https://dl.acm.org/doi/10.1145/3306618.3314289>.
60. Yeung, Karen, Andrew Howes & Ganna Pogrebna, *AI Governance by Human Rights-Centred Designed, Deliberation and Oversight: An End to Ethics Washing*, in Dubber, Markus D. (editor), *The Oxford Handbook of Ethics of AI*, 2020, pp. 76–106, <https://academic.oup.com/edited-volume/34287/chapter-abstract/290657408?redirectedFrom=fulltext>.
61. Zeng, Yi, Enmeng Lu & Cunqing Huangfu, *Linking Artificial Intelligence Principles*, <https://arxiv.org/abs/1812.04814>.
62. Zuiderveen, Borgesius Frederik, *Strengthening legal protection against discrimination by algorithms and artificial intelligence*, 'International Journal of Human Rights', 2020, pp. 1–22, <https://ssrn.com/abstract=3561441>.

II. Reports and expert studies

1. Access Now, *Human Rights in the Age of Artificial Intelligence*, 2018, <https://www.accesnow.org/cms/assets/uploads/2018/11/AI-and-Human-Rights.pdf>.
2. AlgorithmWatch, *AI Ethics Guidelines Global Inventory*, 2020, <https://inventory.algorithmwatch.org>.
3. ENISA, *Cybersecurity of AI and Standardisation*, 14.03.2023, <https://www.enisa.europa.eu/publications/cybersecurity-of-ai-and-standardisation>.
4. Mantelero Alessandro, *Artificial Intelligence and Data Protection: Challenges and Possible Remedies*, 25.01.2019, <https://rm.coe.int/artificial-intelligence-and-data-protection-challenges-and-possible-re/168091f8a6>.
5. Muller Cateljine, *The impact of Artificial Intelligence on Human Rights, Democracy and the Rule of Law*, 24.06.2020, <https://rm.coe.int/cahai-2020-06-fin-c-muller-the-impact-of-ai-on-human-rights-democracy-/16809ed6da>.
6. Pupillo Lorenzo, Fantin Stefano, Ferreira Afonso, Polito Carolina, *Artificial Intelligence and Cybersecurity. Technology, Governance and Policy Challenges*, Centre for European Policy Studies (CEPS), Brussels, 2021, <https://www.ceps.eu/ceps-publications/artificial-intelligence-and-cybersecurity-2/>.
7. PwC, *Sizing de prize. What's the real value of AI for your business and how can you capitalise?*, 2017, <https://www.pwc.com/gx/en/issues/data-and-analytics/publications/artificial-intelligence-study.html>.
8. Sartor Giovanni, *The impact of the General Data Protection Regulation (GDPR) on Artificial intelligence*, [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU\(2020\)641530_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf).
9. Sean McGregor, *Preventing Repeated Real World AI Failures by Cataloging Incidents: The AI Incident Database*, <https://incidentdatabase.ai/apps/incidents/>.
10. Stanford Institute for Human-Centered Artificial Intelligence, *2023 AI Index Report*, <https://aiindex.stanford.edu/report/>.
11. The Council of Europe, *Towards Regulation of AI Systems*, 2020, <https://edoc.coe.int/fr/intelligence-artificielle/9656-towards-regulation-of-ai-systems.html#>.
12. The Council of Europe, *A Legal Framework of AI Systems*, 2021, <https://edoc.coe.int/fr/intelligence-artificielle/9648-a-legal-framework-for-ai-systems.html>.
13. United Nations, *Report of the Secretary-General' Roadmap for Digital Cooperation*, 2020, https://www.un.org/en/content/digital-cooperation-roadmap/assets/pdf/Roadmap_for_Digital_Cooperation_EN.pdf.

III. Regulations

1. Access Now, Amnesty International, *The Toronto Declaration*, 16.05.2018, <https://www.amnesty.org/en/documents/pol30/8447/2018/en/>.
2. Beijing Academy of Artificial Intelligence, *Beijing AI Principles*, 28.05.2019, <https://link.springer.com/content/pdf/10.1007/s11623-019-1183-6.pdf>.
3. Camera Deputaților, *Proiect de Lege privind utilizarea responsabilă a tehnologiei în contextul fenomenului deepfake*, https://www.cdep.ro/pls/proiecte/upl_pk.proiect?cam=2&idp=20853.
4. Department of Industry, Science and Resources, *Australia's Artificial Intelli-*

- gence Ethics Framework*, 07.11.2019, <https://www.industry.gov.au/publications/australias-artificial-intelligence-ethics-framework>.
5. Department for Science, Innovation and Technology, Office for Artificial Intelligence, *Establishing a pro-innovation approach to regulating AI*, <https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach/white-paper>.
 6. European Commission, *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*, COM (2018) 237 final, Bruxelles, 25.04.2018, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018DC0237>.
 7. European Commission, High-Level Expert Group on Artificial Intelligence, *Ethics Guidelines for Trustworthy AI*, 08.04.2019, <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai>.
 8. European Commission, *White Paper on Artificial Intelligence – A European approach to excellence and trust*, 2020, <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020DC0065>.
 9. European Commission, *Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts*, 21.04.2021, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206>.
 10. Executive Office of the President, *Executive Order 13,960 on Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government*, 03.12.2020, <https://www.federalregister.gov/documents/2020/12/08/2020-27065/promoting-the-use-of-trustworthy-artificial-intelligence-in-the-federal-government>.
 11. Google, *AI at Google: Our Principles*, 2019, <https://www.blog.google/technology/ai/ai-principles/>.
 12. G20, *G20 AI Principles*, 2019, <https://wp.oecd.ai/app/uploads/2021/06/G20-AI-Principles.pdf>.
 13. House of Lords – Select Committee on Artificial Intelligence, *AI in the UK: ready, willing and able?*, 16.04.2018, <https://publications.parliament.uk/pa/ld201719/ldselect/ldai/100/100.pdf>.
 14. IBM, *Everyday Ethics for Artificial Intelligence*, <https://www.ibm.com/downloads/cas/VDO5W3JK>.
 15. Microsoft, *Microsoft AI Principles*, 2018, <https://www.microsoft.com/en-us/ai/our-approach?activetab=pivot1%3aprimar5>.
 16. *Montreal Declaration for a Responsible Development of Artificial Intelligence*, 2018, https://www.montrealdeclaration-responsibleai.com/_files/ugd/ebc3a3_5c89e007e0de440097cef36dcd69c7b0.pdf.
 17. National Governance Committee for the New Generation Artificial Intelligence, *Governance Principles for the New Generation Artificial Intelligence*, 2019, <http://www.chinadaily.com.cn/a/201906/17/WS5d07486ba3103dbf14328ab7.html>.
 18. OECD, *Recommendation 0449 of the Council on Artificial Intelligence*, 22.05.2019, <https://oecd.ai/en/assets/files/OECD-LEGAL-0449-en.pdf>.
 19. Tencent Institute, *Technological ethics at intelligent era – reshape trustworthiness in digital society*, 08.07.2019, <https://tisi.org/10890>.

20. The Council of Europe, European Commission for the Efficiency of Justice (CEPEJ), *European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment*, <https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c>.
21. The Cyberspace Administration of China, *Internet Information Service Algorithmic Recommendation Management Provisions*, <https://digichina.stanford.edu/work/translation-internet-information-service-algorithmic-recommendation-management-provisions-effective-march-1-2022>.
22. The European Parliament and the Council of the European Union, *Regulation (EU) 2016/679 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)*, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679>.
23. The European Parliament and the Council of the European Union, *Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA*, <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L0680>.
24. The European Parliament and the Council of the European Union, *Regulation (EU) 2018/1725 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC*, <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32018R1725>.
25. The European Parliament and the Council of the European Union, *Regulation (EU) 2019/881 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology Cybersecurity Certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)*, <https://eur-lex.europa.eu/eli/reg/2019/881/oj>.
26. The Future of Life Institute, *AI Principles*, 11.08.2017, <https://futureoflife.org/open-letter/ai-principles/>.
27. The Institute of Electrical and Electronics Engineers, *Ethically Aligned Design*, 2019, <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9398613>.
28. UNESCO, *Recommendation on the Ethics of Artificial Intelligence*, 23.11.2021, <https://unesdoc.unesco.org/ark:/48223/pf0000381137>.
29. UNI Global Union, *Top 10 Principles for Ethical Artificial Intelligence*, 2017, http://www.thefutureworldofwork.org/media/35420/uni_ethical_ai.pdf.

**PRACTICAL APPLICATIONS AND
CHALLENGES IN TECHNOLOGY LAW**

Hacking Vehicles' Computer System

Associate professor **Adriana-Iuliana STANCU**¹

Abstract

The advent of automotive hacking is a result of the use of electronics in cars. A few years ago, tuning an automobile to produce more power required tuning automotive gear; nowadays, the on – board computer is the new target. For the first time, researchers from Washington and California linked the on – board computer to the OBD – II connector, automatically hacked the system, and installed the Car Shark malware. Aside from other nefarious things, this program could lock the doors, turn off the engine, and force hot air into the cabin. The only solace is that accessing the OBD – II port requires entering the vehicle, and once an attacker is inside, it is simpler for him to take a vehicle than conducting hacking activities. Researchers from the University of South Carolina and Rutgers University had an opposite opinion. They claim that it is possible to remotely hack the car and even control it while it is moving. They use tyre pressure sensors to accomplish it. Radio frequencies are used by these sensors to transmit data. Scientists were able to follow the vehicles and tamper with the transmitted data with the use of this signal.

Keywords: *hackers, engine control, codes, sensors.*

JEL Classification: K24

DOI: <https://doi.org/10.62768/ADJURIS/2024/1/11>

Please cite this article as:

Stancu, Adriana-Iuliana, „Hacking Vehicles' Computer System”, in Pajuste, Tiina, Heliona Bellani (Miço) & Sejla Maslo Cerkcic (eds.), *Legal Perspectives in the Modern Era of Technological Transformations*, ADJURIS – International Academic Publisher, Bucharest, Paris, Calgary, 2024, p. 178-192.

1. Introduction

A computer is a device that processes data and information in accordance with a set of instructions known as a *program*. It is also referred to as a computing system or computer. Since electronic components make up most of the modern computers, the term ‘computer’ typically refers to an electronic calculator. Universal computers are those that can process any type of data or information and are freely programmable. Modern computers are not only information processing

¹ Adriana-Iuliana Stancu, „Dunărea de Jos” University of Galați, Romania, <https://orcid.org/0000-0001-6259-5116>, adriana.tudorache@ugal.ro.

machines; they are also tools that let people communicate with each other, whether it be through text, numbers, images, sound, video, or even all of them at once (multimedia).

Computer science is the study of information processing with the aid of computers. Theoretically, any computer, be it a PDA or a supercomputer that can simulate a Turing machine or has a minimum set of functions may do the operations of any other computer of that type. Because of its compatibility, general-purpose computers (GPCs) are used for a wide range of tasks, from managing industrial or medical robots to processing payroll for businesses. Due to its potential to create industrial value, industrial digital transformation, or IDT, has gained more attention in the context of the fourth industrial revolution. However, better tool and framework support is still needed for practical applications².

2. Objectives

A system incorporated in automotive electronics that regulates one or more of the electrical systems or subsystems in a car or other motor vehicle is called an electronic control unit (ECU), sometimes referred to as an electronic control module (ECM).

Engine Control Module (ECM), Powertrain Control Module (PCM), Transmission Control Module (TCM), Brake Control Module (BCM or EBCM), Central Control Module (CCM), Central Timing Module (CTM), General Electronic Module (GEM), Body Control Module (BCM), and Suspension Control Module (SCM) are just a few of the many ECUs found in modern vehicles. Although these ECUs are all technically distinct computers and not one, they are sometimes referred to as the car's computer. A PCM frequently controls both the engine and the transmission. Occasionally, an assembly combines many separate control units.

A modern car may contain as many as 150 ECUs. The ECU's embedded software keeps getting more sophisticated, intricate, and complex. One of the biggest challenges facing original equipment manufacturers (OEMs) nowadays is controlling the growing complexity and quantity of ECUs in a vehicle.

In general, unapproved access to a computer system or network is referred to as hacking. A hacker is a person who engages in hacking operations. This hacker can alter the system or security features to accomplish an objective that differs from the system's original intent.

Non — malicious activities that typically involve ad hoc or unexpected adjustments to machinery or processes are also referred to as hacking.

Hackers employ a range of hacking methods, such as:

- Vulnerability Scanner: Looks for known vulnerabilities on systems

² Abiodun, T., Rampersad, G., & Brinkworth, R. (2023). Driving Industrial Digital Transformation. *Journal of Computer Information Systems*, 63(6), 1345–1361. <https://doi.org/10.1080/08874417.2022.2151526>.

connected to networks.

- Password cracking: the technique of obtaining passwords from data stored or delivered by computer systems.

- Packet sniffers: Applications for viewing passwords and data while they are being transmitted over networks by capturing data packets.

- Spoofing attack: consists of websites that pose as trustworthy and then utilize false information to trick users or other programs into believing they are authentic.

- Root kit: a collection of applications designed to take an operating system away from authorized users.

- Trojan horse: act as backdoors into computer systems, making it possible for hackers to access the system later.

- Viruses: self-replicating programs that propagate by cloning themselves into executable documents or other code files.

- Key Logs: Tools intended to capture each keystroke made since the compromised machine was pressed in order to be recovered later.

Hackers are employed by some companies as support personnel. By using their expertise to identify holes in a company's security system, these lawful hackers help stop identity theft and other online crimes.

3. Proposals and methodology

The modern individual has a plethora of opportunities in nowadays global society. We increasingly use resources, money, time, and knowledge through electronic methods.

One of the distinctive characteristics of the phenomena of computer crime is, of course, the adaptability and quick evolution of the illicit means employed, closely linked to the advancement of information technology and the exponential expansion of Internet usage opportunities.

Due to this specificity, a false myth about the mental capacity of those who commit crimes of this nature was created in the context of judicial practice. Regrettably, this concept led to an overly lenient view from the judicial bodies during the individualization of sanctions process.

Computer crime stems from the combination of ancient human tendencies such as greed, power, and fame-seeking, attachment to material values (money, things), luxury, pride, and so on, with the rapid technical innovation and ongoing expansion.

Even if there are no distinct definitions of computer crime in either national or international law, the concept of computer crime lends itself to several interpretations. However, to establish the notion, the United States of America and the United Kingdom of Great Britain employed terminology such as

‘computer crime’ and ‘computer – related crime’³.

In doctrine, according to Eoghan Casey, ‘Computer crime is a crime involving a computer, possible in several ways’. At the same time, ‘The methods by which uses a computer to commit crimes are the computer as an instrument of the crime, the computer as the focus of the crime, and the computer as a place to store evidence’⁴.

The regulation of computer crimes in national legislation took place following the ratification of the Council of Europe Convention on computer crime, adopted in Budapest on November 23, 2001, and in accordance with the Council’s Framework Decision of May 28, 2001⁵ on combating fraud and falsification of means of communication payment, other than 2001/413/JAI, the initial solution of the legislator from the point of view of the normative technique being to regulate computer crimes depending on the social value damaged and the specific facts, through Law no. 365/2002 regarding electronic commerce and, respectively, Law no. 161/2003, regarding some measures to ensure transparency in the exercise of public dignities, public functions and in the business environment, preventing and sanctioning corruption, in Title III, ‘Preventing and combating computer crime’⁶.

At the European level, users of digital platforms enjoy a diverse palette of regulations regarding the protection of their rights when purchasing goods or services online.

The community *acquis* includes: ‘Directive no. 2000/31/EC of the European Parliament and of the Council of June 8, 2000 regarding certain legal aspects of information society services, especially electronic commerce, on the internal market (electronic commerce directive)⁷, EU Regulation no. 2016/679 (General Data Protection Regulation), Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services within the internal market, Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, Directive 2003/88/EC of the European Parliament and of the Council of November 4, 2003 on certain aspects of the organization of working time, Directive 2011/83/EU of the European Parliament and of the Council of October 25, 2011 on consumer rights, Directive 2005/36/EC of the European Parliament and of the Council of September 7, 2005 on the recognition of professional qualifications, Directive 2013/11/EU of the

³ *California’s Computer Hacking Laws – What You Need to Know*. 05.02.2024. <<https://www.robertmhelfend.com/criminal-defense/california-computer-hacking-laws/>>.

⁴ Eoghan, Casey. *Digital Evidence and Computer Crime*, 3rd ed. Amsterdam: Elsevier, 2011, p. 25.

⁵ ‘Council Framework Decision of 28 May 2001 combating fraud and counterfeiting of non-cash means of payment (2001/413/JHA).’ 05.28.2001. *Official Journal of the European Communities*. 05 02 2024. <<https://service.betterregulation.com/document/257189>>.

⁶ Voss, Wilfried. *A Comprehensible Guide to Controller Area Network*. Massachusetts: Copperhill Technologies Corporation, 2005, pp. 116–119.

⁷ *Directive 2000/31/EC of the European Parliament*. 17.07.2000. 10.02.2024. <<https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:en:HTML>>.

European Parliament and of the Council of May 21, 2013 on the alternative resolution of consumer disputes and Regulation (EU) no. 524/2013 of the European Parliament and of the Council of May 21, 2013 regarding the online resolution of consumer disputes⁸.

The Council of Europe has requested a study to analyze the legislation of some European countries and some outside the EU, to see how computer crimes are incriminated because of the structure offered by the European Council⁹. The countries under study were: Austria, Albania, Armenia, Bulgaria, Cyprus, Croatia, Czech Republic, Estonia, Latvia, Lithuania, France, Germany, Hungary, Italy, Holland, Portugal, Romania, Serbia, Slovakia, Spain, the former Yugoslav Republic of Macedonia, Turkey, Ukraine and the United Kingdom and Australia, Brazil, Egypt, India, Mexico, the Philippines, South Africa, Sri Lanka and the United States of America¹⁰.

The goal of the study was to clarify the transcription of the concepts of crimes in the laws of certain states:

The offense provided for in art. 2 of the Convention on computer crime – Illegal access: ‘Each party shall adopt the legislative measures and other measures deemed necessary to incriminate as a crime, according to its internal law, the intentional and unauthorized access to the whole or a part of an information system.’ A party may condition such incrimination on the commission of the respective violation by violating security measures, with the intention of obtaining computer data or with other criminal intent, or on the connection between the respective violation and an IT system connected to another IT system.

The need to incriminate this crime is given by the fact that through the object of the crime, dangerous threats and attacks are brought to computer systems and computer data, aiming at their security, integrity and confidentiality.

In order to be able to protect the interests of organizations, natural and legal persons as well as state institutions, the norming aimed at ensuring the possibility to operate, control and use computer systems freely and undisturbed.

Unauthorized infiltration of any type of system is considered illegal, regardless of the method, because it creates problems for legitimate users who can transform or destroy systems and their data. At the same time, by being included in such a system, it can facilitate access to personal and confidential data. The nature of this data can make it easier for the criminal and committing crimes such as computer fraud or forgery.

Art. 3. Illegal interception. ‘Each party shall adopt the legislative measures and other measures deemed necessary to incriminate as a crime, according to its domestic law, the intentional and unlawful interception, carried

⁸ *Resolve your consumer complaint.* n.d. 12.02.2024. <https://commission.europa.eu/live-work-travel-eu/consumer-rights-and-complaints/resolve-your-consumer-complaint_en>.

