Nina Gumzej (ed.)
Olga Sovova (ed.)

Recent Debates in Cyberspace and Artificial Intelligence Law

ADJURIS
International Academic Publisher

Recent Debates in Cyberspace and Artificial Intelligence Law

Editors:

Nina Gumzej

Activity

Nina Gumzej, PhD, is Associate Professor at the University of Zagreb, Faculty of Law at the Chair of Information Technology Law and Informatics. She earned her LL.M. degree (Distinction) in International Business Law at the Central European University in Budapest and the Ph.D. degree in 2011 at the University of Zagreb Faculty of Law. Dr. Gumzej teaches several courses at the University of Zagreb Law Faculty incl. *Information Technology Law*, *Privacy and Electronic Communications*, *Electronic Media Law*, *Internet Governance and Regulation*, *Introduction to Information Security*, *Cybersecurity and Cybercrime* and at the University of Zagreb Faculty of Electrical Engineering and Computing (*„Information Law"*). As a selected representative from the academia, she participated in the Young Leaders Program supported by the European Institute of Innovation and Technology Foundation and the European Commission, academically steered by the Imperial College London. Dr. Gumzej is: editorial board member for international journals *Juridical Tribune – Tribuna Juridica*, *Perspectives of Law and Public Administration*; scientific committee member of the international conferences (*Fintech, Cyberspace and Artificial Intelligence Law*; *Perspectives of Business Law in the Third Millennium*); organizing and program committee member of the international conference *SoftCOM* (*Symposium on Information Security and Intellectual Property - ISIP*) and program committee member of the international conference *MIPRO* (*Information and Communication Technology Law - ICTLAW*). Dr. Gumzej was a national legal expert for several European Commission studies and programs (Formobile – from mobile phones to court – A complete FORensic investigation chain targeting MOBILE devices (Horizon 2020); Study supporting the evaluation of Regulation (EU) 2018/1807 on a framework for the free flow of non-personal data in the European Union - SMART 2019/0024; Study on the implementation of the provisions of the AVMS Directive for the promotion of European works in audiovisual media services - SMART 2019/0037; Cross-border data flow in the digital single market: study on data location restrictions - SMART 2015/0054; Anti-Doping & Data Protection - An evaluation of the anti-doping laws and practices in the EU Member States in light of the General Data Protection Regulation; ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation - SMART 2013/0071; Standard terms and performance criteria in service level agreements for cloud computing services - SMART 2013/0039. She is expert evaluator of projects under EU programs and a reviewer of scientific papers for various journals and international conferences (*IEEE Access*, *Croatian Yearbook of European Law and Policy*, *SoftCOM*, *MIPRO*, etc). Dr. Gumzej is associate member of the Croatian Academy of Legal Sciences.

Publications

Nina Gumzej regularly publishes scientific papers in scientific journals (*Juridical Tribune - Tribuna Juridica, Croatian Yearbook of European Law and Policy, Collected Papers of Zagreb Law Faculty, Media, culture and public relations*, etc) and presents scientific papers at international conferences in the area of information and communications technology law. She is an author of several chapters in the monograph *International Encyclopaedia of Laws: Cyber Law* (Kluwer Law International, Alphen aan den Rijn, 2020) on the regulation of the Croatian ICT incl. telecommunication markets, telecommunications privacy and general personal data protection, and co-author of the textbook „*Pravna informatika i pravo informacijskih tehnologija*" („*Legal Informatics and Information Technologies Law"*), Narodne novine, Zagreb, 2016.

Olga Sovova

Activity

JUDr. Olga Sovova, PhD., is an Associate Professor at the Department of Administrative Law and Administrative Science at the Police Academy of the Czech Republic in Prague. She specializes in administrative procedure, privacy protection, the responsibility of regulated professions and Artificial Intelligence in public administration and finance. She co-founded the Medical Law Center at the Law Faculty, Charles University, Prague. The Center has transformed into the Department of Medical Law, where she is a visiting associate professor. She is a member of the Czech Bar Association. As an attorney-at-law, she advises in medical, civil, family, administrative and tax law. She is a member of the Union of Family Attorneys. She is an editorial board member and regularly contributes to the monthly *Rodinné list (Family papers, Wolters Kluwer)*.

Publications

Restrictive Medical and Social Care Measures according to the Czech Legal Regulation. In *Book of Abstracts of the 18th World Congress on Medical Law, 2009.*

Legal Intervention Issues regarding Human Integrity and the Injured Patient's Rights. In Karczmarek, T., Filipowska-TuthilL, M., Żylińska, J. (red). *Ochrona prawna pokrzywdzonego*. Wrocław, 2017. *Challenges of Public Administration in the Global Digital Era*. In Cazala, J., Zivkovic, V. (ed.): *Administrative Law and Public Administration in the Global Social System*. Contributions to the 3rd International Conference Contemporary Challenges in Administrative Law from an Interdisciplinary Perspective October 9, 2020, Bucharest. ADJURIS – International Academic Publisher. Bucharest, Paris 2021 (co-author Fiala, Z.). *Public Administration between Control and Support*. NORDSCI Conference Proceedings 2021, Book 2. Other papers at the NORDSCI Org. Library. Active participation and papers at SGEM Conferences of Social Sciences, Hradec Days of Social Work – international conference, EU financed conference of Restorative Justice, Mediation and Protection of EU Financial Interests. Articles at *Juridical Tribune, Perspectives of Business Law, Medlaw journal of the Czech Academy of Sciences, Acta Iuridica Medicinae-Slovak Republic, Common Law Review – Law Faculty, Charles University, Heinoline*.

Prizes

Award for the best paper DIGITAL JUSTICE – A STEP TOWARDS DIGITAL SINGLE MARKET in the Law section, NORDSCI 2022 International Conference on Social Sciences

Nina Gumzej (ed.)
Olga Sovova (ed.)

Recent Debates in Cyberspace and Artificial Intelligence Law

Contributions to the 3rd International Conference on FinTech, Cyberspace and Artificial Intelligence Law
March 31, 2023, Bucharest

ADJURIS
International Academic Publisher

Bucharest, Paris, Calgary 2023

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 (Thomson Reuters)**.

ISBN 978-606-95351-7-2 (E-Book)

Editing format .pdf Acrobat Reader
Bucharest, Paris, Calgary 2023

www.adjuris.ro
office@adjuris.ro

Preface

Editors
Associate professor ***Nina Gumzej,***
University of Zagreb, Republic of Croatia
Associate professor ***Olga Sovova****,*
Police Academy of the Czech Republic in Prague

This volume contains the scientific papers presented at the 3rd International Conference on FinTech, Cyberspace and Artificial Intelligence Law that was held on March 31, 2023, Bucharest, online on Zoom. The conference is organized by the *Society of Juridical and Administrative Sciences*. 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:

- *Alchemy of cyberspace in the fire of regulation.* The papers in this chapter refer to: a few comments on FinTech in the light of cyber security; freedom of expression in cyberspace: the good and the bad; cyber space and security in the cyber environment - general considerations; profiling criminals in cyberspace; current standards for information security and privacy.
- *Artificial intelligence through the lens of today's law.* This chapter includes papers on: new technologies are shaping arbitral proceedings; implications of ChatGPT technology on criminal law; the robot as a natural or legal person - another perspective on the concept of person; adapting non-contractual liability rules to artificial intelligence; artificial intelligence and the legal responsibilities in public financial administration.
- *Legal interface of the current standards in digitalization*. The papers in this chapter refer to: brief considerations regarding work on digital platforms; digital Euro currency, economic and legal implications; the complexity of the legislative framework and the difficulties of correlation with economic and social impact in public administration - the digitalization of public services; blockchain technology and smart contracts - public policy needed in the technology race.