⁹ *Council of Europe.* n.d. 15.02.2024. <<https://www.coe.int/en/web/portal>>.

¹⁰ *European Union Agency for Criminal Justice Cooperation.* n.d. 15.02.2024. <<https://www.eurojust.europa.eu/crime-types-and-cases/crime-types/cybercrime>>.

out by technical means, of computer data transmissions that are not public, intended, originated, or learned within a computer system, including electromagnetic emissions from a computer system carrying such data. A party may need the aforementioned violation to be committed with malicious intent or that there is a link between the aforementioned violation and a computer system that is linked to another computer system in order for it to be considered illegal. The fundamental goal of making these activities illegal is to safeguard the right to data communications secrecy. This sort of data privacy infringement is applicable to all forms of electronic data transfer, including file transfers, faxes, e-mail exchanges, and phone calls between individuals. It bears a striking resemblance to the violation of communications privacy.

Art. 4. Affecting data integrity. ‘1. Each party shall adopt the legislative measures and other measures deemed necessary to incriminate as a crime, according to its domestic law, the act committed intentionally and without the right to destroy, delete, damage, modify or eliminate computer data. 2. A party will be able to reserve the right to condition the incrimination of the behavior described in paragraph 1 on the occurrence of serious damages.’

Internal regulation is recommended to protect data and computer programs and provide them with similar protection as in the case of intentional damage to physical property. The main purpose is to ensure the integral protection and correct use and use of stored computer data or computer programs.

According to art. 5 of the Convention, *Affecting the integrity of the system* ‘each party shall adopt the legislative measures and other measures that are necessary to incriminate as a crime, in accordance with domestic law, the serious, intentional and unlawful impairment of the operation of an information system, by introducing, transmitting, endangering, deleting, damaging, altering or suppression of computer data.’

The purpose of the regulation is to protect against unauthorized and intentional use of computer systems, including telecommunications systems, using computer data and even having the possibility to influence it.

At the same time, art. 8 of the *Convention regulates computer fraud*¹¹.

‘Each party shall adopt the legislative measures and other measures that prove necessary to criminalize as a crime, according to its domestic law, the intentional and unlawful act of causing patrimonial damage to another person:

a) by any introduction, alteration, deletion or suppression of computer data;

b) by any form that affects the operation of an IT system, with the fraudulent or delictual intention to obtain an economic benefit without right for himself or for another person.’

The Convention recommends to all signatory states that their national

¹¹ *Convention on Cybercrime*. 2001. 21.02.2024. <<https://www.europarl.europa.eu/cmsdata/179163/20090225ATT50418EN.pdf>>.

legislation includes criminal offenses to stop any unauthorized manipulation during data processing with the intention of carrying out an illegal transfer of ownership.

It is easy to understand that due to the technological evolution, the ways of committing economic crimes, such as frauds, have increased. Assets represented or managed by computer systems (electronic funds, money deposits) have become the target of manipulations like traditional forms of ownership. Crimes operate by introducing incorrect data into computer systems or by altering data with the help of programs.

Until not long ago, most of the acts and documents were tangible, but, as previously mentioned, major and quantitative changes have been produced by current technologies for both the public and private sectors, and thus, national legislation allowed electronic documents to have the same value as tangible documents.

The convention recommends, for the safety in economic or social relations, that all countries should join the convention and ratify or expressly introduce a regulation regarding computer fabrications.

4. Results and implications

‘On March 22, 2021, the Council of Europe passed a few resolutions pertaining to the Digital Decade Cybersecurity Strategy. In December 2020, the Commission and the High Representative for Foreign Affairs put out this idea. The plan lays out the framework for EU action aimed at promoting secure IT systems, shielding enterprises and residents of the EU from cyber threats, and preserving an open, safe, and secure global cyberspace.

The strategy’s findings restate the idea that a resilient, environmentally conscious, and technologically advanced Europe depends on cyber security.

The Council’s recommendations support several areas of focus for this decade of action, such as:

- the need to support the development of strong encryption as a means of protecting fundamental rights and digital security, while ensuring the ability of law enforcement and judicial authorities to exercise their powers, both online and offline;

- increasing the effectiveness and efficiency of the cyber diplomacy toolkit, paying particular attention to preventing and combating cyber – attacks with systemic effects that could affect supply chains, critical infrastructure and essential services, democratic institutions and processes, and undermine economic security;

- order to increase the overall level of security and openness of the global Internet and maintain the competitiveness of EU industry, it is necessary to work together to expedite the adoption of essential Internet security standards;

- strong encryption must be developed to safeguard digital security and

fundamental rights while preserving the ability of law enforcement and judicial authorities to carry out their duties both online and offline;

- emphasizing the value of fortifying partnerships and international organizations to foster a shared understanding of the cyber threat scope;
- the plan to create an EU agenda to improve global cyber resilience, external cyber capabilities, and cyber capabilities.

Fraud and counterfeiting of cashless means of payment is a serious problem for the security of the European Union and a valuable source of income for organized crime. At the same time, this type of fraud affects consumer confidence in the security of digital technologies¹².

‘The Council of Europe, through a second additional protocol signed in November 2021, at the Budapest Convention, established the objective of the protocol:

- provisions for the efficiency of the mutual legal assistance regime (MLA);
- provisions regarding direct cooperation with service providers from other countries that are parties to the convention;
- a framework and safeguards for expanding cross – border searches.

The protocol includes robust data protection safeguards and requirements. The advantage of such an agreement is its potential to apply worldwide.’

The offense of unauthorized access to a computer system is provided for in art. 42 of the Computer Crime Law. The text of the law provides: ‘(1), Unauthorized access to a computer system constitutes a crime and is punishable by imprisonment from 6 months to 3 years or a fine. (2) If the act provided for in paragraph (1) is committed by violating the security measures, the penalty is imprisonment from 3 to 12 years.’

The special legal object is constituted by the social relations regarding the security of the information system, its inviolability and which are of a nature to ensure the confidentiality and integrity of the data contained but also of the information systems themselves.

The material object is made up of the components of the computer system that is the victim of the criminal activity or through the use of which unauthorized access was achieved.

The active subject can be any person and the passive subject is the owner of the IT system and/or the data stored on it¹³.

The objective side is represented by the activity of accessing a computer system or/and the data stored on it without the right.

The crime of unauthorized access in an IT system requires that the legal or contractual basis for the access is absent, or these limits are exceeded, the limits

¹² Grimes, Roger A. *Hacking the Hacker*. New Jersey: Willey, 2017, pp. 221–224.

¹³ Knight, Alissa. *Hacking Connected Cars*. Seattle: Amazon.com, 2020, pp. 233–235.

for which the authorization was offered, or when the access was made in a different interest than that of the service interest, but in personal interest. ‘The criminal law does not provide for a difference regarding how the security measures are violated, being irrelevant if the access credentials used for authentication are real.

To retain the conditions of objective specificity of the crime, it is important that they are introduced by the holder of the right of access by exceeding the authorization given to him, the authorization being granted for the purpose of use in the exercise of the duties of the service, in the interest of the service’¹⁴.

In the recent practice of the courts, a multitude of cases have been encountered in which persons exercising the function of a police officer, i.e. persons who have access guaranteed by law to computer systems that have personal databases, were sent to court for the act consisting of accessing without rights, namely to exceed the authorization initially allowed, of an IT system, such as databases managed by the Directorate of Permitted Traffic and Vehicle Registrations and the Directorate of Personnel Records and Database Administration, using the credentials they could use in the exercise of service duties, to access these computer systems, in order to obtain computer data, not in the exercise of service duties, but in personal interest¹⁵.

‘As the notions of “no right” or “exceeding the limits of authorization” are not concretely defined in the criminal law by reference to the typical conditions of the crime, in order to retain an accusation it is necessary to establish the area of application of the incrimination rule by concrete reference to in the case of persons who can query a database containing non – public information at any time, when such a query is not followed by the subsequent performance of certain acts specific to the exercise of official duties in connection with the query carried out’¹⁶.

In the situation where, if the person who accesses the database has this possibility ensured by the law, but no longer uses it in order to exercise his duties, it can be considered a matter that will make difficult the applicability of the regulation incriminating the act, as it could accurately establish whether the accessed information is relevant and thus fall under the rule of incriminating the act of illegal access to the computer system.

‘Computer fraud is defined but also incriminated by the provisions of the

¹⁴ *Unauthorized Computer Access (Otherwise Known as Hacking)*. n.d. 22 02 2024. <[https:// www.bayarea-attorney.com/unauthorized-computer-access-otherwise-known-as-hacking/](https://www.bayarea-attorney.com/unauthorized-computer-access-otherwise-known-as-hacking/)>.

¹⁵ *Government of Abu Dhabi*. n.d. 23.02.2024. <<https://es.adpolice.gov.ae/trafficservices/PublicServices/Introduction.aspx?Culture=en>>.

¹⁶ Council of Europe, Economic Crime Division, Directorate General of Human Rights and Legal Affairs, National legislation implementing the Convention on Cybercrime – Comparative Analysis and good practices, Discussion paper, http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/reportspresentations/567%20study2-dversion8%20_28%20 accessed on August 9, 2023.

criminal code. Thus, art. 249 includes the following provisions: ‘Introduction, modification or deletion of computer data, restricting access to this data or preventing in any way the operation of a computer system, in order to obtain a material benefit for oneself or for another, if damage has been caused to a person, is punished with imprisonment from 2 to 7 years’¹⁷.

The definition of the crime is done by listing the ways of committing it. Namely entering, modifying or deleting computer data, restricting access to this data or preventing in any way the operation of a computer system. To provide a strong basis for comprehending and addressing information system dangers, researchers must investigate the motivations behind the actions¹⁸.

In the doctrine, it is considered that part of the judicial practice is like ‘a special regulation in relation to the crime of deception, the crime of computer fraud was retained in the hypothesis of some factual situations that assumed as a criminal pattern, broadly speaking, the introduction of fake data, unreal information on e-commerce platforms, in order to mislead *bona fide* users of these sites and to obtain undue material benefits in this way’¹⁹.

The most used method of committing the crime, based on practice in the field, is the one by which on some online auction sites fake offers for the sale of products that may not even exist are posted, but the customers of these sites pay the amounts requested by the seller, directly to them, not through verified or verifiable methods. As expected, after the payment of the price, the alleged goods are no longer shipped by the seller, or other goods and products are sent, the value of which is insignificant compared to the original purchased well.

The way these frauds are committed is based on fake user profiles created on these e-commerce platforms, or data or profiles of pre-existing users whose credentials were obtained in reprehensible or even illegal ways are used. They use these accounts to post ads for which the product does not exist, or if the product does exist, it is not owned by them²⁰.

This method is employed, and it is far more advantageous to the criminal because, if the user whose account has been hacked has performed transactions successfully and has been previously validated by other users, this gives the appearance of genuine and unquestionable activity. As a result, the criminal will profit from this since prospective customers will act without considering the advertised bargain²¹.

¹⁷ Ciopec, F. and M. Roibu. *Infrațiuni informatice – infrațiuni invizibile, Drept penal/Computer crimes – invisible crimes, Criminal law*. Timisoara: West University of Timișoara, 2013. <https://drept.uvt.ro/administrare/files/1481038001-flaviu-ciopec-magdalena-roibu.pdf>, p. 196.

¹⁸ Owen, K., & Head, M. (2023). Motivation and Demotivation of Hackers in Selecting a Hacking Task. *Journal of Computer Information Systems*, 63(3), 522–536. <https://doi.org/10.1080/08874417.2022.2081883>.

¹⁹ Trancă, A. and C. Trancă. *Infrațiunile informatice în Noul Cod Penal/IT crimes in the New Criminal Code*. Bucharest: Universul Juridic, 2014, p. 8.

²⁰ Eoghan, Casey. *Digital Evidence and Computer Crime* 3rd ed. Amsterdam: Elsevier, 2011, p. 40.

²¹ Moise, A. C. *Metrologia investigației criminalistice a infrațiunilor informatice/Metrology of the*

The majority of fraudulent offers include reasonably priced products that are specifically crafted to catch the attention of possible buyers. Cars, artwork, jewellery, technology, and similar items can all be considered goods. Not to mention that there will be announcements regarding them if, at a given point in the market, there is a need for an item that is challenging to obtain.

For example, in the USA, the device was made for demonstration purposes, as a wake – up call to car manufacturers.

This vulnerability has been known for over 20 years, but no one has demonstrated it until now, although many have written about it.

RollJam, the device that Samy Kamkar and others with similar computer skills can use to unlock a modern car, came after the American hacker presented a device that could only unlock cars manufactured by GM and equipped with the OnStar system. In the case of that system, the hacker could start the car's engine, not just unlock the doors, but need to place an object on the vehicle and wait for its driver to access the OnStar service from their mobile phone and connect to the car in order to it goes through the system's security protocols. GM has been receptive to Samy Kamkar's suggestions and is already working on an update to the OnStar mobile app, which they will update to avoid the vulnerability.

Should we worry? Cybersecurity experts have demonstrated in the US the ability to take over the acceleration and braking of a car connected to the Internet.

Also, two American hackers were successful in taking control of an automobile's engine and brakes during the summer of 2015. The innovative aspect of the hack was that it did not require physical access to the car. The mobile phone network was used for the remote hack²².

How can a car be unlocked with the device created by the American hacker?

Kamkar's new hacking system is based on a software vulnerability in central locking systems and can only unlock a car. For the RollJam system to work, the hacker must be in the vicinity of the target vehicle when the driver is nearby and commands the doors to unlock. Anticipating the moment of pressing the button that gives the command to unlock the doors, the hacker must activate the dedicated device, which must be located on the target car²³.

It blocks the radio signal received by the vehicle and receives the code

forensic investigation of computer crimes. Bucharest: Universul Juridic, 2011, p. 16.

²² Schellekens, Maurice, Car hacking: Navigating the regulatory landscape, *Computer Law & Security Review*, Volume 32, Issue 2, 2016, pp. 307–315, <https://doi.org/10.1016/j.clsr.2015.12.019>.

²³ Nestor, R.A. *Incriminarea accesului ilegal la un sistem informatic sau riscul de a transforma un mijloc esențial de obținere a informației în mod de încălcare a legii penale*/Incriminating illegal access to a computer system or the risk of turning an essential means of obtaining information in violation of criminal law. 06.10.2021. 25.02.2024. <<https://www.juridice.ro/700452/incriminarea-accesului-ilegal-la-un-sistem-informatic-sau-riscul-de-a-transforma-un-mijloc-esential-de-obtinere-a-informatiei-in-mod-de-incalcare-a-legii-penale.html>>.

sent by the remote control used by the driver. Then, on the driver's second attempt to unlock the doors, the system receives a second code sent by the remote, but transmits the first code to the car while blocking the second. The entire action assumes that the owner will not try to unlock the car with the key and that the hacker will be able to get to the car again to succeed in unlocking it.

The software vulnerability in modern automobiles with central locking systems occurs because of the chipset manufacturers for the systems that control this vehicle function. Kamkar explained that this vulnerability has existed for over 20 years and also occurs in garage doors and electronically operated remote control gates. As with cars, the vulnerability appears to use a 'rolling code'. This is a code that changes each time the central locking remote is used and allows only one use for that specific code. Unfortunately, the manufacturers did not anticipate the vulnerability and did not introduce a code expiration period.

Thus, if a hacker intercepts a valid code from the remote control and blocks it from being sent to the car, the driver is forced to transmit another code to the car, during which his special device can record a valid and unused code sent by the remote control. Because these codes do not expire, the hacker can come to the target vehicle at any time and unlock it with that code.

How do you hack into a GM vehicle that has driver smartphones unlock and start? ²⁴.

How can a garage with an electronically operated door be unlocked using Samy's method?

A hacker has presented the device with which he can unlock almost any car with central locking by remote control.

Shortly after hacking demonstrations in the US demonstrated the vulnerabilities of Jeep and Tesla models, another hacker in the US presented a device with which he can unlock almost any car with central locking by remote control²⁵.

5. Conclusions

Digital transformation has become one of the most popular strategies for information systems (IS). For any firm that uses information systems, creating and implementing a digital strategy is essential. An IS/IT strategy without security concerns could result in significant data breaches in this digital age. Security is still a big worry in the digital transformation process despite all the safeguards since digitization is misunderstood and raises serious security risks²⁶.

²⁴ *From remote control to scheduling service appointments and beyond, the new myGMC mobile app is a convenient way to stay connected and informed.* n.d. 25.02.2024. <<https://www.gmc.com/gmc-life/technology/stay-connected-with-the-mygmc-mobile-app>>.

²⁵ *Apple – FBI encryption dispute.* 2016. 27.02.2024. <https://en.wikipedia.org/wiki/Apple%E2%80%93FBI_encryption_dispute>.

²⁶ Stewart, H. (2023). Digital Transformation Security Challenges. *Journal of Computer*

Many people don't realize that in newer cars the car computer is a computer like the ones we have at home. In an ordinary car, the multimedia system computer has the power of a mid-range smartphone: it has 1 GB of RAM, it has WiFi, it has a standalone operating system, and it also has GPS. Obviously, in a second-hand car that is many years old, the computer is not so powerful and cannot store so much information, but in newer ones it is powerful.

Because the multimedia system's computer maintains a lot of data that it pulls from the smartphone each time it synchronizes the phone with the car, the automobile was aware of a great deal about the driver.

The computer in the car held a lot of information, including his location, the emails and SMS he had received, his phone book, and even a voice profile—that is, the voice commands he had given while driving. Additionally, it saves telemetric information on driving, braking, and average speed. Similarly, the information of individuals who continue to link their phone to the vehicle's computer is still there.

The data remain on the car's computer even after the session ends and are impossible to delete. Basically, if a hacker manages to insert a USB stick into the car's port, he can extract your personal data and build a kind of 'information files' with all drivers' habits.

The emergence of autonomous vehicles, the growth of car-sharing services, and the day when we share cars rather than own them—and when we don't want our data to get into those cars if we synchronize our phones with them—will all make things more problematic. The car is portrayed as a mobile smartphone. However, the people who write the software for these devices don't often realize how dangerous attacks might be, and they don't write the software with this in mind.

There would also be the problem of WiFi networks. The car, having an ordinary computer, detects and can connect to all WiFi networks on the street, and an attacker can make it connect to all open WiFi networks as you walk with it and can follow you on GPS and can see your route through free, unprotected hotspots. Or, if the hacker writes a simple virus, your personal information can be uploaded to the Internet when you pass by a certain WiFi network, and it doesn't stop there.

The car can be like a kind of weapon, practically when you drive it around town it can attack other cars connected to WiFi networks. What happens is what is called in specialist terms 'wardriving', which means that hackers drive around the city and connect to unsecured WiFi networks, either to steal sensitive data or to use it for illegal actions.

War driving is generally done using a laptop in the car, in this case the car can take the place of the laptop. When the machine detects an unsecured network, it can extract data from it or launch exploits (a program that exploits a vulnerability) against other terminals connected to WiFi.

There could also be a very serious scenario. The infotainment system does absolutely anything and it is possible for the information busses for the sensors to pass through the car's computer and the car can be remotely made to automatically brake suddenly, as if it had an obstacle in front of it.

Another scenario would be, for the distant future when cars will be much more computerised that a hacker infects your car with a ransomware, which makes the software unusable until you pay a financial reward.

The car becomes a second home, others present it as a smartphone on wheels. But those who create the software for these machines are not always aware of how great the danger is in the face of attacks and does not create this machine software with this in mind.

Whether this phenomenon is dangerous or not, European, and international organizations are making every effort to put a stop to it since it invites criminal activity.

Bibliography

1. Abiodun, T., Rampersad, G. & Brinkworth, R. (2023). Driving Industrial Digital Transformation. *Journal of Computer Information Systems*, 63(6), 1345–1361. <https://doi.org/10.1080/08874417.2022.2151526>.
2. Ciopec, F. and M. Roibu. *Infrațiuni informatice – infrațiuni invizibile, Drept penal/Computer crimes – invisible crimes, Criminal law*. Timisoara: Universitatea de Vest Timisoara, 2013. <https://drept.uvt.ro/administrare/files/1481038001-flaviu-ciopec-magdalena-roibu.pdf>, p. 196.
3. Council of Europe, Economic Crime Division, Directorate General of Human Rights and Legal Affairs, National legislation implementing the Convention on Cybercrime – Comparative Analysis and good practices, Discussion paper, http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/reportspresentations/567%20study2-dversion8%20_28%20 accessed on August 9, 2023.
4. Eoghan, Casey. *Digital Evidence and Computer Crime*, 3rd Ed., Amsterdam: Elsevier, 2011.
5. *From remote control to scheduling service appointments and beyond, the new myGMC mobile app is a convenient way to stay connected and informed*. n.d. 25.02.2024. <<https://www.gmc.com/gmc-life/technology/stay-connected-with-the-mygmc-mobile-app>>.
6. Grimes, Roger A., *Hacking the Hacker*. New Jersey: Willey, 2017, pp. 221–224.
7. Knight, Alissa. *Hacking Connected Cars*. Seattle: Amazon.com, 2020.
8. Moise, A. C., *Metrologia investigației criminalistice a infrațiunilor informatice /Metrology of the forensic investigation of computer crimes*. Bucharest: Universul Juridic, 2011.
9. Nestor, R.A., *Incriminarea accesului ilegal la un sistem informatic sau riscul de a transforma un mijloc esențial de obținere a informației în mod de încălcare a legii penale/ Incriminating illegal access to a computer system or the risk of turning an essential means of obtaining information in violation of criminal law*. 6.10.2021. 25.02.2024. <<https://www.juridice.ro/700452/incriminarea-accesu>>.

- lui-ilegal-la-un-sistem-informatic-sau-riscul-de-a-transforma-un-mijloc-esential-de-obtinere-a-informatiei-in-mod-de-incalcare-a-legii-penale.html>.
10. Owen, K., & Head, M. (2023). Motivation and Demotivation of Hackers in Selecting a Hacking Task. *Journal of Computer Information Systems*, 63(3), 522–536. <https://doi.org/10.1080/08874417.2022.2081883>.
 11. Schellekens, Maurice, Car hacking: Navigating the regulatory landscape, *Computer Law & Security Review*, Volume 32, Issue 2, 2016, pp. 307–315, <https://doi.org/10.1016/j.clsr.2015.12.019>.
 12. Stewart, H. (2023). Digital Transformation Security Challenges. *Journal of Computer Information Systems*, 63(4), 919–936. <https://doi.org/10.1080/08874417.2022.2115953>.
 13. Tranca, A. and C. Trancă. *Infrațiunile informatice în Noul Cod Penal/IT crimes in the New Criminal Code*. Bucharest: Universul Juridic, 2014.
 14. *Unauthorized Computer Access (Otherwise Known as Hacking)*. n.d. 22 02 2024. <<https://www.bayarea-attorney.com/unauthorized-computer-access-other-wise-known-as-hacking/>>.
 15. Voss, Wilfried. *A Comprehensible Guide to Controller Area Network*. Massachusetts: Copperhill Technologies Corporation, 2005, pp. 116-119.
 16. *Directive 2000/31/EC of the European Parliament*. 17 07 2000. 10 02 2024. <<https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:on:HTML>>.
 17. Council Framework Decision of 28 May 2001 combating fraud and counterfeiting of non-cash means of payment (2001/413/JHA). 5.28.2001. *Official Journal of the European Communities*. 5.02.2024. <<https://service.betaerregulation.com/document/257189>>.
 18. *California's Computer Hacking Laws – What You Need to Know*. 5.02.2024. <https://www.robertmhelfend.com/criminal-defense/california-computer-hacking-laws/>.
 19. *Resolve your consumer complaint*. n.d. 12.02.2024. <https://commission.europa.eu/live-work-travel-eu/consumer-rights-and-complaints/resolve-your-consumer-complaint_en>.
 20. *Convention on Cybercrime*. 2001. 21.02.2024. <<https://www.europarl.europa.eu/cmsdata/179163/20090225ATT50418EN.pdf>>.
 21. *Government of Abu Dhabi*. n.d. 23 02 2024. <<https://es.adpolice.gov.ae/traffic-services/PublicServices/Introduction.aspx?Culture=en>>.
 22. *Apple – FBI encryption dispute*. 2016. 27.02.2024. <https://en.wikipedia.org/wiki/Apple%E2%80%93FBI_encryption_dispute>.
 23. *European Union Agency for Criminal Justice Cooperation*. n.d. 15.02.2024. <<https://www.eurojust.europa.eu/crime-types-and-cases/crime-types/cybercrime>>.

Cybercrime Victimization

PhD. student **Dora ARIFI**¹

Professor **Besa ARIFI**²

Abstract

Digitization has taken over the whole world and it's terrifying. The reason behind this is that the Internet offers many options for its users, some of which are very productive. Unfortunately, it also creates a space for hackers to operate freely and achieve their goals. As the number of internet users is increasing, cybercrime victimization is at the highest rate every day. Cybercrime is a new term that defines illegal activity that involves a network, computer, or network device. Cybercrime is a criminal offense committed against individuals or institutions. Anyone can be a victim of cybercrime. As a result, combating this type of crime presents a new challenge for law enforcement. It is crucial to understand the risks and consequences to take appropriate measures to protect the victims of such crimes. The paper is prepared based on other works to finally conclude that cybercrime is a worldwide problem, and no one is immune to it. We must raise awareness of the possible consequences and prevent future cyber victimization before it's too late.

Keywords: cybercrime, cyber legislation, victims, cyberstalking, cybersecurity.

JEL Classification: K14, K24

DOI: <https://doi.org/10.62768/ADJURIS/2024/1/12>

Please cite this article as:

Arifi, Dora & Besa Arifi „Cybercrime Victimization”, in Pajuste, Tiina, Heliona Bellani (Miço) & Sejla Maslo Cerbic (eds.), *Legal Perspectives in the Modern Era of Technological Transformations*, ADJURIS – International Academic Publisher, Bucharest, Paris, Calgary, 2024, p. 193-204.

1. Introduction

The Internet is a very powerful tool because it can change everything in a single second. For some users, the Internet brings pleasure and helps in a positive way to carry out work. It is entertaining and provides knowledge for all who are interested. For some people, the Internet is scary, unknown, and dangerous. The Internet today is burdened with information from various fields, including our private ones, because we as Internet users therefore of social networks, with the creation of accounts, and distribution of photos, videos, news, and thoughts,

¹ Dora Arifi - South-East European University, North Macedonia, da24612@seeu.edu.mk.

² Besa Arifi - South-East European University, North Macedonia, b.arifi@seeu.edu.mk.

we give information or data automatically for which, although it is considered to be protected when it comes to bank numbers, given identification, again part of the information we provide, are exposed at any moment to the risk of misuse by various hackers. Social networks are digital platforms that offer different ways of socialization communication, games, work, sharing funny content, etc. People should be careful of what they post on social media. Users post too much, providing personal information and making it easier for hackers to operate. Information on various fields can be found everywhere on the Internet, on websites, forums, books, and online works as well as on social networks. One of the main mistakes in why people become victims of cybercrime is the lack of knowledge regarding the policies of digital platforms and not utilizing privacy settings. Since social accounts are constantly at risk, we try to find the most effective solutions to prevent hacking and combat such crime with new methods, increase the awareness of some about the importance of the information we provide, etc. People sometimes forget that they publish so much data, making it accessible to everyone they know and don't know. Social media users often communicate with strangers with whom they share personal events and details. The scariest part of communicating with people who don't really know each other in person is the fact that they may often hide their true personalities. Some people tend to present a character built on lies and deception. In this way, hackers can easily plan threats, manipulation, and stalking, and cause much damage to victims. Often hackers and other cyber criminals present themselves as polite, ambitious, interested in relationships, and investments, and people dealing with different non-governmental firms or organizations for health, animals, children, etc.

2. Cybercrime is taking over the world

To understand the perspective of the victims of cybercrime (as well as the victims of what Nicole A. Vincent calls *cyberwrongs*³) it is first necessary to understand the offences; how they occur, and how the internet may enable perpetrators to commit them. Again, the dynamism of the cybersphere makes this task daunting given the dizzying speeds at which platforms and usage patterns materialize and dematerialise.⁴ Cybercriminals use the rapid connectivity of the internet to exploit the vulnerabilities of the network.⁵

Most people are unaware of this exploit, which makes bad individuals feel safe committing crimes in the digital era⁶. Hackers use social networks to

³ Nicole A. Vincent, *Victims of cybercrime: definitions and challenges*, in Elena Martellozzo, Emma A. Jane (eds.), *Cybercrime and its victims*, Routledge, London, New York, 2017, p. 27-42.

⁴ *Ibid.*, p. 33.

⁵ Emily Ngo, *Social Media: The Unseen Risks of Cybercrimes*, A Thesis Presented to the Faculty of Anna Maria College, 2020, <https://annamaria.edu/wp-content/uploads/2021/06/Emily-Ngo-Fall-2020.pdf>, p. 2.

⁶ Tariq Rahim Soomro, Mumtaz Hussain, *Social Media-Related Cybercrimes and Techniques for Their Prevention*, Applied Computer Systems, Volume 24 (2019): Issue 1 (May 2019), p. 9-17.

plan and as a tool to commit crimes. First, they think about the target and how they will commit the crime, collecting personal information of the victims because social networks present a whole ocean that serves data for each person very easily and very quickly, for that reason, it is said that they commit crimes in real time. Due to this a cybercriminal can gather all the information and can sell up to \$630 million yearly⁷. Victims will no longer have personal data.⁸ It hides the users' identity as well as not being able to face repercussions immediately.⁹ Computer crime is a new type of crime and also a unique one that differs from traditional crimes. At present, the risk of cybercrime can visualize in the form of offences analogous to the physical world, such as cyberbullying and online harassment which are termed as *cyber-enabled* crimes, or through security risks that affect the computer itself, such as malware infections, ransomware infections, and theft and misuse of personal data which is called *cyber-dependent* crimes.¹⁰

3. Types of cybercrimes

Cybercrime is a term used to broadly describe criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity and include everything from electronic cracking to denial-of-service attacks.¹¹ Cybercrimes can be easily placed into two categories; violent and nonviolent cybercrimes. Most of the cybercrimes are nonviolent offenses, because interaction is without any physical contact.¹² According to the author Vishi Aggarwal, 'Non-violent computer crimes are cyber theft (identity theft, piracy), cyber fraud, cyber trespass, and destructive cybercrimes such as cyber vandalism, and viruses, etc., crimes which are while violent computer crimes are cyber terrorism, cyberstalking, pornography, and cyberbullying.' Nonviolent crimes affect the financial and mental aspect, while violent ones, apart from having a negative impact on the mental aspect, endanger the well-being and life of the victims. Different categories of individuals are attacked virtually in different ways, for example, women and children are mostly targeted through cyberstalking, cyber threats by leaking their pictures, and text messages, harassment, and misuse of data for pornography. Men are also threatened in various ways for financial gain, and elderly people fall prey to viruses that are controlled by hackers. Since older people are not

⁷ Bir, A., & Sodhi, S. (2020). *Social media law & cybercrime*, pp. 28, 29.

⁸ Emily Ngo, *op. cit.*, p. 3.

⁹ *Ibid.*, p. 4.

¹⁰ P. Naveen Prabhu, K. Niranjana, *A Study on Cyber Crime Victims*, International Journal of Research Publication and Reviews, Vol. (2) Issue (9), 2021, p. 89, <https://www.ijrpr.com/v2i9.php> last accessed 01.03.2024.

¹¹ V. Karamchand Gandhi, *An Overview Study on Cybercrimes in the Internet*, Journal of Information Engineering and Applications, Vol. 2, No. 1, 2012, p. 1.

¹² Shruti Vishi Aggarwal, *Cybercrime victims: A comprehensive study*, International Journal of Creative Research Thoughts, Volume 6, Issue 2, 2018 p 641 the document is available at: https://ijcrt.org/viewfull.php?&p_id=IJCRT1807078, last accessed 01.03.2024.

internet experts, they often fall for the lies of hackers since they try to provide help for repairing the damages when in fact, they start stealing personal data such as collecting passwords into accounts to get access most of the time to their bank accounts. Companies, organizations, and institutions are also good targets of computer crime because it involves large sums of money. Hackers can weave the most detailed and advanced plans to achieve their goals at any cost. Victims of cybercrime are generally harmed financially. The consequences caused are also mental aspects because pressure, threats, fear, and stress are present at the time of the cybercrime process. For example, in the female gender, in most cases, the psychological consequences and PTSD are caused because hackers misuse and publish messages, videos, and pictures of them to push them to surrender and adhere to the plan they have woven to arrive at material gain. Famous and wealthy people face different kinds of cyber threats because most of the time, hackers decide to intercept their phone calls as a part of the plan to gain more information for their financial purposes. The data published without the victim's consent can be misused for a longer time by anyone since it can be accessible to any of the internet users. Millions of people and hundreds of businesses and organizations are victims of computer crime every year. The most frequent computer crimes that are committed and victimize individuals are: Cyber stalking – is very common nowadays. Cybercriminals target victims by using different types of social media through threats and harassment. The aim of stalking is to cause stress and fear. The reasons for cyberstalking may be hatred, obsession, and revenge. Cyber stalking can take many forms, including:

- harassment, embarrassment and humiliation of the victim;
- emptying bank accounts or other economic controls such as ruining the victim's credit score;
- harassing family, friends and employers to isolate the victim.¹³

Often the perpetrators are impossible to identify because they present themselves as anonymously by changing their identity on social networks and their IP address, making it impossible to find the location of the action. Hacking and Cracking – every act committed towards breaking into a computer and/or network is hacking.¹⁴ Hackers use their legal tools to commit crimes. On the contrary, crackers do not possess such tools, but by using someone else's tools, they damage the system and as a consequence, the victim. In many pieces of literature, crackers are known as 'bad people' because they undertake criminal actions for personal and financial reasons. On the other side, hackers are often hired by companies to control and change the company's systems and programs. Cyber pornography – it means the publication of erotic materials of victims on social networks, i.e. on the Internet. Many websites exhibit pornographic pictures, photos,

¹³ V. Karamchand Gandhi, *op. cit.*, p 1.

¹⁴ Kejal Chintan Vadza, *Cyber Crime & its Categories*, Indian Journal of Applied Research, Volume 3, Issue 5, 2011, p. 130, DOI:10.15373/2249555X/MAY2013/39.

writing, etc. Such materials can be produced quickly and cheaply through morphing or through sexual exploitation of women and children.¹⁵ Identity theft – impersonating to be someone else on the internet or creating a fake identity and then acquiring information from an individual is known as identity theft. Through identity fraud, purchases and transactions are carried out without the knowledge of the victim, leading him to great financial losses. Identity theft is carried out by hacking into the computers of individuals or organizations, using fake emails, using hacking to collect the necessary data, etc. Cyber trafficking – the impact of technology on trafficking of human beings is of particular concern during two stages of the trafficking process: recruitment and exploitation¹⁶. Plagiarism – the act of taking another person’s work without permission and using the same as ours. Plagiarism is punishable. Various systems detect works borrowed without permission. The more internet users there are, the more widespread this crime will be. The Oxford English Dictionary Online (OED Online) defines plagiarism as ‘the action or practice of plagiarizing; the wrongful appropriation or purloining, and publication as one’s own, of the ideas, or the expression of the ideas (literary, artistic, musical, mechanical, etc.) of another.’¹⁷ In order to avoid plagiarism, authors must give credit in any instance in which they use another author’s idea, opinion or theory; any facts, statistics, graphs or drawings; any pieces of information that are not common knowledge; quotations of another person’s actual spoken or written words; and paraphrased versions of another person’s spoken or written words.¹⁸ According to a cybersecurity report of 2022, it is said that “27% of Millennials and 34% of Gen Zers have lost their money or data due to harmful cyber activity, such as phishing, yet many of them fail to report the incidents or seek out cybersecurity training it”.¹⁹

¹⁵ Dr. Grace Varghese, *A sociological study of different types of cybercrime*, International Journal of Social Science and Humanities Research, Vol. 4, Issue 4, 2016, p. 603, the document is available at <https://www.researchpublish.com/papers/a-sociological-study-of-different-types-of-cyber-crime> last accessed 01.03.2024.

¹⁶ Dr. Paolo Campana, *Online and technology-facilitated trafficking in human beings. Summary and recommendations*, Council of Europe, 2022, p. 7, the document is available at <https://rm.coe.int/online-and-technology-facilitated-trafficking-in-human-beings-summary-/1680a5e10c>, last accessed 01.03.2024.

¹⁷ Patience Simmonds, *Internet Resources: Plagiarism and cyber-plagiarism: A guide to selected resources on the Web*, ACRL College & Research Libraries News, Vol. 64 No. 6, 2023 the documents is available online at: https://crln.acrl.org/index.php/crl_news/article/view/20607/25112 last accessed 10.03.2024.

¹⁸ Nm Lehobye, *Plagiarism: Misconduct awareness on novice research within the cyberworld*, Potchefstroom Electronic Law Journal (PER/PELJ), Volume 13 No. 3, 2010 p. 496.

¹⁹ Paige Gerald, *Cybersecurity report finds cybercrime victims are often Millennials and Gen Zers*, Information Security, 2022, the document is available online at: <https://it.rutgers.edu/2022/10/17/cybersecurity-report-finds-cybercrime-victims-are-often-millennials-and-gen-zers/> last accessed 10.03.2024.