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

ALCHEMY OF CYBERSPACE IN THE FIRE OF REGULATION

A Few Comments on FinTech in the Light of Cyber Security

JUDr. **Tereza JONÁKOVÁ**[1]

Abstract

The following paper examines the current opportunities for ensuring the security of cyberspace and financial technologies in relation to the institutional and legislative environment from the perspective of the European Union. The rapid growth in the field of financial technologies brings with it not only pros and benefits, but also cons and security threats, both on an individual and on a complex systemic level. The use of financial technology tools themselves thus poses not only the necessary co-responsibility of the target entities when using them, but also comprehensive reflections on, institutional security and national and supranational legal regulation of the so-called digital economy.

Keyword: *FinTech, segments of FinTech, cyber security, legislative background of FinTech, institutional background of FinTech.*

JEL Classification**:** K24, K33

1. Introduction

The institutionalisation of financial technologies (hereinafter referred to as "FINTECH") has become a natural matter of course in the society of the 21st century and people have become accustomed to the comfort offered by the innovations in the field of financial services. However, the expansion of services, products and companies in the field of financial technologies has brought not only advantages and positives, but also disadvantages and security risks[2] associated with them, at both individual and comprehensively systemic levels. Financial technologies are present on a daily basis, for example, when making money transfers, providing loans, managing insurance, investing, crowdfunding, mining cryptocurrencies, etc. The use of the financial technology instruments in themselves thus involves the necessary co-responsibility of the target entities in their use as well as comprehensive considerations on financial stability and the national and transnational legal regulation of the so-called digital economy.[3] The basic goal of the vision of the development of individual FINTECH areas is the development of an ideal technical solution for the individual target customer and

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

[2] For more detail, see Vilnius, IMF Deputy Managing Director Tao Zhang and Lithuania, not dated. Balancing FinTech Opportunities and Risks. IMF [online] [accessed on 2023-01-11]. Available from: https://www.imf.org/en/News/Articles/2019/06/10/sp061019-balancing-FinTech-opportunitiesand-risks

[3] For more detail, see BIS, 2019. Innovation and FinTech [online]. [accessed on 2023-02-08]. Available from: https://www.bis.org/topic/FinTech.htm.

streamlining and automation of processes with financial availability resulting from the competitive fight for them.

2. Historical excursion

In the historical context, the first financial technology can be interpreted in connection with the development of finance and written records about it, with historical data from approximately 2500 BC, related to financial transactions of a tax type.[4] However, the beginning of modern financial technologies with information subtext is known only from the 19th century and is associated with the year 1837, when telegraph was patented by Samuel Morse followed by telephone invented by Alexander Graham Bell in 1876. Thanks to the above-mentioned, completely revolutionary, inventions at that time, the boundaries of communication and limited trade were broken.[5] Later, communication technologies were improved in the 1960s in the form of the Telex communication network, operating via a network of interconnected telex machines, followed by further improvement in the form of a fax machine, with Xerox introducing their new Magnafax Telecopier, which could be connected to a regular telephone line, in 1966.[6] For the sector of financial technology, the world wars meant development of computer technology, mainly because of the need to decrypt German war radio messages.[7] The 1970s gave rise to a real basis for digitisation and equipment for contemporary financial technologies.[8] The 1980s are associated primarily with online electronic banking, the emergence of the world's first electronic online exchanges, and a breakthrough in combining financial markets and information technology.[9] In the early 1990s, the term FINTECH

[4] For more detail, see Garbutt, Douglas, 1984. *The significance of ancient mesopotamia in accounting history*. The Accounting Historians Journal. 11(1), 83–101. ISSN 0148-4184.

[5] For more detail, see Federal Reserve Bank of New York, 2015. Fedwire and National Settlement Services [online] [accessed on 2023-03-03]. Available from: https://www.newyorkfed.org/about thefed/fedpoint/fed43.html.

[6] For more detail, see Costigan, Daniel M., 1971. Fax: the Principles and Practice of Facsimile Communication. B.m.: Chilton Book Company. ISBN 978-0-8019-5641-6.

[7] For example, one of the first Colossus vacuum tube computers from 1943 was used for this purpose, which enabled decoding messages encoded using the so-called Lorenz cipher.

[8] For example, the first electronic stock exchange with the NASDAQ digital trading system, which quickly became a tool for trading on stock exchanges around the world, was established by the National Association of Securities Dealers in 1971. The Society for Worldwide Interbank Financial Telecommunication (SWIFT) was established in 1973. In 1977, it implemented a common policy of 239 banks in the field of international payments, communication and data transfer between financial and non-financial institutions and between banks. For more detail, see SWIFT.COM, not dated. SWIFT history. SWIFT – the global provider of secure financial messaging services [online] [accessed on 2023-02-03]. Available from: https://www.swift.com/about-us/history

[9] Michael Bloomberg founded a group of programmers in International Market Systems (IMS), later renamed Bloomberg L.P., who developed a computer information system accessible from a terminal that provided information on current stock market developments, analysed the data, and predicted the relevant financial calculations.

appeared for the first time in project management (Financial Services Technology Consortium) of the American bank Citicorp,[10] followed by advances in financial technologies and FINTECH companies (e.g. Amazon, Apple, PayPal, etc.) including their competitive struggle for customers.

Despite the fact that the FINTECH sector was hit hard by the economic crisis at the beginning of the 21st century, which left, inter alia, a certain disdain of the general society for financial markets, it also made room for innovation in financial technologies, currently including, for example, blockchain[11] and cryptocurrencies,[12] payouts,[13] investments and asset management,[14] loans and capital raising,[15] insurance[16] and more.[17]

3. Theoretical foundation of FinTech and its segments, positives and negatives of a given state

Due to the fact that the field of FINTECH represents a number of difficult-to-grasp technologies, processes and procedures related to them, but also the companies involved in the respective activity, it is difficult to provide not only its terminological interpretation, but also the related legal regulation of the respective issue. According to some experts, the term FINTECH *"covers all activities at the intersection of modern information technologies and traditional financial services."*[18] Others argue that the term primarily refers to *"technology start-ups offering digital technologies that access financial services in an innovative way or that can fundamentally change how banking services and*

[10] For more detail, see Zimmerman, Eilene, 2016. The Evolution of FinTech. The New York Times [online]. [accessed on 2023-02- 02]. ISSN 0362-4331. Available from: https://www.nytimes.com/2016/04/07/business/dealbook/theevolution-of-FinTech.html.

[11] Technologies representing a specific form of distributed database without one specific administrator and used to store embedded records after granting authorisation from all network participants.

[12] A digital, encrypted decentralised medium of exchange used not only to purchase goods and services, but also to invest; there are currently approximately 5,000 different cryptocurrencies, the most famous of which are Bitcoin (developed in 2009 by a group of programmers under the name Satoshi Nakamoto) and Ethereum. For more detail, see ASHFORD, Kate, 2020. What Is Cryptocurrency? Forbes Advisor [online] [accessed on 2023-01-22]. Available from: https://www.forbes.com/advisor/investing/what-is-cryptocurrency/.

[13] Online banking and payment applications for mobile devices and smartphones.

[14] InvestTech or WealthTech. (e.g. Wealthfront, Finmason-InvestTech, Robinhood, etc.) and investment and asset management through so-called robo-advisors.

[15] E.g., online loans and capital raising, peer-to-peer (P2P) loans, machine learning, artificial intelligence, crowdfunding, etc.

[16] InsurTech interconnecting the insurance sector with emerging online technologies through its products.

[17] E.g. provision of software licenses – SaaS (Software as a Service).

[18] Epravo.cz*: Směrnice PSD2 a revoluce v platebních službách* [online]. [accessed on 2023-01-22]. Available from: https://www.epravo.cz/top/aktualne/smernice-psd2-a-revoluce-v-platebnich-sluzbach-102716.html?mail.

products are created and distributed and how profits are generated."[19]

The unified interpretative feature of financial technologies is the fact of innovative solutions and products of the financial market related to it, which improve the process of using and providing financial services, their automation and seamless integration into the software form.

Due to the terminological inconsistency, the FINTECH area is divided into the so-called segments, including the corresponding legislation. The first section of FINTECH is "Financing" (with the subcategories of crowdfunding, loans, and factoring). The second part is "Asset Management" (with the subcategories of "WealthTech", roboconsulting, personal financial management, and social trading).[20] The third segment is "Payments", which consists of blockchain and cryptocurrencies. The last segment is "Other FINTECH", which includes, for example, "InsurTech" or applications comparing individual FINTECH services.[21]

The positive aspects of financial technologies are undoubtedly their timely and financial availability, relative simplicity, speed, and considerable variety of offered services.[22] *However, the above advantages may also mean hidden negatives for many users, where, for example, the simplicity and availability of a loan may mean a significant complication in the future in the event of someone's insufficiently considered step. The weakness of financial technologies is the ever-increasing demand for sufficient protection and security of the processed and provided data,* as well as the slow and highly fragmented process of creating new legislation, which does not correspond to the speed of innovation. In connection with the use of FINTECH, it should also be noted that a significant part of services is provided by artificial intelligence, at the expense of the need for human labour and the increase in the unemployment rate. The disadvantage in the case of cryptocurrency mining is very high energy consumption and, last but not least, the generally negative aspect is the global paradox that people living in developed countries deal with such "problems" as a slow Internet connection, while not so geographically distant other community of society lacks access to drinking water, sufficient food, or high quality education.

[19] INSIDE*: Co je a co není fintech* [online]. [accessed on 2023-01-22]. Available from: https://www.kpc-group.cz/inside/2017/05/co-je-a-co-neni-fintech/.

[20] nextmarkets.com. *What is social trading? Definition & Meaning* [online]. 2023 [accessed on 2023-01-22]. Available from: https://www.nextmarkets.com/en/trading/glossary/social-trading.

[21] Epravo.cz. *FinTech část I. – definice a subjekty?* [online]. 2017 [accessed on 2023-02-22]. Available from: https://www.epravo.cz/top/clanky/fintech-cast-i-definice-a-subjekty-106711.html

[22] Advantages and disadvantages of Fintech companies. *Bbva* [online]. USA: BBVA, 2021, 3 JUNE, 2021 [cit. 2023-02-21]. Available from: https://www.bbva.ch/en/news/advantages-and-disadvantages-of-fintech-companies/.

4. Legislative and institutional background of FinTech from the point of view of the European Union

A very responsible and cautious attitude is applied to the FINTECH legislation from the European perspective, forming the basic constraints of legal regulation, both from the perspective of consumers and investors as well as traditional providers of financial services and the overall concept of financial stability. The international space defines certain standards, serving as possible recommendations for the regulation of financial technologies, and establishes institutions linked to them. In 2011, the European System of Financial Supervision (ESFS) was established, which also includes the European Systemic Risk Board (ESRB). It is appropriate to mention the European Banking Authority (EBA), European Securities and Markets Authority (ESMA) and European Insurance and Occupational Pensions Authority (EIOPA) among the other financial supervisory authorities at the European level. Collectively, these European Supervisory Authorities (ESAs) prepare uniform rules and standards for financial institutions in order to harmonise financial supervision in the European Union.[23]

From the European perspective, the basic legislation in the area of data management and protection is the 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, which permeates the entire area of FINTECH. Another regulatory standard is, for example, the Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market (PSD2), which regulates new payment options and updates the previous Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market. The Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 addresses the issue of preventing the use of the financial system for the purpose of money laundering or financing terrorism, the Directive (EU) 2011/61 of the European Parliament and of the Council of 8 June 2011 addresses alternative investment fund managers, the Directive (EU) 2014/65 of the European Parliament and of the Council of 15 May 2014 focuses on markets and their financial instruments.

5. Legislative and institutional background of FinTech from the point of view of the Czech Republic

In the Czech Republic, the legal regulation of FINTECH is not only

[23] For more detail, see European Central Bank, 2015. European System of Financial Supervision. European Central Bank - Banking Supervision [online] [accessed on 2023-02-03]. Available from: https://www.bankingsupervision.europa.eu/about/esfs/html/index.en.html.

significantly fragmented, but at the same time insufficiently addressed in relation to the constantly growing trends and innovations in the field. The main legislation includes Act No. 370/2017 Coll., on Payment Systems, as amended (hereinafter also referred to as the "Payment System Act")[24] and Act No. 253/2008 Coll., on Selected Measures Against Legitimisation of Proceeds of Crime and Financing of Terrorism, as amended.[25] Other specific areas are regulated, for example, by Act No. 21/1992 Coll., on Banks, as amended, Act No. 229/2002 Coll., on the Financial Arbitrator, as amended, Act No. 277/2013 Coll., on Currency Exchange, as amended, Act No. 6/1993 Coll., on the Czech National Bank, as amended, Act No. 240/2013 Coll., on Investment Companies and Investment Funds, as amended, or Act No. 277/2009 Coll., on Insurance, as amended.

From the institutional background, the Czech National Bank should be mentioned in the first place, which is the main regulating and supervisory authority in the area of payments and the central issuing institution for authorisation and approval proceedings, where it issues authorisations to most entities that provide services on the financial market. The Financial Analytical Office is an administrative body directly subordinate to the Ministry of Finance and it primarily performs the function of a financial intelligence unit for the Czech Republic and administrative supervision in the field of measures against the legalisation of proceeds from crime and for the collection and analysis of suspicious transactions.[26] The Financial Arbitrator of the Czech Republic is a state-established body for out-of-court settlement of consumer disputes on the financial market between consumers and financial institutions providing or intermediating payment services, electronic money, loans, collective investing, investments, life insurance, building savings, currency exchange or pension products.[27] Finally, the Czech FINTECH Association, which was established in 2016, aims to support innovation in the financial sector, consultancy and development coordination.