4. How do cybercriminals operate?

Cybercriminals also exploit the natural desires of humans to trust others to send unsolicited electronic mail to unsuspecting victims as though they originated from legitimate sources.²⁰ Because victims of cybercrime are an invisible constituency, they are often overlooked by policy-makers and those who assist victims of traditional criminal offenses. Yet the harms are substantial and deserve greater attention.²¹ Most of the time fraudsters and hackers try to gain the victim's trust to achieve their goals. They work hard for weeks or months until they betray the victim and get the money. For most cybercrimes, no physical contact takes place between perpetrator and victim, and in the case of online banking fraud, victims are often compensated for financial damage. Because victimization impact cannot be measured based on physical injury and not always on actual financial damage, the impact of cybercrime seems to be underestimated, or cybercrime is even considered a victimless crime.²² Concerns over online anonymity, privacy, and security are valid. It is difficult to determine who exactly is the person online or how protected a person's data is over the internet²³. Cybercriminals use the rapid connectivity of the internet to exploit the vulnerabilities of the network. Most people are unaware of this exploit, which makes bad individuals feel safe committing crimes in the digital era²⁴. Cybercriminals most of the time use methods to scare victims and cause panic and fears in order to make them guess and not think rationally or make a scam believable by making the victim think they are doing the right thing. Cybercrime perpetrators can operate alone, as a group, or even as a criminal organization. Today there are such organizations that actually function like any other organization. Some criminals use their skills and knowledge to damage computer equipment, and software or block programs by publishing photos and other illegal information. Cybercriminals use phishing and phishing to achieve their goals. They also use different methods to change databases on many websites without authorization. They manipulate data or gain information such as passwords, trade secrets, credit card numbers, and other sensitive personal and government information. To further reduce the chances of detection, and prosecution, cybercriminals often choose to operate in countries with

²⁰ Obinna J. Eze, John Thompson Okpa, Chukwuemeka Dominic Onyejebu and Benjamin Okorie Ajah, *Cybercrime: Victims' Shock Absorption Mechanisms*. From the edited volume Eduard Babulak Malware – Detection and Defense, 2022, the document is available online at: <https://www.intechopen.com/chapters/83682> last accessed 12.03.2024.

²¹ Victims of cybercrime Workshop, Council of Europe p. 1 the documents is available online at: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016803075c3> last accessed 11.03.2024.

²² Jildau Borwell, Jurjen Jansen and Wouter Stol, *Comparing the victimization impact of cybercrime and traditional crime: literature review and future research directions*, Journal Digital Social Research, Vol. 3, No. 3, 2021, p. 96.

²³ Emily Ngo, *op. cit.*, p. 1.

²⁴ Tariq Rahim Soomro, Mumtaz Hussain, *op. cit.*, p. 9.

weak or nonexistent cybercrime laws.²⁵ As more people engage in an ever-increasing variety of online activities and more businesses conduct their affairs online, it is predictable that there would be a rise in cybercrime.²⁶

5. Challenges of cybercrime

In many ways, it is unsurprising that cybercrime has increased in recent years. As technology becomes more sophisticated, so do cybercriminals, and cybercriminals now target individuals, businesses, healthcare facilities, educational institutions, and governments.²⁷ Although an increased number of studies on the impact of crime on victims have been conducted, most of the work in this field focusses on traditional crimes such as violent crime, theft and criminal destruction, rather than cybercrime.²⁸ Some experts believe that cybercrime is nothing more than ordinary crime committed by high-tech computers where computer is either a tool or target or both and other expert view that cybercrime is a new category of crime requiring a comprehensive new legal framework to address a unique nature of emerging technologies and the unique set of challenges that traditional crime does not deal with such jurisdiction, international cooperation, intent and the difficulty of identifying a perpetrator²⁹. The challenges of the digital age and for the investigation of electronic crime or cybercrime or computer crime are numerous and diverse, and include:

Bridging multi-jurisdictional boundaries; Retaining and preserving evidence; Acquiring appropriate powers decoding encryption Proving Identity Knowing where to look for evidence Tackling the tools of crime and developing tools to counter crime Rethinking the costs and priorities of investigations responding to crime in real time coordinating investigative activities improving training at all levels of the organization developing strategic partnerships and alliances Improving the reporting of electronic crime Enhancing the exchange of information and intelligence Acquiring. Developing and retaining specialist staff; and avoiding “tech lag” (or getting access to cutting-edge technology).³⁰

Considering the importance of the internet in today’s world, experiencing a crime online might cause severe psychological issues in the individual (from

²⁵ Kate Brush, Michael Cobb, *Cybercrime, TechTarget*, 2021, revised 2024, the document is available online at: <https://www.techtarget.com/searchsecurity/definition/cybercrime> last accessed 14.03.2024.

²⁶ James Hawdon, *Cybercrime: Victimization, Perpetration and Techniques*, American Journal of Criminal Justice, 2021, vol. 46, <https://doi.org/10.1007/s12103-021-09652-7>, p. 838.

²⁷ *Ibid*, p. 837–838.

²⁸ Jildau Borwell, Jurjen Jansen, Wouter Stol, *op. cit.*, pp. 86–87.

²⁹ Neelesh Jain, Vibhash Shrivastava, *Cybercrime changing everything – an empirical study*, International Journal of Computer Application, Issue 4, Volume 1, 2014, p. 77, the document is available at https://www.researchgate.net/publication/275709598_CYBER_CRIME_CHANGING_EVERYTHING_-_AN_EMPIRICAL_STUDY last accessed 01.03.2024.

³⁰ *Ibid*, p. 82.

loss of trust to symptoms of post-traumatic stress disorder – PTSD – or suicide), as it potentially would after an offline crime.³¹ Cybercrime seems to challenge the principles upon which our conventional understandings of criminal harm and justice are based, because it results in the globalization of crime, new forms of victimization, extensive data trails, and changes in the organization of criminal activities.³² A restorative orientation is both more consistent with the policy objectives of “putting the victims” first’ and meeting victims’ needs and, given the challenges of policing global cybercrime and the low levels of investigatory and prosecutorial success, a more meaningful response to these crime types.³³ Finally, given the stigma associated with both being victimised and victims’ self-identification with states of ‘vulnerability’ more generally, while a vulnerability framework may be useful to understand and respond to victimisation in its wider context, framing the victim response as one that builds resilience may be more effective at reaching victims.³⁴

6. Cybercrime impact on victims

Cybercrime’s victims are very common nowadays. Examples of the unique cybercrime victimization elements are the scale on which victims can be approached, the technology that is part of the offense and its anonymity, intangibility, and remoteness.³⁵ Cybercrime generally leaves negative consequences for the victim like any other crime, but the damage is much longer. Any material published without the victim’s consent remains on the Internet for a long time. Anyone can access, misuse, and publish the victim’s photographs, videos, and other personal materials. The victims do not face fear, stress, and depression from this criminal activity but also must deal with the ‘victim blaming’ phase, where society blames the victim for the activity and deserves consequences. There are many cases where photos, videos, and other data are published to the victims, destroying their careers, family, marriage, and so on. Such a crime can happen through sending an email, call, advertisement, etc. It is crucial to take preventive measures and notice unusual activities on time. For example, we are logged out from our social media unexpectedly or cannot complete a bank transaction. In

³¹ Louisa von der Ahe, *Mental Wellbeing and Cybercrime: The Psychological Impact of Cybercrime on Victims*, University of Twente, 2022, p. 4, the document is available at <https://essay.utwente.nl/91014>, last accessed 01.03.2024.

³² Jildau Borwell, Jurjen Jansen and Wouter Stol, *op. cit.*, p 88.

³³ Sara Correia, *Cybercrime victims: victim policy through a vulnerability lens*, Cyber Threats Research Centre, Swansea University, 2021, p. 15 the document is available at: Correia, Sara, *Cybercrime Victims: Victim Policy through a Vulnerability Lens* (August 2, 2021). Available at SSRN: <https://ssrn.com/abstract=3897927> or <http://dx.doi.org/10.2139/ssrn.3897927> last accessed 01.03.2024.

³⁴ *Ibid*, p. 15.

³⁵ Jildau Borwell, Jurjen Jansen, and Wouter Stol, *The Psychological and Financial Impact of Cybercrime Victimization: A Novel. Application of the Shattered Assumptions Theory*, Sage Journals Volume 40, Issue 4, 2021, p. 3. <https://doi.org/10.1177/0894439320983828>.

such a way, when we feel that someone else controls our social networks or bank accounts, they understand that we have fallen victim to hackers and cybercrime. In the first moments, victims face panic and inexplicable fear because the fate of accounts and money is unknown. In some ways, a cyber-attack can feel like the digital equivalent of being robbed, with a corresponding wave of anxiety and dread.³⁶ Depending on the cybercrime, victimization may require law enforcement, medical, or psychiatric assistance because victims may become suicidal, depressed, nervous, anxious, fearful, or afraid.³⁷ Victimization can happen more than once. If the victim does not take certain protective measures, he may again fall victim to the same or different cyber-attacks. Electronic devices such as laptops used away from secure internet connections are vulnerable to external threats, since fraudsters sometimes offer free Wi-Fi connections or interfere with legitimate Wi-Fi connections to steal the personal information of individuals at airports or shopping malls.³⁸ Social media tools, a platform that is very open to manipulation and crime, also cause trust issues, especially due to the potential of creating fake profiles, fictitious and suspicious identities. When the texts, images, animated images, etc. shared without paying attention to the language used on social media platforms are used in an uncontrolled manner and spread to large masses, it creates a huge data cloud and causes content density.³⁹ Social networks when used in an uncontrolled or illegal manner bring problems and increase the predispositions for cyber victimization.⁴⁰ In an interview conducted (01.03.2024) with an 18-year-old female victim for the matter of the research, we see what trauma victims of computer crime experience and how much society should support them.

Q: What type of cybercrime have you been victimized by? When did it happen?

A: Hacking and publishing my photos. It happened a year ago.

Q: How did you feel in those moments?

A: My friends notified me about the photos published. They were very

³⁶ Amber Steel, *The Psychological Impact of Cyber Attacks*, LastPass, 2022 the documents is available online at: <https://blog.lastpass.com/posts/2022/08/the-psychological-impact-of-cyber-attacks> last accessed 15.03.2024.

³⁷ Claudia San Miguel, Kristina Morales, and Marcus Antonius Ynalvez, *Online Victimization, Social Media Utilization, and Cyber Crime Prevention Measures*, *Asia-Pacific Social Science Review* 20(4), p. 124, the document is available at https://rio.tamtu.edu/soc_sci_facpubs/7/, last accessed 15.03.2024.

³⁸ N. Akdemir, *Exploring the Human Factor in Cyber-enabled and Cyber-dependent Crime Victimization: A Lifestyle Routine Activities Approach*, Durham Research Online, 2020, p. 13, the document is available at <https://durham-repository.worktribe.com/output/1299418/exploring-the-human-factor-in-cyber-enabled-and-cyber-dependent-crime-victimisation-a-lifestyle-routine-activities-approach>, doi: <https://doi.org/10.1108/intr-10-2019-0400> last accessed 15.03.2024.

³⁹ Murat Eddogdu, Murat Kocuyigit, *The Correlation between Social Media Use and Cyber Victimization: Research on Generation Z in Turkey*, *Connectist: Istanbul University Journal of Communication Sciences*, Istanbul 2021, p. 3.

⁴⁰ *Ibid*, pp. 3-4.

personal, sent from my side on chats. I felt terrible. I cried. I was afraid of people. I isolated myself from everyone for a long time.

Q: What happened to your photos?

A: My social account was closed. My friends reported the account. Hackers posted everything on my account. Since then, I haven't noticed any criminal activity. I don't know if someone from my friend's list has the photos yet. It is scary.

7. Conclusion

Cybercrime is a widespread crime. Cyber-attacks are getting more advanced. Governments must take effective measures to prevent and slow down the cybercrime consequences by raising awareness, developing strategies, and improving current laws for combating cybercrime. In addition, organizing training for officers and other cybersecurity workers will be a preventive measure.

Maybe we will never be victims of cybercrime, but that doesn't mean we aren't in danger. Hackers are everywhere around us. Every moment by using their 'weapons' they can operate and cause damage. Therefore, I specifically mentioned the need to increase awareness because most people do not know the types of cybercrime except the 'hacking' type and are not informed about the basic preventive measures that they should take to protect themselves from victimization, such as using strong passwords, check secure websites, install and update anti-viruses, never open spam e-mails, never share personal information in suspicious sites, we need to secure our home network, always use a secure internet connection, never save passwords in the browsers, keep most of the personal information private on social media, make backups on data, etc. It is very important to educate children and teenagers since mostly they can easily fall victim to such crimes since they can be manipulated in many ways by cyber criminals.

Bibliography

1. Aggarwal, Shruti Vishi, *Cybercrime victims: A comprehensive study*, International Journal of Creative Research Thoughts, Volume 6, Issue 2, 2018, the document is available at: https://ijcrt.org/viewfull.php?&p_id=IJCRT1807078, last accessed 01.03.2024.
2. Ahe, Louisa von der, *Mental Wellbeing and Cybercrime: The Psychological Impact of Cybercrime on Victims*, University of Twente, 2022, the document is available at <https://essay.utwente.nl/91014>, last accessed 01.03.2024.
3. Akdemir, N., *Exploring the Human Factor in Cyber-enabled and Cyber-dependent Crime Victimization: A Lifestyle Routine Activities Approach*, Durham Research Online, 2020, the document is available at <https://durham-repository.worktribe.com/output/1299418/exploring-the-human-factor-in-cyber-enabled-and-cyber-dependent-crime-victimisation-a-lifestyle-routine-activities-approach>, doi: <https://doi.org/10.1108/intr-10-2019-0400> last accessed 15.03.2024.

4. Bir, A., & Sodhi, S. (2020). *Social media law & cybercrime*.
5. Borwell, Jildau, Jurjen Jansen & Wouter Stol, *Comparing the victimization impact of cybercrime and traditional crime: literature review and future research directions*, Journal Digital Social Research, Vol. 3, No. 3, 2021.
6. Borwell, Jildau, Jurjen Jansen & Wouter Stol, *The Psychological and Financial Impact of Cybercrime Victimization: A Novel. Application of the Shattered Assumptions Theory*, Sage Journals Volume 40, Issue 4, 2021, <https://doi.org/10.1177/0894439320983828>.
7. Brush, Kate & Michael Cobb, *Cybercrime, TechTarget*, 2021, revised 2024, the document is available online at: <https://www.techtarget.com/searchsecurity/definition/cybercrime>, last accessed 14.03.2024.
8. Campana, Paolo, *Online and technology-facilitated trafficking in human beings. Summary and recommendations*, Council of Europe, 2022, the document is available at <https://rm.coe.int/online-and-technology-facilitated-trafficking-in-human-beings-summary-/1680a5e10c>, last accessed 01.03.2024.
9. Correia, Sara, *Cybercrime victims: victim policy through a vulnerability lens*, Cyber Threats Research Centre, Swansea University, 2021, the document is available at: Correia, Sara, *Cybercrime Victims: Victim Policy through a Vulnerability Lens* (August 2, 2021). Available at SSRN: <https://ssrn.com/abstract=3897927> or <http://dx.doi.org/10.2139/ssrn.3897927> last accessed 01.03. 2024.
10. Eddogdu, Murat & Murat Kocyyigit, *The Correlation between Social Media Use and Cyber Victimization: Research on Generation Z in Turkey*, Connectist: Istanbul University Journal of Communication Sciences, Istanbul 2021.
11. Eze, Obinna J., John Thompson Okpa, Chukwuemeka Dominic Onyegbu & Benjamin Okorie Ajah, *Cybercrime: Victims' Shock Absorption Mechanisms*. From the edited volume Eduard Babulak Malware – Detection and Defense, 2022, the document is available online at: <https://www.intechopen.com/chapters/83682>, last accessed 12.03.2024.
12. Gandhi, V. Karamchand, *An Overview Study on Cybercrimes in the Internet*, Journal of Information Engineering and Applications, Vol. 2, No. 1, 2012.
13. Gerald, Paige, *Cybersecurity report finds cybercrime victims are often Millennials and Gen Zers*, Information Security, 2022, the document is available online at: <https://it.rutgers.edu/2022/10/17/cybersecurity-report-finds-cybercrime-victims-are-often-millennials-and-gen-zers/>, last accessed 10.03.2024.
14. Hawdon, James, *Cybercrime: Victimization, Perpetration and Techniques*, American Journal of Criminal Justice, 2021, vol. 46, <https://doi.org/10.1007/s12103-021-09652-7>.
15. Jain, Neelesh & Vibhash Shrivastava, *Cybercrime changing everything – an empirical study*, International Journal of Computer Application, Issue 4, Volume 1, 2014, the document is available at https://www.researchgate.net/publication/275709598_CYBER_CRIME_CHANGING_EVERYTHING_-_AN_EMPIRICAL_STUDY last accessed 01.03.2024.
16. Lehigh, Nm, *Plagiarism: Misconduct awareness on novice research within the cyberworld*, Potchefstroom Electronic Law Journal (PER/PELJ), Volume 13, No. 3, 2010.
17. Miguel, Claudia San, Kristina Morales & Marcus Antonius Ynalvez, *Online Victimization, Social Media Utilization, and Cyber Crime Prevention Measures*, Asia-Pacific Social Science Review 20(4), the document is available at <https://>

- rio.tamtu.edu/soc_sci_facpubs/7/, last accessed 15.03.2024.
18. Ngo, Emily, *Social Media: The Unseen Risks of Cybercrimes*, A Thesis Presented to the Faculty of Anna Maria College, 2020, <https://annamaria.edu/wp-content/uploads/2021/06/Emily-Ngo-Fall-2020.pdf>.
 19. Prabhu, P. Naveen & K. Niranjana, *A Study on Cyber Crime Victims*, International Journal of Research Publication and Reviews, Vol. (2) Issue (9), 2021, <https://www.ijrpr.com/v2i9.php> last accessed 01.03.2024.
 20. Simmonds, Patience, *Internet Resources: Plagiarism and cyber-plagiarism: A guide to selected resources on the Web*, ACRL College & Research Libraries News, Vol. 64 No. 6, 2023 the documents is available online at: https://crln.acrl.org/index.php/crl_news/article/view/20607/25112 last accessed 10.03.2024.
 21. Soomro, Tariq Rahim & Mumtaz Hussain, *Social Media-Related Cybercrimes and Techniques for Their Prevention*, Applied Computer Systems, Volume 24: Issue 1 (May 2019), p. 9-17.
 22. Steel, Amber, *The Psychological Impact of Cyber Attacks*, LastPass, 2022 the documents is available online at: <https://blog.lastpass.com/posts/2022/08/the-psychological-impact-of-cyber-attacks> last accessed 15.03.2024.
 23. Vadza, Kejal Chintan, *Cyber Crime & its Categories*, Indian Journal of Applied Research, Volume 3, Issue 5, 2011, DOI:10.15373/2249555X/MAY20 13/39.
 24. Varghese, Grace, *A sociological study of different types of cybercrime*, International Journal of Social Science and Humanities Research, Vol. 4, Issue 4, 2016, the document is available at <https://www.researchpublish.com/papers/a-sociological-study-of-different-types-of-cyber-crime> last accessed 01. 03.2024.
 25. Vincent, Nicole A., *Victims of cybercrime: definitions and challenges*, in Elena Martellozzo, Emma A. Jane (eds.), *Cybercrime and its victims*, Routledge, London, New York, 2017, p. 27-42.

Integrating AI in Bank Digitalization: Strategies, Challenges and Future Perspectives

PhD. student **Isabelle OPREA**¹

PhD. student **Daniela DUȚĂ**²

Abstract

The paper delves into the burgeoning role of artificial intelligence (AI) within the realm of banking digitalization. It begins by contextualizing the necessity for banks to adapt to digital transformation, driven by the increasing demand for efficient, personalized banking services and the pressure of fintech competitors. The core of the paper is dedicated to discussing the multifaceted strategies that banks are employing to integrate AI technologies, including automated customer service, fraud detection algorithms, and personalized financial advice systems. Moreover, the paper highlights significant challenges banks face in this integration process, such as data privacy concerns, and the need for substantial investment in technology and employees' training. The issue of a potential digital divide and its implications for customer access to banking services is also explored. Future perspectives are optimistically outlined, emphasizing AI's potential to revolutionize banking by further enhancing customer experience, optimizing operational efficiency, and fostering financial inclusion. The article argues that with thoughtful regulation, continuous innovation, and a focus on AI use, the integration of AI into banking can lead to more resilient and customer-centric financial institutions.