[24] The Payment System Act was adopted for the purpose of harmonisation with PSD2. The relevant legal regulation regulates the activities of persons authorised to provide payment services and issue electronic money, participation, establishment and operation of payment systems, the rights and obligations of entrepreneurs who provide payment services as well as the rights and obligations of entrepreneurs who issue electronic money, uniform designation of services associated with a payment account, procedure for changing a payment account and access to it, etc.

[25] After the last amendment to the act of 01.08.2021, for example, there was an extension of obliged persons, defining more identification obligations, client control, reporting suspicious transactions, etc.

[26] Financial Analytical Office. *Finanční analytický úřad* [online]. Praha: FAU, 2022 [accessed on 2023-02-03]. Available from: https://www.financnianalytickyurad.cz/.

[27] Office of the Financial Arbitrator, organisational unit of the state. *FA: https://finarbitr.cz/cs/* [online]. Praha: Kancelář finančního arbitra, 2023 [accessed on 2023-02-01].

6. Cybersecurity in relation to the modern trends in FinTech

Based on the direct proportion to the constantly improving FINTECH capabilities, it is necessary to increase the security mechanisms and improve the current methods and tactics to prevent cybercrime. During the COVID pandemic, many human activities shifted to the digital environment, which made people's lives easier in many respects and supported the economy in times of emergency, however, statistical outputs from the second point of view clearly speak of the resulting increase in cybercrime, where European Union surveys from 2022 show that 28% of medium and small enterprises in Europe encountered cybercrime in 2021. The issue of cybersecurity, which is constantly under threat, is an obvious part of all day-to-day activities of society and has an impact on a wide range of areas, including the basic principles of democracy. Thus, cyber attacks not only individually commit evil, but also systemically disrupt the operation of government agencies or critical infrastructure and weaken the citizens' confidence in the faith in progress.[28]

The main sectors affected by cyber attacks (e.g., ransomware, malware, cryptojacking, social engineering threats, deepfake, etc.), according to the European Union Agency for Cybersecurity, in the period from June 2021 to June 2022, included:

- Public administration (24% of the total number of reported incidents)
- Digital service providers (13%)
- General public (12.4%)
- Services (11.8%)
- Banking/finance (8.6%)
- Healthcare (7.2%)[29]

7. Conclusion and prospects for progress

Although the digitisation of financial services represents the highest possible level of comfort for the target entities when needed, it also creates many pitfalls and threats for them. Rapidly emerging financial technologies are making significant progress and the products of the market, which seemed unrealistic until recently, are now not only a matter of course, but also soon become obsolete, outdated and unsatisfactory. Modern trends in the form of, e.g., *start-ups, NFT, smart payments, online identification, market places, Web3, cryptotechnology, regulatory sandbox, payouts as salary advances, e-money payouts, crypto*

[28] Cybersecurity: why reducing the cost of cyberattacks matters. [online]. European Parliament, 2022, [accessed on 2023-02-03]. Available from: https://www.europarl.europa.eu/news/en/headlines/society/20211008STO14521/cybersecurity-why-reducing-the-cost-of-cyberattacks-matters.

[29] Cybersecurity: main and emerging threats. europarl.europa.eu [online]. European Parliament, 2022, [accessed on 2023-02-03]. Available from: https://www.europarl.europa.eu/news/en/headlines/society/20220120STO21428/cybersecurity-main-and-emerging-threats.

payouts, or early payouts, will be an outdated category soon again and services that are above standard today are already waiting to be overcome, e.g., in the form of automated use of artificial intelligence,[30] consisting in the ability of machines to imitate human capabilities, such as thinking, learning, planning, or creativity.[31] *Artificial intelligence enables* technical systems to respond to perceptions (data) from the environment, solve problems and invent solutions, copy human capabilities and subsequently evaluate them, respond to them and replace human activity, and it will be a key area in the transformation of digital society.

Along with the soaring development of FINTECH, it is also necessary to consider its sustainability, uniformity of development and, above all, sufficient legal background and security. The near future of FINTECH is aimed at combining artificial intelligence and machine learning, which have the potential to improve the efficiency and accuracy of financial services,[32] to improve and develop new applications for the blockchain technology and cryptocurrencies, to create new payment portals and technologies, or to improve digital payments and transfers.

The seemingly different worlds of finance and technology are thus cumulatively creating the progress, innovation and modernisation of the 21st century.

Bibliography

1. Advantages and disadvantages of Fintech companies. *Bbva* [online]. USA: BBVA, 2021, 3 June, 2021 [cit. 2023-02-21]. Available from: https://www.bbva.ch/en/news/advantages-and-disadvantages-of-fintech-companies/.
2. Ashford, Kate, 2020. *What Is Cryptocurrency? Forbes Advisor* [online] [accessed on 2023-01-22]. Available from: https://www.forbes.com/advisor/investing/what-is-cryptocurrency/.
3. BIS, 2019. Innovation and FinTech [online]. [accessed on 2023-02-08]. Available from: https://www.bis.org/topic/FinTech.htm.
4. Costigan, Daniel M., 1971. Fax: *the Principles and Practice of Facsimile Communication*. B.m.: Chilton Book Company. ISBN 978-0-8019-5641-6.
5. *Cybersecurity: main and emerging threats. europarl.europa.eu* [online]. European Parliament, 2022, [accessed on 2023-02-03]. Available from: https://www.europarl.europa.eu/news/en/headlines/society/20220120STO21428/cybersecurity-main-and-emerging-threats.

[30] For more detail, see PWC, 2016. Q&A What is FinTech [online] [accessed on 2023-02-03]. Available from: https://www.pwc.com/us/en/financial-services/publications/viewpoints/assets/pwc-fsi-what-isFinTech.pdf.

[31] Europarl.europa.eu. *Umělá inteligence: definice a využití. Evropský parlament* [online]. [accessed on 2023-02-03]. Available from: https://www.europarl.europa.eu/news/cs/headlines/society/20200827STO85804/umela-inteligence-definice-a-vyuziti.

[32] Lazarow, Alex, *The Future of Fintech, According to AI*. Forbes [online]. USA: Forbes, 2022 [cit. 2023-02-21]. Available from: https://www.forbes.com/sites/alexlazarow/2022/12/10/the-future-of-fintech-according-to-ai/?sh=75eac3dc3336