Keywords: artificial intelligence, banking financial system, AI Act, Convention on Artificial Intelligence, facial recognition.

JEL Classification: K22, K24

DOI: <https://doi.org/10.62768/ADJURIS/2024/1/13>

Please cite this article as:

Oprea, Isabelle & Daniela Duță, „Integrating AI in Bank Digitalization: Strategies, Challenges and Future Perspectives”, in Pajuste, Tiina, Heliona Bellani (Miço) & Sejla Maslo Cerkić (eds.), *Legal Perspectives in the Modern Era of Technological Transformations*, ADJURIS – International Academic Publisher, Bucharest, Paris, Calgary, 2024, p. 205-216.

¹ Isabelle Oprea - Doctoral School of Economic Sciences of the Romanian Academy, National Institute of Economic Research ‘Costin C. Kirițescu’, Romania, isabelle.oprea@gmail.com.

² Daniela Duță - School of Advanced Studies of the Romanian Academy (SCOSSAR), Legal Research Institute ‘Acad. Andrei Rădulescu,’; member of the Legal Research Laboratory Regarding New Technologies (‘LCJNT’) within the Legal Research Institute ‘Acad. Andrei Rădulescu’ of the Romanian Academy, ghituleasad@yahoo.com.

1. Introduction

Traditional banks are currently under significant pressure from customers and competition to undergo digital transformation, with Artificial Intelligence playing a key role in fulfilling these demands and significantly enhancing bank operations and performance. Sopra Steria, a top tech company in Europe known for its consulting, digital services, and software development, highlights that banks' efforts in digital transformation are starting to show positive outcomes. The introduction of artificial intelligence (AI) tools have accelerated their technological advancements, showcasing to a wider audience the beneficial effects such systems can bring to the banking sector.³ AI is revolutionizing the banking sector by enhancing customer service, refining risk management strategies, boosting operational efficiency, and paving the way for innovative business models.⁴ Financial fraud, which can lead to losses in the billions, is a significant issue for banks and financial institutions that process sensitive data online, thus heightening the risk of cyberattacks. Traditional fraud detection systems, which rely on predefined rules or algorithms, are now easily bypassed by sophisticated fraudsters. Consequently, an increasing number of companies are leveraging machine learning technologies to detect and prevent unauthorized financial activities. AI is instrumental in optimizing banking operations, minimizing expenses, and improving client experiences. Here are a few examples of AI's impact on the banking industry and the opportunities they offer:

- **Customer Experience:** The Amalgamation of Big Data analytics, AI, and blockchain technology is unlocking new possibilities in business and management, transforming operational procedures, and facilitating the creation of novel business models through digitalization. AI and Big Data enable banks to deliver personalized and streamlined services to their clients, utilizing tools like chatbots, voice assistants and robo-advisors. For instance, language models, which utilize natural language processing and machine learning to generate humanlike responses, can be used by banks to provide continuous customer support, financial guidance, and product recommendations.

- **Risk Management:** By analyzing vast datasets to identify patterns, anomalies, and behaviors, AI and Big Data can assist banks in detecting and averting fraud, money laundering, cyber threats, and other risks. AI-driven cybersecurity measures are designed to safeguard computer networks, programs,

³ Sopra Steria Report 2023. Digital Banking Experience Report 2023 Banks accelerate AI adoption amid growing Big Tech threat and customer demand for enhanced personalization and digitization. <https://www.soprasteria.com/mwg-internal/de5fs23hu73ds/progress?id=MH16g8eCuW8Acn1KN60vhjhp0Tg1I-Z8Fb2TfQzj0,&dl>

⁴ Sina Ahmadi. *A Comprehensive Study on Integration of Big Data and AI in Financial Industry and its Effect on Present and Future Opportunities*. International Journal of Current Science Research and Review, 2024, 07 (01), pp. 66–74.

and data from unauthorized access or attacks. For example, AI technologies enable banks to monitor transactions in real time, highlight unusual activities, and notify both customers and authorities of potential risks.

- **Efficiency:** AI contributes significantly to process automation, offering genuine insights, and identifying patterns and trends within datasets, which in turn makes operations more efficient and less labor-intensive. This reduces costs, minimizes errors, and improves overall productivity and efficiency. AI aids banks in assessing borrower reliability, processing credit applications swiftly and transparently, and providing loans to customers.

- **Business Models:** The Adoption of Big Data and AI tools facilitates the introduction of inventive services such as predictive analytics, social banking, behavioral finance, and open banking. These services not only enhance the banking experience and strengthen customer relationships but also open up new avenues for revenue generation. AI helps banks gather data on customer preferences and timely offer solutions to their problems, illustrating its potential to transform the banking landscape.⁵

Artificial Intelligence is emerging as a critical component of bank digital transformation strategy to meet customer digitalization demands and drive efficiency, with almost one-in-two banks (47%) planning to integrate AI into their business.⁶

2. Bank's AI strategies

For banks to fully harness the benefits of AI, a well-defined AI strategy is critical. Initially, banks must pinpoint business areas where AI can have the most impact, such as risk management, customer interaction, and operational efficiency. Following this, it's important to outline the AI initiative's scope and objectives, which might range from broad-scale implementation across various departments to targeted process automation. These objectives should align with the bank's overarching goals, like enhancing customer satisfaction or boosting profitability. The final step involves creating an implementation plan for the AI solution, which includes choosing the right technology, recruiting or upskilling AI talent within the bank, and establishing data requirements.

A successful AI deployment in the banking sector demands a robust AI strategy, continual investment in skilled personnel and infrastructure, and fostering a culture inclined towards innovation and exploration. Banks that adeptly integrate AI can offer superior customer service, diminish operational expenses, and maintain a competitive edge in the swiftly evolving market landscape. Nonetheless, AI integration is an ongoing endeavor necessitating perpetual enhance-

⁵ Ibid, p. 68 et seq.

⁶ Sopra Steria Report 2023, *op. cit.*

ments and updates. Consequently, banks need to commit to sustaining investments in AI expertise, technology, and infrastructure to keep their AI solutions efficient and pertinent over time.⁷

Today, many banks are testing AI applications within their operations, ranging from pilot projects to establishing a reputation as technology pioneers. Most are in various stages of adopting or implementing artificial intelligent systems. However, in order to maintain their competitiveness in the near future, banks need to elevate AI to a core element of their operations, rather than viewing it as an isolated project. Banks should transition from ad hoc AI implementations to fully integrating AI into their organizational fabric and culture, shifting from merely being AI-aware to becoming formidable AI competitors. Current strategies often focus on identifying the bank's specific objectives and ensuring they align with its mission and vision. During the strategy phase, executives must outline not just the objectives, but also the methods to achieve them, with a plan that covers how to: ensure access to the right data, foster a human centric and AI-centric culture throughout the organization, integrate AI applications into existing workflows, choose the appropriate AI technologies, keep AI initiatives ethical and minimize risks. Crafting an AI vision that encompasses these elements enables an organization to envision potential outcomes, setting priorities and goals that steer the AI adoption journey.⁸

3. Challenges and considerations for banks

The digital banking system has introduced a multitude of advantages, yet it faces significant hurdles. With the increasing number of digital transactions, cybersecurity risks are a major concern. Moreover, traditional banking face competition from innovative as FinTech startups that provide specialized services more affordably. Additionally, as world economies intertwine, banks must navigate the uncertainties of geopolitics and the complexities of cross-border regulations⁹. Nonetheless, these challenges also present opportunities for growth. The banking sector's future depends on its capacity to evolve, innovate, and meet the

⁷ Akinloose F., *The Three Pillars of Successful AI Implementation in Banking: Strategy, Talent, and Innovation*. Retrieved from <https://www.linkedin.com/pulse/three-pillars-successful-ai-implementation-banking-ph-d-scholar>, 2023. See also Cristina Elena Popa Tache, *Ranking of Treatment Standards in International Investments*, *International Investment Law Journal*, volume 1, Issue 1, February 2021, pp. 79-87; Cristina-Elena Popa Tache, *International investment protection in front of the states role in crisis times to managing disputes*, *Juridical Tribune - Tribuna Juridică*, volume 10, issue 3, December 2020, p. 455-465.

⁸ Omer Sohail, Prakul Sharma, Shailender Sidhu, Shawn Magill, Kairavi Bavishi, *Artificial intelligence: Transforming the future of banking*. Deloitte Report, 2021, <https://www2.deloitte.com/content/dam/Deloitte/us/Documents/process-and-operations/us-ai-transforming-future-of-banking.pdf>.

⁹ See some specific debates in Cristina Elena Popa Tache, *Public International Law and FinTech Challenge*, *Perspectives of Law and Public Administration*, Volume 11, Issue 2, June 2022, pp. 218-226.

changing demands of consumers and businesses.¹⁰ Despite the inspiring prospects that AI technology opens up for improving the customer experience in banking, implementing it into banking products can pose some challenges.¹¹ These challenges are¹²:

1. Transformation of existing processes, as a way to improve efficiency.
2. Change in customer behavior/digital customer experience. Customers are eager for banks to adopt best practices from other sectors, including high-quality service, swift transactions, robust security, data protection, competitive pricing, and round-the-clock availability. They expect banks to handle incidents effectively and offer pertinent solutions. Engaging digitally with customers necessitates continuous communication and proactive incident management.¹³

Another obstacle is encouraging customer usage of new technologies. Banks must make sure their clients are informed about and comfortable with using chat interfaces, necessitating improvements in user experience (UX) design and investment in educational initiatives to ensure the interface is user-friendly. With advancements in natural language processing and insights from customer data, AI has the potential to deliver a tailored, efficient, and convenient banking experience, enhancing overall customer service in the banking and financial sector.¹⁴

3. Technological innovations. A challenge for organizations adopting AI in their operations is that AI platforms vary in both scope and complexity, which hinders familiarity with them and hence their deployment to obtain competitive advantage.¹⁵

4. Data governance and reporting requirements.¹⁶

5. Improved solutions for the bank analysis (Big Data, Advanced Analytics).

¹⁰ Hassan, M., Aziz, L. A. R., & Andriansyah, Y. *The role of artificial intelligence in modern banking: an exploration of AI-driven approaches for enhanced fraud prevention, risk management, and regulatory compliance*. *Reviews of Contemporary Business Analytics* (2023) 6(1), 110–132. Cristina Elena Popa Tache, Constantin Brânzan, *L'évolution de la régulation bancaire et financière sous l'effet des règles de protection de la clientèle*, in *Banque et Droit N°HS-2023-1*, Paris, accessed at: <https://www.revue-banque.fr/espace-banque-droit/la-protection-des-consommateurs-de-services-bancaires-en-roumanie-entre-education-et-reforme-MD13766974>, in 06.04.2024.

¹¹ Kreger A. *The Future of AI in Banking*. 2023, <https://www.forbes.com/sites/forbesbusinesscouncil/2023/03/20/the-future-of-ai-in-banking/?sh=15bb453a5ed5>.

¹² Dan Costin Nitescu & Florin Alexandru Duna, 2018, *Managing Digitalization In Banking: Challenges And Implications*, Proceedings of the International Management Conference, Faculty of Management, Academy of Economic Studies, Bucharest, Romania, vol. 12(1), pp. 339-349, November.

¹³ *Ibid*, p. 342 et seq.

¹⁴ Kreger A., *op. cit.*, 2023.

¹⁵ Iansiti, M. & Lakhani, K., *Competing in the age of AI: Strategy and leadership when algorithms and networks run the world*. Boston, MA: Harvard Business Review Press (2020).

¹⁶ ESMA clarifies certain best execution reporting requirements under MiFID II: <https://www.esma.europa.eu/press-news/esma-news/esma-clarifies-certain-best-execution-reporting-requirements-under-mifid-ii>.

6. Cyber Security is a top priority for the banking business. Banks are using biometrics, behavioral analytics when proving services to the customers.

7. Regulatory and supervisory requirements (FinTech, the Internet of Things – IoT).

As AI regulatory framework continues to evolve, there's a possibility of variances in oversight and requirements between different regions. Such discrepancies could significantly impact many industries, with the banking sector being particularly affected due to its stringent regulatory environment and the higher risks it faces in terms of conduct, reputation, and systemic stability. With the increasing regulation of AI and new rules across key regions, banks could face penalties or even suspension of operations if AI models lead to undesirable customer outcomes (like discrimination or data breaches), contribute to avoidable risk management failures, or fall short of standards for transparency, safety, and robustness.

The pace at which AI is developing and being applied to new use cases means that regulatory responses can vary, leading to regional disparities and uncertainty regarding regulatory goals and requirements. This variation could affect the competitive dynamics within the industry. The regulation of AI is jurisdiction-specific, posing challenges for banks that operate internationally and must navigate a patchwork of regulations. For instance, in Europe, the EU AI Act could impose fines of up to 7% of a bank's revenue for regulatory infringements.¹⁷ Meanwhile, in China, provisional regulations on generative AI introduced in August 2023 are aimed at services available to the public.¹⁸

In this context, securing large volumes of data presents a significant challenge for an industry in which information plays a crucial role in determining profitability, alongside broader considerations of clientele and market share. Banks are required to maintain data storage for a certain period of time post-collection to meet regulatory standards.¹⁹ However, they must also adapt and to implement by altering specific policy, such as those introduced by the General Data Protection Regulation²⁰. This regulation represents the first comprehensive data protection law in Europe. Trust is fundamental in the banking sector, especially in the adoption of new technologies. The introduction of such regulations

¹⁷ EU AI Act proposal https://assets-global.website-files.com/637e4725db842e4068de0899/65c10bb08b530991de1cc9f9_AI%20ACT%20COREPER%20TEXT.pdf.

¹⁸ Fernández M. (2023). *AI in Banking: AI Will Be an Incremental Game Changer, Report*, S&P Global. <https://www.spglobal.com/en/research-insights/featured/special-editorial/ai-in-banking-ai-will-be-an-incremental-game-changer>.

¹⁹ Law no. 129 of July 11, 2019 for the prevention and combating of money laundering and terrorist financing, as well as for amending and supplementing certain normative acts, issuers, the Parliament of Romania, Published in the Official Gazette no. 589 of July 18, 2019.

²⁰ 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) OJ L 119, 4.5.2016, pp. 1–88.

can have a beneficial impact by reinforcing this trust.²¹

8. How to balance and mix human capital and technological capital. Transforming a bank requires a strategic management approach, led by a management team equipped with a blend of business and technical skills. The collaboration between the bank's IT and business functions is a crucial element in the management of digital transformation. The IT department must evolve its skills to keep pace with quick market shifts and embrace an agile operational framework. This approach enables the fast delivery of value and flexibility in resource allocation within the bank, supporting external reporting and meeting regulatory compliance demands.²²

9. New Architecture to accommodate the dynamic development for the ICT infrastructure, within a lively banking organization.

10. Strategic relationships with 'the right partners'. Building strategic partnerships with technological companies, buying and adapting business solutions, but also developing internal capacities and knowledge may support the change in the paradigm and the digitalization process in banking.²³

4. Legislative provisions

In addition to those already presented regarding remote video identification through electronic means²⁴, viewed both through the ADR Instruction²⁵ and the EBA Guide²⁶, a subject already addressed²⁷, as a novelty, the EU AI Regulation and the Council of Europe AI Convention must be taken into account.

On Wednesday, March 13, 2024, the European Parliament approved the Artificial Intelligence Act.²⁸ Focusing on safety, respect for fundamental rights,

²¹ Dan Costin Nitescu & Florin Alexandru Duna, *op. cit.*, p. 342 et seq.

²² *Ibid.*, p. 343.

²³ *Ibid.*, p. 344.

²⁴ Daniela Duță, *Remote identification using facial recognition. Data protection and privacy concerns* prepared for the International Conference 'Challenges of Doing Business in the Global Economy' CBGE 2022, IX Edition, Bucharest, May 13–14, 2022, organized by the 'Dimitrie Cantemir' Christian University; RRDE 44 (2022): <https://heinonline.org/HOL/LandingPage?handle=hein.journals/rianrwoe2022&div=27&id=&page>.

²⁵ Instruction no. 4/2023 for the implementation of the Guide on the use of remote customer recording solutions under Article 13(1) of Directive (EU) 2015/849, Official Gazette, Part I, no. 964/25 October 2023.

²⁶ Guide on the use of remote customer recording solutions under Article 13(1) of Directive (EU) 2015/849, EBA/GL/2022/15, 22/11/2022.

²⁷ Daniela Duță, Isabelle Oprea, *The Role of Artificial Intelligence in the Digital Banking System*, in Cristina Elena Popa Tache, Renata Treneska Deskoska, Nathaniel Boyd (eds.), *Adapting to Change Business Law Insights from Today's International Legal Landscape*, ADJURIS – International Academic Publisher, Bucharest · Paris · Calgary, 2024, p. 230-244, <https://adjuris.ro/reviste/acbl/Adapting%20to%20Change%20Business%20Law%20Insights.pdf>.

²⁸ Artificial Intelligence Act: MEPs adopt landmark law, Press Releases: <https://www.europarl.europa.eu/news/en/press-room/20240308IPR19015/artificial-intelligence-act-meps-adopt-landma>

and innovation, the AI Act aims to establish common rules and obligations for AI systems within the EU.

The Framework Convention on Artificial Intelligence, Human Rights, Democracy, and the Rule of Law (draft treaty) was finalized on Thursday, March 14, 2024, by the Council of Europe's Artificial Intelligence Committee.

The Council of Europe's AI Convention is an international treaty that extends beyond the EU and binds the 46 member states of the Council of Europe and nine non-European countries, representing a global 'normative' instrument for AI regulation based on human rights, democracy, and the rule of law, once ratified by the CoE member states.²⁹

While the EU AI Regulation emphasizes a risk-based approach to regulate AI systems in the EU, the Council of Europe's AI Convention aims to establish international standards for AI regulation, aiming to be a broadly accepted framework beyond Europe.

5. Future perspectives

AI's potential impact on the finance function extends beyond just the immediate benefits.

The capacity for AI to automate report creation, enhance forecasting accuracy, and manage compliance through the verification of statutory reporting disclosures will revolutionize the way finance teams interact with data. This transformation will facilitate deeper insights, improving decision-making and possibly uncovering new avenues for business expansion.

Looking ahead, future finance centers of excellence will utilize AI and other cutting-edge technologies to provide quicker, more cohesive financial analytics and insights. Key advancements could include:

- enhanced forecasting accuracy by integrating enterprise data with external information like customer behavior (with the consent of the customers for their use);

- a deeper comprehension of strategic risk and resilience, featuring predictive early warning systems;

- more interconnected financial reporting that informs key performance indicators (KPIs), stakeholder management, and multichannel communication.³⁰

With swift technological progress, AI is becoming a crucial part of the banking and financial services sector. Its capability to process and analyze large

rk-law.

²⁹ Artificial Intelligence, Human Rights, Democracy and the Rule of Law Framework Convention, <https://www.coe.int/en/web/portal/-/artificial-intelligence-human-rights-democracy-and-the-rule-of-law-framework-convention>.