6. *Cybersecurity: why reducing the cost of cyberattacks matters.* [online]. European Parliament, 2022, [accessed on 2023-02-03]. Available from: https://www.europarl.europa.eu/news/en/headlines/society/20211008STO1451/cybersecurity-why-reducing-the-cost-of-cyberattacks-matters.
7. *Epravo.cz: Směrnice PSD2 a revoluce v platebních službách* [online]. [accessed on 2023-01-22]. Available from: https://www.epravo.cz/top/aktualne/smernice-psd2-a-revoluce-v-platebnich-sluzbach-102716.html?mail.
8. *Epravo.cz. FinTech část I. – definice a subjekty?* [online]. 2017 [accessed on 2023-02-22]. Available from: https://www.epravo.cz/top/clanky/fintech-cast-i-definice-a-subjekty-106711.html.
9. Europarl.europa.eu. *Umělá inteligence: definice a využití. Evropský parlament* [online]. [accessed on 2023-02-03]. Available from: https://www.europarl. europa.eu/news/cs/headlines/society/20200827STO85804/umela-inteligence-definice-a-vyuziti.
10. European Central Bank, 2015. European System of Financial Supervision. European Central Bank - Banking Supervision [online] [accessed on 2023-02-03]. Available from: https://www.bankingsupervision.europa.eu/about/esfs/html/index.en.html.
11. Federal Reserve Bank of New York, 2015. Fedwire and National Settlement Services [online] [accessed on 2023-03-03]. Available from: https://www.newyorkfed.org/aboutthefed/fedpoint/fed43.html.
12. Financial Analytical Office. *Finanční analytický úřad* [online]. Praha: FAU, 2022 [accessed on 2023-02-03]. Available from: https://www.financnianalytickyurad.cz/.
13. Garbutt, Douglas, 1984. *The significance of ancient mesopotamia in accounting history.* „The Accounting Historians Journal". 11(1), 83–101. ISSN 0148-4184.
14. INSIDE: Co je a co není fintech [online]. [accessed on 2023-01-22]. Available from: https://www.kpc-group.cz/inside/2017/05/co-je-a-co-neni-fintech/.
15. Lazarow, Alex. *The Future of Fintech, According to AI*. Forbes [online]. USA: Forbes, 2022 [cit. 2023-02-21]. Available from: https://www.forbes.com/sites/alexlazarow/2022/12/10/the-future-of-fintech-according-to-ai/?sh=75eac3dc3336.
16. Nextmarkets.com. *What is social trading? Definition & Meaning* [online]. 2023 [accessed on 2023-01-22]. Available from: https://www.nextmarkets.com/en/trading/glossary/social-trading.
17. Office of the Financial Arbitrator, organisational unit of the state. [online]. Praha: Kancelář finančního arbitra, 2023 [accessed on 2023-02-01] Available from: https://finarbitr.cz/cs/.
18. PWC, 2016. Q&A What is FinTech [online] [accessed on 2023-02-03]. Available from: https://www.pwc.com/us/en/financial-services/publications/viewpoints/assets/pwc-fsi-what-isFinTech.pdf.
19. Swift.com, not dated. SWIFT history. SWIFT – the global provider of secure financial messaging services [online] [accessed on 2023-02-03]. Available from: https://www.swift.com/about-us/history.
20. Vilnius, IMF Deputy Managing Director Tao Zhang and LITHUANIA, not dated. Balancing FinTech Opportunities and Risks. IMF [online] [accessed on 2023-01-11]. Available from: https://www.imf.org/en/News/Articles/2019/06/

10/sp061019-balancing-FinTech-opportunitiesand-risks.
21. Zimmerman, Eilene, 2016. The Evolution of FinTech. The New York Times [online]. [accessed on 2023-02- 02]. ISSN 0362-4331. Available from: https://www.nytimes.com/2016/04/07/business/dealbook/theevolution-of-FinTech.html.

Freedom of Expression in Cyberspace: The Good and the Bad

Associate professor **Carmen MOLDOVAN**[1]

Abstract

The hegemony of Internet and social networks created an unprecedented environment for communication of opinions and ideas, a fundamental need for the information society. Freedom of expression is one of the most important digital rights and strongly connected to the idea of a fundamental right to access to the Internet (supported by Special Rapporteur Frank la Rue and other international bodies) as part of fundamental rights. The aim of the paper is to analyse the flexibility of the scope and limits of freedom of expression in Cyberspace having as a starting point the general accepted approach that the same safeguards are applicable. The debate also concerns the power relationship between the owners of different parts of Cyberspace and the holders of rights that will be addressed from two different perspectives: positive and negative consequences. The constant evolution and development of communication technologies supports all components of expression and can be easily observed. The negative effects are more sensitive as they imply dissemination of hate speech, incitement to discrimination, war propaganda, misinformation, manipulation, and fake news.

Keywords: *free marketplace of ideas, scope, limits, normative equivalence, digital fundamental rights.*

JEL Classification*:* K24, K33, K38.

1. Preliminary aspects

The emergence of the Internet, its continuous development and the almost unlimited communication through it have certainly contributed to the amplification of freedom of expression as a fundamental right, putting into question both the scope of protection established by international legal acts and the interpretation concerning its extent, given by various bodies and international courts, either through *soft law acts* or legally binding rulings. At the same time, questions arose on the flexibility of its limits and regarding the dilution of its legal protection, under all its components or of other fundamental rights with which it may come into conflict; these aspects were subjected to new analyses from States, which must fulfill both negative and positive obligations in order to ensure the protection standards established by international instruments.

The constant evolution of *Cyberspace* and the direct effects on freedom of expression have determined effort for the recognition of a right to access the Internet as part of fundamental rights. From a broader perspective, the presence

[1] Carmen Moldovan - Faculty of Law, „Alexandru Ioan Cuza" University of Iași, Romania, carmen.moldovan@uaic.ro.

of people in Cyberspace has determined the emergence of the concept of *digital rights*[2], which implies the recognition of new fundamental rights or new dimensions or interpretations of the rights and freedoms already recognized internationally and accepted in the systems of domestic law.

The right to access the Internet is part of this category, although it is not enshrined in binding international legal instruments and can be seen as an additional guarantee of the right to free expression both in terms of freedom of opinion and the right of access to information, its main components.

In 2011, the Special Rapporteur for the promotion and protection of the right to freedom of opinion and expression[3], within the Human Rights Council of the United Nations, Frank La Rue, emphasized that access to the Internet is not yet recognized as a human right, but states have a positive obligation to create a favourable environment that allows the exercise of the right to freedom of expression and opinion by all persons, which implies the establishment of effective and concrete policies in order to ensure universal access to the Internet[4]. This position emphasizes the importance of the Internet for communication today, but also the need to adapt to new requirements.

In the *General Comment no. 34 to article 19 of the International Covenant on Civil and Political Rights*[5], the Human Rights Committee recommends that states undertake all measures to protect the independence of new means of communication and ensure people's access to them. This represents a new approach of international bodies, as a result of the awareness of the influence of the Internet in many aspects of human interaction and substantial changes of legal relations in certain fields, including the exercise of freedom of expression, information and opinion. Although the direct reference in the General Comment no. 34, may seem natural and obvious, its significance should not be minimized or neglected, as the scope of Article 19 of the International Covenant on Civil and Political Rights includes not only freedom of expression, but the technical means through which it is exercised are also protected; therefore, there is a very close connection between Internet and expression, a strong link that determines an increased level of protection in the case of expression on the Internet, as compared

[2] D. Dror- Shpoliansky, Y. Shany, *It's the End of the (Offline) World as We Know It: From Human Rights to Digital Human Rights – A Proposed Typology*, „The European Journal of International Law", Vol. 32, 2021, no. 4, pp. 1249–1282, https://doi.org/10.1093/ejil/chab087.

[3] Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, A/HRC/17/27, 2011. Available at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G11/132/01/PDF/G1113201.pdf?OpenElement (accessed 20 March 2023).

[4] Ibid.