³⁰ Burns K., 2023. *The CFO, the finance function and the future with AI*. Retrieved from <https://www.charteredaccountants.ie/Accountancy-Ireland/Articles2/News/Latest-News/the-cfo-the-finance-function-and-the-future-with-ai> on the 13th of March 2024.

datasets, recognize patterns, and forecast outcomes offers the potential to transform operations within financial institutions.

AI's influence is already evident in various areas, including fraud prevention, risk assessment, customer support, and tailored services, and this is merely the initial phase.

As the industry navigates through regulatory and privacy challenges, the future is likely to witness an expanded adoption of AI solutions in banking and financial services, further revolutionizing the sector.³¹

6. Conclusion

Banks must adopt a forward-thinking approach, embracing technological advancements to stay relevant. Importantly, their primary focus should be on enhancing and delivering services that prioritize the customer's perspective, which is essential for crafting an exceptional customer experience. The value proposition of fourth-generation banks increasingly relies on fostering collaboration between banks and their customers.

Moreover, it's crucial for banks to form partnerships with tech and knowledge-driven companies to pioneer innovative operational practices. In the near future, banks will resemble tech companies closely and will need to engage with these entities to expedite their transformation and business model evolution. In the context of Industry 4.0, economies that prioritize digitizing their assets, activities, and focus are poised for success. The integration of technology in banking is still a relatively fresh endeavor globally, marking the beginning of a significant shift in how financial services.³²

Banks are increasingly acknowledging the transformative impact of cutting-edge technologies and, crucially, are beginning to adopt them. Over time, the ability of banks to compete may hinge significantly on their capacity to establish the technological infrastructure and workflows necessary to harness the full potential of AI. However, there's a possibility that technological progress could surpass the rate at which the industry adapts, despite banks moving swiftly towards modernization. For banks to fully leverage the future advantages of AI, it's imperative they maintain their current trajectory towards innovation. This commitment, while essential, may prove challenging for some institutions.³³

Navigating the digital transformation in banking demands considerable time, adaptability, extensive testing, financial investment, and compliance with

³¹ Bristol A. 2023. *Artificial Intelligence (AI) and its Impact on the Future of Banking and financial services*. Retrieved from <https://fortyseven47.com/blog/artificial-intelligence-ai-and-its-impact-on-the-future-of-banking-and-financial-services/> on the 13th of March 2024.

³² Mehdiabadi, A., Tabatabaieinasab, M., Spulbar, C., Karbassi Yazdi, A., & Birau, R. (2020). *Are we ready for the challenge of Banks 4.0? Designing a roadmap for banking systems in Industry 4.0.* International Journal of Financial Studies, 8(2), 32, p. 10 et seq.

³³ Omer Sohail, Prakul Sharma, Shailender Sidhu, Shawn Magill, Kairavi Bavishi, *op. cit.*, 2021.

regulatory constraints. Banks must dedicate both financial and temporal resources, upskill their workforce, bring in external specialists, and find the optimal equilibrium between digital and physical services while ensuring data privacy and security risk management. Simultaneously, they need to maintain their ongoing business operations.³⁴

Bibliography

1. Ahmadi, Sina, *A Comprehensive Study on Integration of Big Data and AI in Financial Industry and its Effect on Present and Future Opportunities*. International Journal of Current Science Research and Review, 2024, 07 (01), pp. 66–74.
2. Akinloose F., *The Three Pillars of Successful AI Implementation in Banking: Strategy, Talent, and Innovation*. Retrieved from <https://www.linkedin.com/pulse/three-pillars-successful-ai-implementation-banking-ph-d-scholar>, 2023.
3. Artificial Intelligence Act: MEPs adopt landmark law, Press Releases: <https://www.europarl.europa.eu/news/en/press-room/20240308IPR19015/artificial-intelligence-act-meps-adopt-landmark-law>.
4. Artificial Intelligence, Human Rights, Democracy and the Rule of Law Framework Convention, <https://www.coe.int/en/web/portal/-/artificial-intelligence-human-rights-democracy-and-the-rule-of-law-framework-convention>.
5. Bristol A., 2023. *Artificial Intelligence (AI) and its Impact on the Future of Banking and financial services*. Retrieved from <https://fortyseven47.com/blog/artificial-intelligence-ai-and-its-impact-on-the-future-of-banking-and-financial-services/> on the 13th of March 2024.
6. Burns K., 2023. *The CFO, the finance function and the future with AI*. Retrieved from <https://www.charteredaccountants.ie/Accountancy-Ireland/Articles2/News/Latest-News/the-cfo-the-finance-function-and-the-future-with-ai> on the 13th of March 2024.
7. Duță, Daniela & Isabelle Oprea, *The Role of Artificial Intelligence in the Digital Banking System*, in Cristina Elena Popa Tache, Renata Treneska Deskoska, Nathaniel Boyd (eds.), *Adapting to Change Business Law Insights from Today's International Legal Landscape*, ADJURIS – International Academic Publisher, Bucharest · Paris · Calgary, 2024, p. 230-244, <https://adjuris.ro/reviste/acbl/Adapting%20to%20Change%20Business%20Law%20Insights.pdf>.
8. Duță, Daniela, *Remote identification using facial recognition. Data protection and privacy concerns* prepared for the International Conference ‘Challenges of Doing Business in the Global Economy’ CBGE 2022, IX Edition, Bucharest, May 13–14, 2022, organized by the ‘Dimitrie Cantemir’ Christian University; RRDE 44 (2022): <https://heinonline.org/HOL/LandingPage?handle=hein.journals/rianrwioe2022&div=27&id=&page>.
9. EU AI Act proposal https://assets-global.website-files.com/637e4725db842e4068de0899/65c10bb08b530991de1cc9f9_AI%20ACT%20COREPER%20TEXT.pdf.
10. Fernández M. (2023). *AI in Banking: AI Will Be an Incremental Game Changer*,

³⁴ Dan Costin Nitescu & Florin Alexandru Duna, *op. cit.*, p. 342 et seq.

- Report*, S&P Global. <https://www.spglobal.com/en/research-insights/featured/special-editorial/ai-in-banking-ai-will-be-an-incremental-game-changer>.
11. Hassan, M., Aziz, L. A. R., & Andriansyah, Y. *The role of artificial intelligence in modern banking: an exploration of AI-driven approaches for enhanced fraud prevention, risk management, and regulatory compliance*. *Reviews of Contemporary Business Analytics* (2023) 6(1), 110–132.
 12. Iansiti, M. & Lakhani, K., *Competing in the age of AI: Strategy and leadership when algorithms and networks run the world*. Boston, MA: Harvard Business Review Press (2020).
 13. Instruction no. 4/2023 for the implementation of the Guide on the use of remote customer recording solutions under Article 13(1) of Directive (EU) 2015/849, Official Gazette, Part I, no. 964/25 October 2023.
 14. Kreger A., *The Future of AI in Banking*. 2023, <https://www.forbes.com/sites/forbesbusinesscouncil/2023/03/20/the-future-of-ai-in-banking/?sh=15bb453a5ed5>.
 15. Law no. 129 of July 11, 2019 for the prevention and combating of money laundering and terrorist financing, as well as for amending and supplementing certain normative acts, issuers, the Parliament of Romania, published in the Official Gazette no. 589 of July 18, 2019.
 16. Mehdiabadi, A., Tabatabeinasab, M., Spulbar, C., Karbassi Yazdi, A., & Birau, R. (2020). *Are we ready for the challenge of Banks 4.0? Designing a roadmap for banking systems in Industry 4.0.*, *International Journal of Financial Studies*, 8(2), 32.
 17. Nitescu, Dan Costin & Florin Alexandru Duna, 2018, *Managing Digitalization In Banking: Challenges And Implications*, Proceedings of the International Management Conference, Faculty of Management, Academy of Economic Studies, Bucharest, Romania, vol. 12(1), pp. 339-349, November.
 18. Popa Tache, Cristina Elena & Constantin Brânzan, *L'évolution de la régulation bancaire et financière sous l'effet des règles de protection de la clientèle*, in *Banque et Droit N°HS-2023-1*, Paris, accessed at: <https://www.revue-banque.fr/espace-banque-droit/la-protection-des-consommateurs-de-services-bancaires-en-roumanie-entre-education-et-reforme-MD13766974>, in 06.04.2024.
 19. Popa Tache, Cristina Elena, *Public International Law and FinTech Challenge*, *Perspectives of Law and Public Administration*, Volume 11, Issue 2, June 2022, pp. 218-226.
 20. Popa Tache, Cristina Elena, *Ranking of Treatment Standards in International Investments*, *International Investment Law Journal*, volume 1, Issue 1, February 2021, pp. 79-87.
 21. Popa Tache, Cristina-Elena, *International investment protection in front of the states role in crisis times to managing disputes*, *Juridical Tribune - Tribuna Juridică*, volume 10, issue 3, December 2020, p. 455-465.
 22. 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) OJ L 119, 4.5.2016, pp. 1–88.
 23. Sohail, Omer & Prakul Sharma, Shailender Sidhu, Shawn Magill, Kairavi Bavishi, *Artificial intelligence: Transforming the future of banking*. Deloitte Report,

- 2021, <https://www2.deloitte.com/content/dam/Deloitte/us/Documents/process-and-operations/us-ai-transforming-future-of-banking.pdf>.
24. Sopra Steria Report 2023. Digital Banking Experience Report 2023 Banks accelerate AI adoption amid growing Big Tech threat and customer demand for enhanced personalization and digitization. <https://www.soprasteria.com/mwg-internal/de5fs23hu73ds/progress?id=MH16g8eCuW8AcnlKNN60vhjhpF0Tg1I-Z8Fb2TfQzj0,&dl>.

Information Support for Combating Criminal Offences by the State Border Guard Service of Ukraine

Associate professor **Iryna KUSHNIR**¹
Senior researcher **Yuliia STEPANOVA**²

Abstract

The article deals with the research of information support for combating criminal offences of the State Border Guard Service of Ukraine taking into account the criminological aspect. This area of information support is directly related to the development of the modern information digital society. The State Border Guard Service of Ukraine (SBGSU) uses modern methods and technologies of criminology to combat criminal offences. The need to improve the organisational and legal instruments (methods) of information support and continuous improvement of information technologies in the field of combating criminal offences determine the relevance of the research topic raised in the article. The purpose of the article is to study, identify the peculiarities and prospects of using information support for combating criminal offences by the SBGSU in the criminological aspect. The methodological basis of the research was formed by a combination of general scientific, sectoral and special scientific methods, which enabled to achieve the research objective when applied in a comprehensive manner. The dialectical method made it possible to consider information support as a complex legal phenomenon in the search for opposites of the essence, elements, and features in their interconnection. The structural and functional method was used to establish the components of information support and the relationship between them. The formal and logical method enabled to formulate concepts and identify areas of information support for combating criminal offences by the SBGSU. To formulate proposals for improving information support for combating criminal offences, the forecasting method was used. Within the article: the essence of information support is clarified; the information support of criminological monitoring is studied; the possibilities of risk analysis as a component of information support of criminological monitoring are analysed; information support for combating criminal offences based on open data is considered; the prospects for using artificial intelligence are studied, and promising directions for information support for combating criminal offences by the State Border Guard Service of Ukraine are proposed.

Keywords: *information support, cross-border crime, information systems, artificial intelligence, criminological monitoring, risk analysis.*

JEL Classification: K14, K24

DOI: <https://doi.org/10.62768/ADJURIS/2024/1/14>

¹ Iryna Kushnir - Deputy Chief of Administrative Activities Department of the Bohdan Khmelnytskyi National Academy of the State Border Guard Service of Ukraine, ikushnir010@gmail.com.

² Yuliia Stepanova - Deputy Chief of the Scientific Research Department of the Bohdan Khmelnytskyi National Academy of the State Border Guard Service of Ukraine, yulia.sp81@ukr.net.

Please cite this article as:

Kushnir, Iryna & Yuliia Stepanova, „Information Support for Combating Criminal Offences by the State Border Guard Service of Ukraine”, in Pajuste, Tiina, Heliona Bel-lani (Miço) & Sejla Maslo Cerkcic (eds.), *Legal Perspectives in the Modern Era of Technological Transformations*, ADJURIS – International Academic Publisher, Bucharest, Paris, Calgary, 2024, p. 217-235.

1. Introduction

Information support as a component of the criminological support for combating criminal offences by the State Border Guard Service of Ukraine (hereinafter – SBGSU) is to create and operate an information system which, on the one hand, would ensure the information security of the SBGSU, and on the other hand, would cover the information process of collecting, accumulating, storing, transmitting information required by the SBGSU to combat crime, and ensure information interaction with other law enforcement agencies, in particular, the subjects of integrated border management in the field of combating crime.

The development of the SBGSU information component is taking place in parallel with the processes occurring in society – processes that are caused by the improvement of information technologies, methods of analysis, information processing and the development of artificial intelligence. The state of such support should be in line with the current development of information processes. Because cross-border crime in Ukraine is constantly undergoing transformation. In the conditions of globalisation of political, economic, information and communication processes, national crime is transforming into transnational international forms³. Persons involved in illegal activities use the most up-to-date technical equipment, surveillance systems and covert receipt or transmission of information necessary for illegal activities in ultra-profitable areas, and further ways of legalising (laundering) the proceeds of crime.

For this reason, the regulatory framework in this area needs to be constantly improved. The peculiarity of the information support for combating crime by the SBGSU is in its close interconnection with the information support for integrated border management. Information cooperation in integrated border management is considered as a separate area of joint activities of law enforcement agencies in ensuring border security⁴. Currently, the problems of information support for integrated border management are as follows:

³ Gubanova E. V., *Criminality as Negative Aspect of Globalization*. Scientific Notes of Tavrida National V. I. Vernadsky University. Series: Juridical sciences. 2013. Vol. 26 (65). No. 1., p. 177.

⁴ Vikhtiuk A. V., *Legal and regulatory framework for information cooperation in integrated border management. Priority areas of science development during martial law*, XCII International Scientific and Practical Internet Conference. City of Odesa, 24 June 2022, p. 77.

- the need to develop effective mechanisms of interaction and information exchange, including automated, on possible violations of the law or identification of suspicious persons and transactions;
- insufficient speed of processing and transmission of information, which prevents from timely responding to changes in the operational situation;
- the need to continue technical re-equipment, increase the automation of processes in the field of integrated border management, introduce European standards, and ensure the development of information exchange between all subjects of integrated border management⁵.

The above aspects determine the relevance of the subject of our research.

2. The essence of information support

Stokorosa T. M. understands the concept of "information support" as a dynamic system of obtaining, evaluating, storing and processing data created for the purpose of making management decisions. The scientist reasonably points out the dual role of information support – both as a process of providing information and as a set of regulatory framework, forms of documents, implemented decisions on the scope, placement and forms of existence of information used in the information system in the process of functioning⁶.

However, this definition covers only the intellectual component of information support. As can be seen from the above problematic issues outlined in the Integrated Border Management Strategy, effective information support is possible if both intellectual and technical components are adequate. The intellectual component, in turn, is based on a methodology that allows obtaining the information necessary to make timely and correct decisions in combating crime and training of specialists of the appropriate level capable of providing the product of the required quality with proper technical equipment.

Revealing the features of information support of administrative and jurisdictional activities of law enforcement agencies, Shoptenko S. S. focuses on the process of providing, collecting, processing, analysing, systematising and recording information about an administrative legal dispute or administrative offence⁷. However, today the object of information and analytical activity as a component of information support for combating criminal offences by the SBGSU is not only information about a criminal offence, but a much wider range of statistical information and data on socio-political processes that have an impact on crime, information about the identity of a criminal offender, which allows for its

⁵ Integrated Border Management Strategy for the period up to 2025, approved by the Cabinet of Ministers of Ukraine on 24 July 2019 No. 687-r.

⁶ Stokorosa T. M., *Informatisation and information support: approaches to the interpretation of concepts*. Scientific Bulletin of NFU of Ukraine. 2008. Issue 18.9, p. 299.

⁷ Shoptenko S. S. *Administrative and jurisdictional activities of law enforcement agencies of Ukraine*: S.J.D thesis abstract: 12.00.07. Kharkiv. 2018, p. 21.

criminological profiling.

Analysing the information support of border control, Kushnir I. P., Kuryliuk Yu. B. and Filippov S. O. defined it as a set of information of appropriate expression and fixation, which is important and decisive for a particular legal situation, the performance of a specific task in the SBGSU activities, in particular for carrying out border control at air border crossing points on the state border of Ukraine. The scientists note that information support involves processing a wide range of information that ensures the fulfilment of the SBGSU tasks⁸.

So, information support of public administration in the activities of the state border protection bodies of Ukraine is a complex integrated concept that involves the management of information flows, use and processing of information that forms the basic principles and contributes to the creation of conditions for public administration in the field of state border protection of Ukraine, implementation of specific tasks and functions defined in the legislation or in certain areas (for example, combating criminal offences).

3. Information support for criminological monitoring

Scientific sources identify the following methods of information support in combating crime: statistical observation, analysis of criminal proceedings, analysis of reports, analytical information, surveys of members of the public, victimisation monitoring of individuals, content monitoring of Internet resources, method of expert assessments⁹. Each of them has its own advantages and peculiarities and can be used in combating criminal offences by the SBGSU, taking into account the peculiarities of the object and subject of this activity. At the same time, they can be used both separately and in a logical combination of all or several methods, depending on the purpose of the study. It seems that such a comprehensive activity to study the array of information necessary to combat criminal offences falls under the signs of criminological monitoring – a concept that has received considerable attention in criminology today, given that its application enables to take into account globalisation processes and the development of information technology in combating crime.

The scientific basis for the implementation of criminological monitoring is found in the research of Bandurka O. M., Blazhkiivskiyi Ye., Kovalenko A. V., Litvinov O. M., Maslova N. H., Myroniuk D., Sydorenko N. S., Orlov Yu., Fomenko A. Ye., Mukto M., Hitesh K. R., Kamalruddin S. The term "monitoring" is used by scientists in such terminological constructions as "crime monitoring" and "law enforcement monitoring", "monitoring of the state and trends of the

⁸ Kushnir I. P., Kuryliuk Yu. B., and Filippov S. O., *Information support of border control at airport border crossing points on the state border of Ukraine*. Air and space law. 2021. Vol. 4. No. 61, p. 18-19.

⁹ Beschastyi V. M., *Methods of information support as tools for collecting and processing information on crime*. Law and Society. 2017. No. 1. p. 206–212.

spread of terrorism"¹⁰, "monitoring of the crime situation", "monitoring of the operational situation".

Criminological monitoring is a system of observation, measurement and assessment of the state of a certain phenomenon or process in different periods of time, based on the knowledge of the regularities of its development, determined by practical necessity¹¹. It is the operational and analytical core of the management component of the crime prevention system, which provides the process of making criminologically significant decisions with complete (reliable), timely, comprehensive, prognostic information. It determines the adaptability, flexibility, and proactive nature of criminal prevention activities¹².