[5] Human Rights Committee, *General comment No. 34. Article 19: Freedoms of opinion and expression* (CCPR/C/GC/34), 102nd session, Geneva, July 11-29, 2011. Available at: http://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf (accessed 20 March 2023).

to the protection recognized only for the freedom of expression[6].

From a critical perspective, the emergence and recognition of new categories of fundamental rights, in relation to Cyberspace, creates the conditions to address the issue of dilution of protection for those rights already recognized in the offline environment[7].

Beyond possible criticism or underlining some aspects regarding the inadequacy of the use of the same rules and principles as those from the offline environment, the dark side of using freedom of expression and the freedom of the Internet to spread ideas, opinions, statements, messages that exceed the universally admitted and accepted limits of exercise of freedom of expression, raises many issues regarding the prompt identification of these types of speech excluded from protection, the removal of the content and the sanctioning of the authors.

The elements that complicate this apparently simple mechanism are represented by the fact that platforms and social networks are owned by private entities, which have established rules and automatic mechanisms for removing inappropriate content, but their actions are not always prompt or proportionate. In addition, there may be differences in the legal approach of certain notions, topics, from one state or to another, which may determine the application of different standards or special rules.

2. Exercising freedom of expression without borders

Freedom of expression is a characteristic of democratic societies, it has axiomatic and transversal value, in the sense that it does not only have an individual function, based on values associated with *the forum internum* of the person[8], on human dignity and autonomy[9], it also serve a social function and impacts the development of other fundamental rights and of the entire society, by creating the favourable framework for participation in the debates on subjects of public interest, guaranteeing pluralism and tolerance.

The expression of opinions and ideas serves to achieve a social goal, because it is a means by which people interact with each other, reveal themselves, communicate ideas, opinions, thoughts and feelings, build connections, communicate messages in different forms and ways, create artistic works and so they support a varied and broad social order. Special roles of freedom of expression

---

[6] C. Moldovan, *Libertatea de exprimare. Garanții și responsabilități. Ghid de standarde internaționale și europene*, Ed. Hamangiu, Bucharest, 2018, p. 6.

[7] S. Kaplan, *When everything is a human right , nothing is*, 2019, https://foreignpolicy.com/2019/09/06/when-everything-is-a-human-right-nothing-is/.

[8] G. Gunatilleke, *Justifying Limitations on the Freedom of Expression*, Human Rights Review, Volume 22, 2021, pp. 91–108, https://doi.org/10.1007/s12142-020-00608-8.

[9] MA Civic, *The Right to Freedom of Expression as the Principal Component of the Preservation of Personal Dignity: An Argument for International Protection Within All Nations and Across All Borders*, „University of Pennsylvania Journal of Law and Social Change", Volume 4. Issue 1, 1997, pp. 117-145.

are recognized in the political activities, and also in the way public authorities conduct their activities in general, considering is essential role in building a correctly informed public opinion, the collective will, and providing an effective communication and verification mechanism with the government.

Freedom of expression is guaranteed in all international instruments for the protection of fundamental rights and is core right[10]. The international standards established at the universal and regional level were also acknowledged by the national bodies, thus a symmetry of the regulatory instruments and common elements has been created. Moreover, as regards he protection framework, all analysis have as a starting point *the Universal Declaration of Human Rights*[11], which in its Article 19 provides:

"*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*."

The Universal Declaration directly refers to the irrelevance of state borders in the transmission of opinions and access to information. These terms – *regardless of frontiers* – are a feature of all international instruments guaranteeing freedom of expression and was an important element in recognizing the application of the same principles to communication on the Internet as those in the offline environment.

Also at the universal level, the International Covenant on Civil and Political Rights[12], in Article 19, guarantees this right to freedom of expression in a more detailed manner, including the limitation clause of the right and the admissibility requirements[13]. Regarding the possibility of restricting freedom of expression, article 20 para. (2), is highly relevant as its content is clear and provides that the support of national, racial or religious hatred that represents incitement to discrimination, hostility or violence will be prohibited by law. Consequently, states parties to the Covenant have the obligation to criminalize such actions in their domestic legislation.

At the European level, a similar content can be found in the European

[10] S. Fredman, *Comparative Human Rights*, Oxford University Press, 2028, p. 305.
[11] *Universal Declaration on Human Rights*, December 1948, GA Res. 217 A (III), UN Doc. A/810.
[12] *International Covenant on Civil and Political Rights*, UNGA Res. 2200A (XXI), December 1966, 21 U. N. GAOR Supp. (No. 16), UN Doc. A/6316 (1966), 999 UNTS 171, entered into force on March 23, 1976.
[13] Article 19 reads as follows: "1. Everyone shall have the right to hold opinions without interference. 2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice. 3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary: (a) For respect of the rights or reputations of others; (b) For the protection of national security or of public order (*ordre public*), or of public health or morals."

Convention on Human Rights[14], in Article 10[15] and in the Charter of Fundamental Rights of the European Union[16], an instrument with binding legal force[17], which in Article 11 enshrines freedom of expression[18], and in Article 52 expressly establishes that the interpretation and application of must be made by reference to the standards established by the European Convention on Human Rights[19].

Although the expression *regardless of frontiers* is common to all said international instruments, obviously meant the physical borders between states, it is also applicable in terms of communication in the digital environment, which appeared as a free, open space outside the control of states (at least until of the doctrine of digital sovereignty emerged, supported by the Russian Federation and China[20]).

3. The free market *place of idea*[21] in Cyberspace

The digital environment is practically unlimited, in continuous expansion, in principle for the most part outside the control of states and allows the

[14] *The Convention for the Protection of Human Rights and Fundamental Freedoms* (known as the European Convention on Human Rights) was adopted by the Council of Europe, in Rome, on November 4, 1950, and entered into force on September 3, 1953. Romania ratified the Convention on June 20, 1994 by Law no. 30/1994 (Oficial Gazette no. 135 of May 31, 1994).

[15] Article 10 of the European Convention reads as follows: "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. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises. 2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary."

[16] OJ C 326, 26.10.2012, p. 391–407.

[17] By the Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed in Lisbon, December 13, 2007, entered into force on December 1, 2009 (OJ C no. 306, December 17, 2007).

[18] Art. 11. Freedom of expression and information - reads as follows: "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. 2. The freedom and pluralism of the media shall be respected."

[19] In this sense, article 52 para. (3) of the Charter provides:" In so far as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention. This provision shall not prevent Union law providing more extensive protection."

[20] C. Moldovan, *Suveranitatea digitală- viitorul spațiului virtual, „*Analele Științifice ale Universității „Alexandru Ioan Cuza" din Iași", Tom LXVII, Supplement 2, Juridical Sciences, 2021, pp. 271-284, DOI: 10.47743/jss-2021-67-4-19.

[21] The term was first used by Justice Holmes of the United States Supreme Court in the 1919 dissenting opinion in *Abrams v. US*.

transmission, with an astonishing speed, of opinions, ideas, statements, throughout the globe (except in cases where governmental authorities use censorship and exercise control over information) and provide anonymity if that is the user's option.

All these features contribute to a more extensive protection of communication, placed in the sphere of positive consequences on the development of freedom of expression. Moreover, General Comment no. 34, includes in the category of journalist's bloggers or people who engage in various forms of self-publishing on the Internet or by other means[22], which determines the application of the broadest standards regarding the recognized safeguards for freedom of expression of opinions and access to information.