Since it is about the use of criminological monitoring to counter criminal offences by the SBGSU, the phenomenon under study – the main object – is a certain part of crime, which is manifested in the totality of criminal offences counteracted by the SBGSU. In addition, the object of criminological monitoring can include "background" phenomena for crime (alcoholism, drug addiction, prostitution), causes and conditions (determinants), social consequences of crime, the degree of criminalisation of society, individual criminal offences in the dynamics of changes in individual components of their mechanism, depending on the object of the offence, methods, means, motives for committing the crime; the state of combating crime¹³, – those elements, knowledge of which in the course of implementation of the practical and transformative function of criminology can be used to improve the fight against crime.

The following stages of criminological monitoring are distinguished: 1) pre-monitoring stage; 2) diagnostic stage; 3) evaluation stage; and 4) post-monitoring stage¹⁴. The content of these stages shows the integrity of the research process, which begins with the formulation of goals, objectives, terms, hypotheses, research tools and techniques, adaptation of methods to a specific purpose and conditions of the research, and continues with the collection of information about the factors that affect the object of research, as well as the object of research itself, and the assessment of the possibility of solving problematic issues using the available forces and facilities. During criminological monitoring, recommendations are developed to optimise relevant activities and select means of influencing negative trends; monitoring findings are provided for further use, taking

¹⁰ Regulation on the Unified State System of Prevention, Response and Suppression of Terrorist Acts and Minimisation of Their Consequences, approved by the Cabinet of Ministers of Ukraine on 18 February 2016, No. 92. URL: <https://zakon.rada.gov.ua/laws/show/92-2016-%D0%BF#n9>.

¹¹ Lytvynov O., *Criminological monitoring*, Bulletin of the Criminological Association of Ukraine. 17 March 2018. URL: <https://visnikkau.webnode.com.ua/news/kriminologichnij-monitoring/>.

¹² Orlov Yu. V., Myroniuk D. M., *Criminological monitoring of the legal regulation effectiveness as a tool for combating crime*. Bulletin of the Criminological Association of Ukraine. 2014. No. 6. p. 161–177.

¹³ Blazhkovskiy Ye. *Monitoring the fight against crime in Ukraine*: monograph. Kharkiv: Zolota mylia, 2013. 372 p.

¹⁴ Lytvynov O., *op. cit.*

into account the needs of practice, control over the implementation of relevant measures, evaluation of their effectiveness and adjustment if necessary.

The specificity of criminological monitoring in the SBGSU is that at each of these stages, information cooperation in integrated border management with both national and international partners takes place (or may take place, depending on the need).

4. Risk analysis as a component of information support for criminological monitoring

The components of criminological monitoring in the SBGSU are risk analysis, risk profiling and criminal analysis, which are implemented systematically on an ongoing basis. Also, there are *other specific information support measures* carried out at the departmental, national and international levels.

The risk analysis system has been implemented in the SBGSU since 2006. Since then, three programmes have been implemented to introduce a risk management system in the SBGSU¹⁵. This system is based on the principles set out in the Integrated Border Management Strategy, has an anti-crime focus and is an integral part of integrated border management.

Since its introduction, the SBGSU risk analysis system has been developing in three areas: 1) the functioning of analytical centres established by the integrated border management entities; 2) improvement of information exchange and joint risk analysis with the border services of foreign countries and Frontex; 3) cooperation with Frontex, EUAM, EUBAM, IOM and OSCE on the exchange of statistical information, joint assessment of certain types of illegal activities¹⁶.

Risk analysis in the SBGSU is defined as a set of procedures and methods for processing information in order to identify existing and potential risks in the sphere of state border security¹⁷. It is aimed at providing information and analytical support for managerial decision-making to identify existing (potentially possible) risks and preventive response to manifestations of cross-border illegal activity at the state border of Ukraine, in particular by risk profiling in conditions of limited resources and capabilities¹⁸.

Types of risk analysis by level are strategic, operational and tactical; by purpose – periodic, thematic, and situational. The risk analysis process begins with an assessment of local, regional, national and global threats. These activities

¹⁵ Risk analysis / Border protection / Activities. State Border Guard Service of Ukraine. Official website. URL: <https://dpsu.gov.ua/ua/rozvitok-sistemi-analizu-rizikiv-derzhprikordonsluzhbi/>.

¹⁶ Ibid.

¹⁷ Guidelines for conducting risk analysis in the State Border Guard Service of Ukraine, approved by Order of the Ministry of Internal Affairs of Ukraine No. 1007 on 11 December 2017. URL: <https://zakon.rada.gov.ua/laws/show/z0091-18#Text>.

¹⁸ Integrated Border Management Strategy for the period up to 2025, approved by the Cabinet of Ministers of Ukraine on 24 July 2019 No. 687-r.

are based on the following information: information received in the course of operational activities, from international organisations, border guard and other authorised bodies of foreign states, in accordance with international agreements, mass media, including the Internet, results of strategic analysis, own analytical developments; intelligence, operational and investigative data (if necessary). It is also necessary to take into account other sources of information support of the SBGS, such as: social networks, messengers, databases in information systems, video surveillance processing tools, artificial intelligence resources, etc.¹⁹

Based on their results, the factors of influence – external and internal – that negatively affect the security of the state border are identified. Threats can be identified at one of three levels – low, moderate, and high²⁰. For terrorist threats, other, separate levels are defined – "grey (possible threat)"; "blue (potential threat)"; "yellow (probable threat)"; "red (real threat)"²¹.

An important element of risk analysis is risk profiling, which is a set of methods and techniques for assessing risks²². Risk profiling is one of the most important forms of applying risk analysis in the day-to-day management and control of the state border. It is not practically possible to carry out 100% screening of persons, vehicles and cargoes. Controlling authorities have limited resources, so they need to use them with maximum efficiency. Risk profiling ensures that controls are applied where they are most effective²³.

In the course of risk profiling, depending on the available information about the threat, preventive, potential, and certain risk indicators are identified. In developing risk profiles, in addition to the results of the risk analysis provided by the relevant SBGSU units, proposals from other integrated border management subjects, the International Organization for Migration office in Ukraine are taken into account.

Thus, in accordance with the requirements of the Order of the Administration of the State Border Guard Service of Ukraine "On the Organisation and Application of Risk Profiles" of 26.12.2023, 13 national risk profiles were approved, which in many respects differ from the so-called "traditional" ones

¹⁹ Kushnir I. P., *Sources of information support for the activities of the State Border Guard Service of Ukraine*. Legal novels. 2022. No. 17. p. 21-27.

²⁰ Guidelines for conducting risk analysis in the State Border Guard Service of Ukraine, approved by Order of the Ministry of Internal Affairs of Ukraine No. 1007 on 11 December 2017. URL: <https://zakon.rada.gov.ua/laws/show/z0091-18#Text>.

²¹ Regulation on the Unified State System of Prevention, Response and Suppression of Terrorist Acts and Minimisation of Their Consequences, approved by the Cabinet of Ministers of Ukraine on 18 February 2016, No. 92. URL: <https://zakon.rada.gov.ua/laws/show/92-2016-%D0%BF#n9>.

²² Guidelines for conducting risk analysis in the State Border Guard Service of Ukraine, approved by Order of the Ministry of Internal Affairs of Ukraine No. 1007 on 11 December 2017. URL: <https://zakon.rada.gov.ua/laws/show/z0091-18#Text>.

²³ Bereziuk V., Zabolotna O., Samoilenko O., *Profiling the risk of the introduction and spread of COVID-19 coronavirus infection in Ukraine at state border crossing points*. Collection of scientific papers of the National Academy of the State Border Guard Service of Ukraine. Series: Military and Technical Sciences. 2020. No. 2 (83). p. 41–57.

formed before the start of Russia's full-scale invasion of Ukraine and are aimed at ensuring national and military security.

Approved risk profiles are to be studied and used by the personnel of regional directorates, state border protection bodies and maritime guard units. Access to them is ensured by entering risk profiles into the Risk Profile Form module of the Risk subsystem. The results of the risk profiles are entered into the Gart-5 ITS database.

The risk profiles developed by the SBGSU include the following components: date of development, initiator of the risk profile development, structural unit that developed the risk profile, territorial scope, aggregate information about the threat, risk indicators (indicator name, indicator value), action algorithm (measures and forms of control in case of identification of certain risk indicators, recommendations when identifying a suspicious person, interviewing a suspicious person, in case of hostage-taking).

The report on the results of risk profiling for 2022 states that the risk profiling focused on preventive measures to counter the main threats in the field of border security, took into account the priority classification system of risk indicators, and took into account proposals from other subjects of integrated border management – the Security Service of Ukraine, the National Police, the State Customs Service, and the State Migration Service. Thus, the report states that 31 risk profiles were applied in 2022, including 14 national, 3 regional, and 14 local ones. The results of risk profiling account for 42% of the total results of operational and service activities. In particular, 20 migrants were detained for violating the state border, 1,540 potential migrants were not allowed to cross, 298 weapons, 10,114 pieces of ammunition, 1,088 forged and other people's documents, goods worth about UAH 262 million, 67 kg of drugs, 396 thousand packs of cigarettes, 3,212 litres of alcohol, 82 kg of amber were found. The SBGSU also identified 258 people who could be involved in terrorist activities and anti-state activities in Ukraine, 80 people who violated the procedure for entering/exiting the TOT of Ukraine within the Autonomous Republic of Crimea, Luhansk and Donetsk regions, 141 people possibly involved in the armed aggression of Russia in Ukraine, who were detained by SBGSU personnel while serving at checkpoints²⁴.

Let us review the process of taking into account risk profiles on the example of combating human trafficking. We can distinguish three main areas of combating human trafficking by the SBGSU bodies and units:

- combating trafficking in human beings at border crossing points during border control;
- combating trafficking in human beings beyond the border crossing points by stopping the illegal trafficking of victims of human trafficking across the state border of Ukraine;

²⁴ Risk profiling in the State Border Guard Service of Ukraine: Newsletter for 2022.

- combating trafficking in human beings by operational and search units.

However, risk profiling is carried out only during border control, since the territorial scope of the risk profile "Trafficking in Human Beings from/to Ukraine and Illegal Removal of Children of Ukrainian Citizens" applies only to border crossing points (control points) at the state border. However, it is advisable to consider its application in other areas as well.

The first area. In defining the purpose of border control, the legislator emphasises its law enforcement orientation: border control is carried out in order to counteract the illegal movement of persons across the state border, illegal migration, human trafficking, as well as illegal movement of weapons, narcotic drugs, psychotropic substances and precursors, ammunition, explosives, materials and items prohibited for movement across the state border (part 2 of Art. 2 of the Law of Ukraine "On border control").

Border control is carried out on two levels, which increases the possibility of identifying victims of human trafficking. When carrying out first-line border control, measures are taken to check the minimum necessary to determine whether there are legal grounds for crossing the state border by persons, vehicles and cargoes (clause 8 of Art. 1 of the Law of Ukraine "On border control"). In particular, the inspection of passports or other documents specified by law with the use of technical control measures, during which border guards may detect forged documents or those that do not belong to the bearer. Thus, in 2022, the SBGSU prevented 2,074 attempts to cross the state border with forged documents, 44 – with other people's documents, 3,273 – with invalid documents, 467 people travelling without documents. It should be borne in mind that traffickers often resort to the production or acquisition of forged documents in order to ensure the trafficking of victims across the state border. When checking documents, border guards determine the presence or absence of information in the databases on law enforcement orders regarding persons crossing the state border.

In addition, an effective means of identifying victims of human trafficking is to interview people during border control. The following may indicate the presence of a potential human trafficking risk indicator: 1) the person cannot provide details of the travel route; 2) the person does not know where and when they received a foreign passport of a citizen of Ukraine; 3) the person does not know the name of the company that issued the travel documents; 4) the person does not know the meeting party, the address or name of the employer, the place of future residence and the duration of stay; 5) the person returning to Ukraine reports that they have been a victim of human trafficking. Other risk indicators are also taken into account: purpose of the trip, availability and condition of documents, signs of their forgery, appearance of the person, contents of the luggage, route, behaviour, availability of sufficient financial support for the trip.

In the event of certain doubts about the legality of crossing the state border by a foreigner or stateless person, including to determine the possibility that the person is a victim of human trafficking, second-line control is carried out.

It should also be noted that the Council of Europe Convention on Action against Trafficking in Human Beings²⁵ regulates the strengthening of border control measures that may be necessary to prevent and detect trafficking in human beings. In particular: taking measures to prevent traffickers from using vehicles operated by commercial carriers; introducing an obligation for commercial carriers to ensure that all passengers have the necessary travel documents (under threat of sanctions); denying entry or cancelling visas to persons involved in trafficking in human beings; strengthening cooperation between border services (Art. 7 of the Convention).

The second area is to combat trafficking in human beings beyond the border crossing points by stopping the illegal trafficking of victims of human trafficking across the state border of Ukraine. Such activities are ensured by conducting patrol, search, control and security measures by border details patrolling the state border. Moreover, in this area, measures to combat human trafficking should be considered in the context of comprehensive activities to combat illegal migration. As noted by Yu. B. Kuryliuk, illegal migration is considered a "background phenomenon for crime", as it is usually associated with various types of illegal activities, including human trafficking, smuggling, poaching, and increasingly migrants are influenced by extremist and terrorist organisations²⁶.

The third important area is combating trafficking in human beings by operational and search units. Operational and search activities to combat trafficking in human beings are mainly searching in nature, carried out by special covert methods and means and aimed at timely detection of criminal offences and perpetrators, victims of trafficking in human beings, establishment of factual data important for further investigation, as well as circumstances that contributed to the commission of criminal offences.

The effectiveness of combating trafficking in human beings by the SBGSU bodies and units is based on a comprehensive approach to combating offences, which is carried out with due regard to risk profiling and the organisation of proper information interaction with other law enforcement agencies in these areas²⁷. Therefore, we believe that familiarisation with the risk profile of human trafficking and other risk profiles, their study and consideration in view of the content of risk profiles should be carried out not only by officials serving at border crossing points, but also by officials of other bodies and units involved

²⁵ Council of Europe Convention on Action against Trafficking in Human Beings (2005). https://zakon.rada.gov.ua/laws/show/994_858.

²⁶ Kuryliuk Yu. B., *Administrative, Legal and Criminological Principles of Ensuring Law and Order in the Border Area of Ukraine*: Thesis of S.J.D: 12.00.07, 12.00.08. National Academy of Management; Classic Private University. Kyiv-Zaporizhzhia. 2020, p. 142.

²⁷ Stepanova Yu. P., *Combating trafficking in human beings by bodies and units of the State Border Guard Service of Ukraine*, in H. Ya. Savchyn, U. O. Tsmots (eds.) *State policy on combating human trafficking: Ukraine and the world: Collection of abstracts of the International Scientific and Practical Conference (8 October 2021)*, Lviv State University of Internal Affairs, Lviv, 2021. p. 180–183.

in operational activities, in particular, operational and search units.

In turn, employees of operational and search units actively use operational criminal analysis in their work, the pioneer of which was the SBGS of Ukraine²⁸. Criminal analysis is a specific type of information and analytical activity, which consists in identifying and determining as accurately as possible the internal links between information relating to a criminal offence and any other data obtained from various sources, their use in the interests of conducting operational and search activities, their analytical support^{29,30}.

The use of criminal analysis in Ukraine has been launched in the SBGSU since 2006. Its implementation was actively supported by the US Department of State, IOM and the Polish Border Guard, with financial and technical assistance from the OSCE and EUBAM. In particular, the State Border Guard Service was provided with the IBM i2 Analyst's Notebook software free of charge³¹, which allows processing large amounts of information related to telephone contacts and other resources accumulated in databases. In addition, domestic software and hardware systems "Gart" (Gart-1, Gart-1/P, Gart-1/KDL, Gart-2, Gart-3, Gart-3/P, Gart-2/O, Gart-19, Gart-12, ARM "Violator", ARM "Surface Situation", ARM "e-Inspector"), databases of other law enforcement agencies, mobile operators, banking institutions, and other state and non-state structures are actively used by border guard units.

The methodology of criminal analysis is used in the following sequence: an operative collects data, submits it to the criminal analysis unit to verify the information and obtain new data. Criminal analysis can be carried out both after the fact and proactively. Based on the results of the data processing, the criminal analyst provides the operative with information on the most optimal further steps³².

An important component of the implementation of criminal analysis is the training of specialists, which was initially carried out at the Academy of the Polish Border Guard. Later, border guards began to share their experience in criminal analysis with the National Police³³.

5. Information support for combating criminal offences based on

²⁸ Fedchak I. A., *Fundamentals of criminal analysis: Study Guide*. Lviv: Lviv State University of Internal Affairs, 2021. p. 121.

²⁹ Vlasiuk O. V., *The role and place of criminal analysis in the detection and investigation of crimes at the state border of Ukraine*. Materials of the permanent scientific and practical seminar. Kharkiv: Institute of Legal Training for the Security Service of Ukraine of the Yaroslav Mudryi National Law Academy of Ukraine, 2011. Issue 3. Part 1, p. 83.

³⁰ Kushnir I., Tsarenko O., Tsarenko S., *Legal and organizational problems on identification of persons in activities of the State Border Guard Service of Ukraine*, Juridical Tribune - Tribuna Juridica, Volume 11, Issue 1, March 2021. p. 113–130.

³¹ Filippov S. O., *Criminological Principles of Counteracting Transborder Crime*: Doctoral dissertation: Specialty 12.00.08. SBGSNA, DSUIA. Khmelnytskyi, 2019, p. 407.

³² In the footsteps of the "tarantula" / Border Guard of Ukraine. No. 41. 04 November 2016. [https://dpsu.gov.ua/upload/file/pu_41_2016_\(2\).pdf](https://dpsu.gov.ua/upload/file/pu_41_2016_(2).pdf).

³³ Ibid.

open data

Other individual information support measures include Open Source Intelligence (OSINT), the Automated Pre-Travel Information Processing System (API/PNR), checks against the International Criminal Police Organisation database.

So, OSINT is called open source intelligence. This is a method of collecting operational and operationally relevant information from sources of information that are publicly available and open. Such sources provide data in the format of text, video, images, audio recordings, and OSINT provides accelerated analysis of that information³⁴. The main sources of online OSINT include websites; social networks (Facebook, Instagram, TikTok, LinkedIn, Twitter, Telegram, etc.); personal credentials (first name, last name, nickname, email address, phone number, etc.); maps, documents, photos/videos, IP addresses, business and state registers, virtual currency transactions, Internet archives³⁵. It results in specific information, collected and structured in a particular way, and for a specific purpose, to answer a specific question or to achieve a specific goal. When using the OSINT methodology by law enforcement agencies to obtain operationally relevant information, it is necessary to take into account the need to process significant amounts of data from reliable sources of information and the high cost of software^{36,37}.

Analysing the practice of using open sources of information in the field of state security, Bykov I. O. notes the active development of projects that use the OSINT methodology in the investigation of crimes of military aggression³⁸. For example, the Truth Hounds organisation successfully uses this methodology in combination with eyewitness and victim testimonies to document crimes of military aggression and search for war criminals³⁹. Its employees have created a database that accumulates information from the media, allows it to be analysed and used promptly. Thus, during 2023, the organisation's monitors entered 13,273 episodes into the database – the information about incidents with signs of war crimes. They created 32,119 new entries in the I-DOC database (a system

³⁴ What is Open-Source Intelligence (OSINT)? / Opendtext. URL: <https://www.opentext.com/what-is/open-source-intelligence-osint>.