One should stress that the entire evolution of communication in Cyberspace has not transformed this fundamental right, a derogable or relative right, into an absolute one. On the contrary, the requirements established by international instruments adopted long before the creation of the Internet and Cyberspace are equally applicable to communication in this environment, both in scope and in terms of the possibility of establishing restrictions, conditions or limits to its exercise. In other words, as it results from different interpretations, the same standards and safeguards from the offline environment are to be applied in the online environment; and this describes the so-called doctrine of normative equivalence[23].

This doctrine was developed as a solution to the attempts to identify to what extent the digital space can be regulated by the will of states, given that it is a creation of private entities. The *post factum* efforts of states to regulate it or to create a partially regulated framework, represent significant steps in the changes of humanity, that raises questions on the power structure, especially in terms of communication and circulation of ideas and opinions. Given the lack of a special legal framework applicable to this environment, the rules and principles already established and implemented must be taken into account. The general approach now is that individuals should enjoy the same rights online as they do offline[24].

Within UNESCO, the development and evolution potential of the Internet was recognized, as well as the fact that it represents an unprecedented resource of information, which opens new opportunities for communication and, in this context, the application of the principles of freedom of expression and human rights appears natural for communication on the Internet and for all types of media platforms, as they will contribute to the development of democracy and dia-

[22] General comment no. 34, para. 44.
[23] D. Dror- Shpoliansky, Y. Shany, *op. cit.*, 2021, pp. 1249–1282, https://doi.org/10.1093/ejil/chab087.
[24] W. Benedek, M.C. Kettemann, *Freedom of expression and the Internet*, Council of Europe Publishing, 2013, pp. 74-107.

logue, so that the Organization promotes the idea of the universality of the Internet, respecting the rules of human rights[25].

This idea correlates to the statement of the United Nations Human Rights Council that the same rights protected offline must be protected in the online environment, in particular, freedom of expression, which applies regardless of borders and through any type of means of communication, as provided for in article 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights[26].

General comment no. 34 also provides that restrictions on the operation of websites must comply with the same requirements as those established by article 19 in para. 3[27]. In the same line of approach, within the Council of Europe, the 2016 Recommendation of the Committee of Ministers to Member States on Internet Freedom mentions that the provisions of the European Convention on Human Rights apply to both offline and online speech, and that states members of the Council of Europe have negative and positive obligations to respect, protect and promote fundamental rights and freedoms on the Internet[28].

Communication, as a generic notion, closely related to all components of freedom of expression is a need in the digital age, not just a freedom guaranteed at different normative levels as part of a relationship between states and rights beneficiaries.

4. Misappropriation of the principles of freedom of expression in Cyberspace

The topic of the extent of specific safeguards of freedom of expression in the online environment also describes the elements of a power relationship between the owners of the digital space and the holders of fundamental rights, in general. Relevant to this point is the fact that states have failed to adopt regulations regarding this environment and the decisive influence that social networks or platforms can exert on users. Control over information or the flow of information on the Internet and different platforms determines the creation of a framework for exercising a wide influence on the narratives, the topics covered and those considered relevant, according to subjective criteria and without pursuing the achievement of a function to disseminate information.

---

[25] UNESCO, *Journalism as a public good* , 2021. Available at: https://unesdoc.unesco.org/ark:/48223/pf0000379826.

[26] Human Rights Council, *The promotion, protection and enjoyment of human rights on the Internet*, A/HRC/20/L.13, June 29, 2012. Available at: https://documents-dds-ny.un.org/doc/UNDOC/LTD/G12/147/10/PDF/G1214710.pdf?OpenElement (accessed 20 March 2023).

[27] Paragraph 43.

[28] *Recommendation CM/ Rec(2016)5 of the Committee of Ministers to member States on Internet freedom*, Adopted by the Committee of Ministers on 13 April 2016 at the 1253rd meeting of the Ministers' Deputies. Available at: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016806415fa (accessed 20 March 2023).

From the perspective of the application of normative equivalence doctrine and the category of *digital rights*, which also includes digital freedom of expression, another right should be recognized - the right to benefit from protection against *hate speech*[29], a type of speech that cannot be included in the scope of protection of freedom of expression. *Hate speech* is not defined as such, comprehensibly, in international instruments.

Its prohibition and qualification as hate speech or hate language is based on the interpretation of the provisions of international acts prohibiting incitement to racial discrimination or war propaganda. Thus, article 20 para. 2 of the International Covenant on Civil and Political Rights prohibits "advocacy of national, racial or religious hatred which constitutes incitement to discrimination, hostility or violence". Similar terms are used in the International Convention on the Elimination of All Forms of Racial Discrimination[30], which provides in article 4 letter a) that states expressly have the obligation "to criminalize the dissemination of ideas based on racial superiority or hatred, incitement to racial discrimination, as well as all acts of violence or incitement to such acts against any race or group of persons of another colour or ethnic origin".

Regarding the European Convention of Human Rights and the jurisprudence of the Strasbourg Court, the prohibition of hate speech is based on the provisions of article 10 para. 2 and article 17 which prohibits the abuse of law[31].

In order to better understand he possible involvement of the use of social media platforms for the spread of hateful language, reference to a specific case registered at the International Court of Justice, involving Facebook and the incitement to hatred and incitement to commit genocide,[32] acts prohibited by the rules of international law and which constitute, and thus excluded from the scope of protection of freedom of expression, may prove useful.

The case addresses the issue of the use of social networks for dissemination, since 2012 of messages that can be qualified as incitement to hatred and to the commit genocide, according to the 1948 Convention on the Prevention and

---

[29] Human Rights Council, *Annual report of the United Nations High Commissioner for Human Rights Addendum Report of the United Nations High Commissioner for Human Rights on the expert workshops on the prohibition of incitement to national, racial or religious hatred, A/HRC/22/* 17 /Add.4, 2013. Available at: https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/SeminarRabat/Rabat_draft_outcome.pdf (accessed on 20 March 2023).

[30]Adopted and opened for signature by the General Assembly of the United Nations by Resolution no. 2106 (XX) of December 21, 1965. Entered into force on January 4, 1969, according to the provisions of art. 19. Romania acceded to the Convention on July 14, 1970, through Decree no. 345 (Official Gazette no. 92 of July 28, 1970).

[31] Article 17 of the European Convention on Human Rights reads as follows:" Nothing in this Convention may be interpreted as implying for any State, group or person any right to engage in any activity or perform any act aimed at the destruction of any of the rights and freedoms set forth herein or at their limitation to a greater extent than is provided for in the Convention".

[32] International Court of Justice, *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (The Gambia v. Myanmar).* Available at: https://www.icj-cij.org/case/178 (accessed March 20, 2023).

Suppression of the Crime of Genocide[33], against the Rohingya Muslims. The analysis is based on the application from November 2019 of Gambia against Myanmar, alleging the violation of international obligations under the Genocide Convention, Rohingya Muslims, which generated the killing of civilians or their leaving the national territory.

In January 2020, the International Court of Justice granted Gambia's request for interim measures and ordered Myanmar to prevent acts of genocide against the Rohingya Muslims[34].