³⁵ Halustian O.A., *Profiling and OSINT: modern technologies for detecting collaborators and collaboration activities in wartime*. Topical issues of using OSINT methods and means in the work of national statehood defence units: Roundtable Proceedings (Kyiv, 31 March 2023): in 2 parts. Part 1. Kyiv: SSU NA, 2023, p. 24-25.

³⁶ Bykov I. O., *Open Data and OSINT in the investigation of war crimes. Current issues of criminal proceedings in modern conditions*: Proceedings of the international scientific-practical conference. Odesa, 31 May 2023. Odesa: OSUIA, 2023, p. 132.

³⁷ Bykov I., *The use of open sources of information (OSINT) in the sphere of state security: technologies and prospects* / YouTube / Helvetika Publishing Group. <https://www.youtube.com/watch?v=c23liBuStsE>.

³⁸ Bykov I. O., *op. cit. (Open Data and OSINT...)*, p. 38-41.

³⁹ About us / Truth Hounds URL: <https://truth-hounds.org/en/about/>.

for analysing and systematising investigations of war crimes and crimes against humanity), including information on 667 incidents with signs of war crimes, 1,521 witnesses to war crimes, 1,736 attacks on internationally protected objects, 2,067 identified victims, and carried out 5 independent investigations⁴⁰. Using OSINT intelligence, employees of the organisation identified all units of the armed forces of the Russian Federation that occupied the Sumy region in February-April 2022⁴¹, identified a significant part of the personnel of the 26th Missile Brigade of the 6th Combined Arms Army of the Russian Federation, together with its command, who most likely gave the order to attack Chernihiv on 19 August 2023, when 214 people were injured in the explosion, seven of whom died⁴².

An important part of building an effective OSINT strategy is finding the right tools. The most common free tools today are Maltego, Harvester, Meta-goofil, SpiderFoot, Framework, DarkOwlVision, PhoneInfoga. At the same time, when conducting research, a criminal analyst should take care of information security so as not to disclose information about the user and not to jeopardise the operation being conducted⁴³.

Law enforcement agencies of foreign countries have created special units that carry out intelligence on the basis of open sources of information. For example, the Royal Canadian Mounted Police OSINT, Scotland Yard OSINT, the OSINT unit of the New York Police Department, Israel's Hatsaf, the British BBC Monitoring, the Australian Office of National Assessments,⁴⁴ etc. The research structures of the OSINT community in Ukraine are the NGOs "Institute of Post-Information Society", "Molfar", "YouControl", "Kiber Polk". A characteristic feature of the Russian-Ukrainian war is the cyber front, the establishment and subsequent mobilisation of the cyber volunteer movement.

Currently, the Office of the Prosecutor General, the Security Service of Ukraine, and the Ministry of Internal Affairs are actively implementing the OSINT methodology. For example, as a pilot project, in June 2023, the Odesa State University of Internal Affairs introduced a training course on searching and analysing information from open sources OSINT, organised by the university's research laboratory for problematic issues of criminal analysis⁴⁵. The use of

⁴⁰ Annual report of 2023 / TruthHounds. https://truth-hounds.org/wp-content/uploads/2024/01/ric_hnyj-zvit-2023.pdf.

⁴¹ The units of the Russian armed forces that occupied the Sumy region / OSINT-intelligence / TruthHounds, https://truth-hounds.org/cases/pidrozdily-zs-rf-shho-okupovuvally-sumsh_hynu/.

⁴² Actors in the attack on the Chernihiv theatre / OSINT-intelligence / TruthHounds. URL: <https://truth-hounds.org/cases/dijovi-osoby-ataky-na-chernigivskiy-dramteatr/>.

⁴³ Kireieva O. S., *Using OSINT methods in the work of criminal analysts*. Topical issues of using OSINT methods and means in the work of national statehood defence units: Roundtable proceedings (Kyiv, 31 March 2023): in 2 parts. Part 1. Kyiv: SSU NA, 2023. 75 p.

⁴⁴ Klimushyn P. S., Bilobrov A. V., *Using OSINT technologies to obtain information*. Combating crime and human trafficking. 2020. p. 135–137. URL: https://www.univd.edu.ua/general/publicshing/konf/27_05_2020/pdf/39.pdf.

⁴⁵ Welcome to the course on search and analysis of information from open sources (OSINT - Open source intelligence) / Odesa State University of Internal Affairs. Official website. URL:

OSINT analysis methodology in the activities of specialised SBGSU bodies and units that counter criminal offences, as well as for searching for SBGSU personnel who are missing or in captivity, and exposing enemy agents, is highly prospective. At the same time, military personnel need training in information hygiene and cyber hygiene⁴⁶.

One of the types of information technologies for collecting and analysing information from open sources is another area of intelligence - HUMINT (human intelligence), literally "intelligence on people". These technologies include social media monitoring, surveys, social engineering, legendary conversations, etc⁴⁷. Profiling is also identified as a promising tool for identifying collaborators⁴⁸. Profiling is a law enforcement tactic in which a certain set of characteristics (profiles) is used to find and detain a person who has committed a crime (criminal profiling) or to identify people who are likely to be involved in criminal activity (behavioural profiling)⁴⁹.

The considered methods of information and analytical support for combating criminal offences are mainly aimed at detecting offences and detaining the individuals who committed them. However, the emergence of new technologies, such as artificial intelligence (AI) applications, has opened up a new era of possibilities to help law enforcement agencies prevent crime.

New technologies enable overworked and understaffed law enforcement agencies to collect, process, analyse and present relevant data for subjects combating any types of criminal offences. In particular, AI is used to collect and interpret links and patterns in financial records, geospatial images, surveillance camera footage, social media data, public records, news feeds, and many other open and closed sources.

One of the most useful applications of AI in the fight against crime is in resource allocation. As virtually all law enforcement agencies are under-staffed and underfunded, the proper allocation and deployment of resources plays an important role in combating crime. Sophisticated algorithms are effective in helping to understand who, when, where, how and why a criminal offence may be committed within the jurisdiction of certain law enforcement agencies⁵⁰, including the most likely ways and means of violating the state border. AI can identify relevant crime prevention models and ways to implement them, in particular by

<http://surl.li/izigs>.

⁴⁶ Marenych O. V., *Processing of primary data, search for information in the WEB environment*. Topical issues of using OSINT methods and means in the work of national statehood defence units: Roundtable Proceedings (Kyiv, 31 March 2023): in 2 parts. Part 1. Kyiv: SSU NA, 2023. p. 39–41.

⁴⁷ Klimushyn P.S., Bilobrov A.V., *op. cit. (Using OSINT technologie...)*, p. 135–137.

⁴⁸ Halustian O.A., *op. cit. (Profiling and OSINT...)*, p. 25.

⁴⁹ Halustian A. O., Zakharenko L.M., Motliakh O.I., *Profiling technologies in investigative activities*. Kyiv: 2019. 45 p.

⁵⁰ Leveraging Artificial Intelligence for Crime Prevention. March 2022 URL: <http://surl.li/qmjam>

adjusting the allocation of resources, such as scheduling border patrols, determining the optimal time and routes of their movement, the procedure for reconnaissance and search groups, the use of mobile units to strengthen border protection, the location of engineering facilities, technological equipment of border units, etc., while taking into account seasonal, geographical or demographic trends, or fluctuations in passenger flows or alterations in illegal activities due to certain socio-economic changes.

6. Use of artificial intelligence

Another area of information support is artificial intelligence (AI). Global trends show a marked increase in the use of video surveillance combined with AI. Owing to advances in the field of analytics, this has led to the expansion of remote and preventive video surveillance systems⁵¹. Chinese scientists have already developed a system for facial recognition, recognising people by their gait. The United States uses the ShotSpotter system, which is capable of detecting the type of firearm, the coordinates of the scene of the incident using sound sensors⁵². The face recognition technology (FRT) developed by the Israeli company Cortica provides ethical and accurate biometric detection and is aimed at finding behavioural anomalies in human movements that indicate that a person is about to commit a crime. One Mind Hypervisor SVI combines licence plate recognition, vehicle registration and facial recognition solutions to support police departments in combating car theft⁵³.

In view of this and taking into account the peculiarities of the SBGSU operational activities both at and outside border crossing points, it is worth recognising the promising use of AI capabilities in combination with video surveillance systems to counter criminal offences.

The prospective areas of information support for combating criminal offences by the SBGSU are the use of AI for the purpose of: optimisation of resource allocation; development of relevant models for combating crime in the SBGSU; verification of the effectiveness of crime prevention measures; use of AI systems in combination with video surveillance systems.

At the same time, possible risks associated with the use of AI should be taken into account. The introduction of such technologies as the iBorderCtrl ar-

⁵¹ Kurt Takahashi, *What factors had the biggest impact on security in 2023?* URL: <http://surl.li/qlzcc>.

⁵² Mordvyntsev M. V., Khlietkov O. V., Nytsiuk S. P., *Trends in the global development of video surveillance systems for public security*. Counteraction to cybercrime and human trafficking: Proceedings of the international scientific and practical conference. (Kharkiv, 18 May 2021) / Ministry of Internal Affairs of Ukraine, Kharkiv National University of Internal Affairs; NGO "Global Centre for Interaction in Cyberspace". Kharkiv, 2021. p. 71–72.

⁵³ Corsight AI partners with One Mind Technologies to enhance security in smart cities. URL: <http://surl.li/qlzdw>.

tificial intelligence system or ARI/PNR in the interests of border security, Filipov S.O. notes, creates certain problems due to the gap between the introduction of innovations and their normative regulation⁵⁴.

Legal regulation of the use of AI should be carried out at the international level, given the global scale of its use and the corresponding threats. It is currently under development. Thus, on 26 January 2023, the US National Institute of Standards and Technology published its AI risk management framework⁵⁵. After that, a number of important documents were adopted – the US Presidential Decree of 30 October 2023 on safe, reliable, and trustworthy AI⁵⁶, and the Bletchley Declaration on AI Security was signed by 28 states and the EU on 31 October 2023⁵⁷.

Thus, the introduction of AI opens up significant opportunities for combating criminal offences by the SBGSU, but its use is possible only with the application of the necessary security measures, proper legal regulation and human coordination – primarily to avoid the risks of unplanned control by AI over the processes regulated by the SBGSU, human rights, and information security.

However, AI's conclusions should be advisory in nature. The subjective assessment of a law enforcement officer should be decisive. Especially when a criminal offence involves a victim (in particular, trafficking in human beings) or a migrant is involved in the mechanism of its commission.

7. Conclusions

So, when studying information support as a component of criminological support for combating criminal offences by the State Border Guard Service of Ukraine, we have come to the following conclusions:

It is determined that the purpose of information support for combating criminal offences of the SBGSU is to form an information system which, on the one hand, would ensure information security of the SBGSU, and on the other hand, would cover the information process of collecting, accumulating, storing, transmitting information required by the SBGSU to combat crime, and would

⁵⁴ Filipov S. O., *Certain aspects of the use of passenger data (ARI/PNR) in the interests of border security*. Rule of law. 2021. No. 43. p. 169–176. <http://pd.onu.edu.ua/article/view/240997/241027>.

⁵⁵ AI Risk Management Framework / Information Technology Laboratory / NIST. URL: <https://www.nist.gov/itl/ai-risk-management-framework>.

⁵⁶ Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence / The White House. URL: <https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/>.

⁵⁷ The Bletchley Declaration by Countries Attending the AI Safety Summit, 1-2 November 2023 / GOV.UK. URL: <https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration/the-bletchley-declaration-by-countries-attending-the-ai-safety-summit-1-2-november-2023>.

ensure information interaction with other law enforcement agencies, in particular, the subjects of integrated border management in the field of combating crime.

The expediency of introducing criminological monitoring of combating criminal offences in the SBGSU as a certain system capable of combining the main methods of information support for combating criminal offences is substantiated: statistical observation, analysis of criminal proceedings, analysis of reports, analytical information, surveys of members of the public, victimisation monitoring of individuals, content monitoring of Internet resources, method of expert assessments.

It is established that today the components of criminological monitoring in the SBGSU include risk analysis, risk profiling and criminal analysis (which are implemented systematically on an ongoing basis), as well as other separate information support measures are carried out at the departmental, national and international levels: Open Source Intelligence (OSINT), the Automated Pre-Travel Information Processing System (API/PNR), checks against the International Criminal Police Organisation database, use of artificial intelligence.

It is proposed to consider the use of artificial intelligence as a promising area of information support for combating criminal offences by the SBGSU in the following areas: 1) optimisation of resource allocation; 2) formation of relevant models of combating criminal activity in the SBGSU; 3) verification of the effectiveness of measures to combat criminal activity; 4) use of artificial intelligence systems in combination with video surveillance systems.

Bibliography

1. Bereziuk V., Zabolotna O. and Samoilenko O., *Profiling the risk of the introduction and spread of COVID-19 coronavirus infection in Ukraine at state border crossing points*. Collection of scientific papers of the National Academy of the State Border Guard Service of Ukraine. Series: Military and Technical Sciences. 2020. No. 2 (83). p. 41–57.
2. Beschastyi, V. M. *Methods of information support as tools for collecting and processing information on crime*. Law and Society. 2017. No. 1. p. 206–212.
3. Blazhkovskiy, Ye. *Monitoring the fight against crime in Ukraine*: monograph. Kharkiv: Zolota mylia, 2013. 372 p.
4. Bykov, I. O., *Open Data and OSINT in the investigation of war crimes. Current issues of criminal proceedings in modern conditions*: Proceedings of the international scientific-practical conference. Odesa, 31 May 2023. Odesa: OSUIA, 2023. 286 p.
5. Bykov, I., *The use of open sources of information (OSINT) in the sphere of state security: technologies and prospects* / YouTube / Helvetika Publishing Group. <https://www.youtube.com/watch?v=c23liBuStsE>.
6. Fedchak, I. A., *Fundamentals of criminal analysis: Study Guide*. Lviv: Lviv State University of Internal Affairs, 2021. 288 p.
7. Filippov, S. O., *Certain aspects of the use of passenger data (ARI/PNR) in the interests of border security*. Rule of law. 2021. No. 43. p. 169–176. <http://pd>.

- onu.edu.ua/article/view/240997/241027.
8. Filippov, S. O., *Criminological Principles of Counteracting Transborder Crime*: Doctoral dissertation: Specialty 12.00.08. SBGSNA, DSUIA. Khmelnytskyi, 2019. 561 p.
 9. Gubanova, E. V., *Criminality as Negative Aspect of Globalization*. Scientific Notes of Tavrida National V. I. Vernadsky University. Series: Juridical sciences. 2013. Vol. 26 (65). No. 1. p. 177–179.
 10. Halustian, A. O., Zakharenko, L.M. and Motliakh, O.I., *Profiling technologies in investigative activities*. Kyiv: 2019. 45 p.
 11. Halustian, O. A., *Profiling and OSINT: modern technologies for detecting collaborators and collaboration activities in wartime*. Topical issues of using OSINT methods and means in the work of national statehood defence units: Roundtable Proceedings (Kyiv, 31 March 2023): in 2 parts. Part 1. Kyiv: SSU NA, 2023. p. 23–27.
 12. Kireieva, O. S., *Using OSINT methods in the work of criminal analysts*. Topical issues of using OSINT methods and means in the work of national statehood defence units: Roundtable proceedings (Kyiv, 31 March 2023): in 2 parts. Part 1. Kyiv: SSU NA, 2023. 75 p.
 13. Klimushyn, P. S. and Bilobrov, A. V., *Using OSINT technologies to obtain information*. Combating crime and human trafficking. 2020. p. 135–137. URL: https://www.univd.edu.ua/general/publ shing/konf/27_05_2020/pdf/39.pdf.
 14. Kuryliuk, Yu. B., *Administrative, Legal and Criminological Principles of Ensuring Law and Order in the Border Area of Ukraine*: Thesis of S.J.D: 12.00.07, 12.00.08. National Academy of Management; Classic Private University. Kyiv-Zaporizhzhia. 2020. 472 p.
 15. Kushnir, I. P., Kuryliuk, Yu. B. and Filippov S. O., *Information support of border control at airport border crossing points on the state border of Ukraine*. Air and space law. 2021. Vol. 4. No. 61. p. 17–23.
 16. Kushnir, I. P., *Sources of information support for the activities of the State Border Guard Service of Ukraine*. Legal novels. 2022. No. 17. p. 21–27.
 17. Kushnir, I., Tsarenko, O. and Tsarenko, S., *Legal and organizational problems on identification of persons in activities of the State Border Guard Service of Ukraine*, Juridical Tribune - Tribuna Juridica, Volume 11, Issue 1, March 2021. p. 113–130.
 18. Lytvynov, O., *Criminological monitoring*, Bulletin of the Criminological Association of Ukraine. 17 March 2018. URL: <https://visnikkau.webnode.com.ua/news/kriminologichni-monit ring/>.
 19. Marenych, O. V., *Processing of primary data, search for information in the WEB environment*. Topical issues of using OSINT methods and means in the work of national statehood defence units: Roundtable Proceedings (Kyiv, 31 March 2023): in 2 parts. Part 1. Kyiv: SSU NA, 2023. p. 39–41.
 20. Mordvyntsev, M. V., Khliestkov, O. V. and Nytsiuk, S. P., *Trends in the global development of video surveillance systems for public security*. Counteraction to cybercrime and human trafficking: Proceedings of the international scientific and practical conference. (Kharkiv, 18 May 2021) / Ministry of Internal Affairs of Ukraine, Kharkiv National University of Internal Affairs; NGO "Global Centre for Interaction in Cyberspace". Kharkiv, 2021. p. 71–72.

21. Orlov, Yu. V. and Myroniuk D. M., *Criminological monitoring of the legal regulation effectiveness as a tool for combating crime*. Bulletin of the Criminological Association of Ukraine. 2014. No. 6. p. 161–177.
22. Shoptenko, S. S. *Administrative and jurisdictional activities of law enforcement agencies of Ukraine*: S.J.D thesis abstract: 12.00.07. Kharkiv. 2018. 43 p.
23. Stepanova, Yu. P., *Combating trafficking in human beings by bodies and units of the State Border Guard Service of Ukraine*, in Savchyn, H. Ya. and U. O. Tsmots (eds.) *State policy on combating human trafficking: Ukraine and the world: Collection of abstracts of the International Scientific and Practical Conference (8 October 2021)*, Lviv State University of Internal Affairs, Lviv, 2021. p. 180–183.
24. Stokorosa, T. M., *Informatisation and information support: approaches to the interpretation of concepts*. Scientific Bulletin of NFU of Ukraine. 2008. Issue 18.9. p. 196–301.
25. Takahashi, Kurt, *What factors had the biggest impact on security in 2023?* URL: <http://surl.li/qlzcc>.
26. Vikhtiuk, A. V., *Legal and regulatory framework for information cooperation in integrated border management. Priority areas of science development during martial law*, XCII International Scientific and Practical Internet Conference. City of Odesa, 24 June 2022. p. 76–78.
27. Vlasiuk, O. V., *The role and place of criminal analysis in the detection and investigation of crimes at the state border of Ukraine*. Materials of the permanent scientific and practical seminar. Kharkiv: Institute of Legal Training for the Security Service of Ukraine of the Yaroslav Mudryi National Law Academy of Ukraine, 2011. Issue 3. Part 1. p. 82–85.