The relevance of Facebook's involvement is determined by the fact that in Myanmar, during the analysed period, Facebook represented the main news platform and the means of transmitting messages inciting to hatred and to violence, facts brought to the attention of the International Court of Justice by the application of Gambia. Facebook's refusal to provide information on the content of these messages, which had been deleted, led Gambia to turn to the competent court in the United States of America to obtain them - the District Court for the District of Columbia, which granted the request.

On September 22, 2021, the District Court for the District of Columbia ruled that Facebook must disclose material related to incitement to ethnic hatred against the Rohingya Muslim minority in Myanmar. The request referred to both the content that was deleted from the platform and internal investigation documents, and in the opinion of the American court, the deleted content of Facebook was not subject to the non-disclosure rule of the legislation on stored communications (*Stored Communications Act*); pages and posts that were still publicly accessible before Facebook's deletion fell within the statutory exception to the non-disclosure rule.

As relevant factual elements in this case, in 2012 in the state of Rakhine, in Myanmar, where the Rohingya Muslims lived, violence broke out that caused their large-scale displacement. Acts such as burning and looting of houses and summary executions were committed. Internationally, several human rights organizations, including the United Nations Human Rights Council, have alleged that the acts of violence were planned and supported by Myanmar's military and security forces. Since October 2016, the Myanmar military has carried out "purging operations" that have resulted in mass killings, executions, disappearances, deprivation of liberty and torture of Rohingya civilians, as well as rape and other sexual and gender-based violence.

---

[33] UN General Assembly, *Convention on the Prevention and Punishment of the Crime of Genocide*, 9 December 1948, United Nations, Treaty Series, vol. 78, p. 277.

[34] International Court of Justice, *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (The Gambia v. Myanmar)*, Order of 23 January 2020. Available at: https://www.icj-cij.org/sites/default/files/case-related/178/178-20200123-ORD-01-00-EN.pdf (accessed on 20 March 2023).

Within the United Nations, more specifically the Human Rights Council[35], a commission of inquiry made up of independent experts was established in 2017 - *Independent International Fact-Finding Mission on Myanmar* - to conduct research in Myanmar.

One of this commission most important findings was in relation to the particularly important role that Facebook played in disseminating information, being "by far the most common social media platform used in Myanmar" for online news. At the same time, Myanmar officials frequently relied on Facebook to release news and information, and it was also used by media outlets as their primary method of publishing[36].

Within Facebook, the reaction was to carry out an evaluation, in 2018, regarding the impact of its presence in Myanmar on human rights, a report which revealed that in this state, "Facebook was the Internet" and that Myanmar officials were able[37] to credibly spread rumours about people and events by using the platform to influence public perception and spread anti-Muslim sentiment and misinformation, all of which led to widespread acts of violence. The entire Rohingya community has been labelled and presented as "illegal migrants" and terrorists (such as the Myanmar state spokesperson, who on June 1, 2012, posted a statement on his Facebook account characterizing them as terrorists), which what contributed to the scale of violent acts in 2012[38].

Also in 2018, Facebook, in an update on the situation in Myanmar, admitted that it had acted too slowly to prevent misinformation and hate[39]. In August 2018, in enforcing the rules on the use of the platform, the company undertook a number of measures: it closed the accounts of important people and organizations in Myanmar, such as the commander-in-chief of the armed forces, the television network, deleted news pages that rebroadcast the messages of state. For "inauthentic coordinated behaviour," consisting of misinformation and hate

[35] United Nations General Assembly, *Situation of human rights in Myanmar,* A/HRC/RES/34/22, 3 April 2017. Available at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G17/081/98/PDF/G1708198.pdf?OpenElement (accessed March 23, 2023).

[36] Human Rights Council, *Report of the independent international fact-finding mission on Myanmar*, A/HRC/39/64, 12 September 2018. Available at: https://www.ohchr.org/en/press-releases/2019/10/un-independent-international-fact-finding-mission-myanmar-calls-a-member?LangID=E&NewsID=25197 (accessed 22 March 2023).

[37] BSR, *Human Rights Impact. Facebook in Myanmar*, October 2018. Available at: https://about.fb.com/wp-content/uploads/2018/11/bsr-facebook-myanmar-hria_final.pdf (accessed March 23, 2023).

[38] United States District Court for the District of Columbia in Application Pursuant to 28 USC § 1782 of The Republic of the Gambia, Petitioner, v. Civil Action No. 20-mc-36-JEB-ZMF. Available at: https://globalfreedomofexpression.columbia.edu/wp-content/uploads/2021/10/In-re-Gambia-v-Facebook.pdf (accessed March 23, 2023).

[39] BSR, *Human Rights Impact. Facebook in Myanmar*, October 2018. Available at: https://about.fb.com/wp-content/uploads/2018/11/bsr-facebook-myanmar-hria_final.pdf (accessed March 23, 2023).

speech against the Rohingya, Facebook deleted 438 pages, 17 groups, 160 Facebook and Instagram accounts followed by nearly 12 million people. All of the deleted content was preserved, but the company`s position on the request to communicate this content was to deny it, even though its own findings qualified the removed messages as hate speech.

Incitement to commit genocide, expressly provided for in Article III of the 1948 Convention, the instrument on which Gambia's claim is based, constitutes the most serious form of hate speech.

The case pending before the International Court of Justice is the first one in which the use of a platform such as Facebook is mentioned, acts carried out through the use of the Internet and means of communication such as social media platforms, as being relevant for establishing the violation of the obligations of a state, based on the Convention since 1948.

As regards Facebook, one could argue that it failed to comply with its *due diligence* and the responsibility to protect obligations, established in the *UN Guiding Principles on Business and Humana Rights*[40], a soft law instrument adopted within the United Nations and to which the Human Rights Council made direct reference, when establishing the commission of inquiry[41].

The 2019 report of the Special Rapporteur on freedom of expression carries out an analysis of *hate speech* in the online environment, of the appropriate means to combat such speeches and ideas, taking as a starting point and example the inaction of Facebook and the failure to manage hateful messages from Myanmar[42].

5. Conclusions

The exercise of freedom of expression on the Internet still generates dilemmas in terms of its content and the application of restrictive measures, not in the sense that they are not determined sufficiently clear, but in the sense that the traditional architecture in the matter of fundamental rights is modified, because

[40] United Nations Human Rights, Office of the High Commissioner, Guiding Principles on Business and Human *Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework*, 2011. Available at: https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf (accessed 20 March 2023).

[41] 24. Encourages all business enterprises, including transnational corporations and domestic enterprises, to respect human rights in accordance with the Guiding Principles on Business and Human Rights, calls upon the Government of Myanmar to meet its duty to protect human rights, and calls upon home States of business companies operating in Myanmar to set out clearly the expectation that all business enterprises domiciled in their territory and/or jurisdiction are to respect human rights throughout their operations.

[42] United Nations General Assembly, *Report of the Special Rapporteur on the promotion and protection of the right to freedom* of opinion and expression, A/74/486, 2019. Available at: https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/A_74_486.pdf (accessed 23 March 2023).

the subjects are no longer just the state and the holders of rights. The digital environment is characterized by the interaction of an array of global factors, and the impact of companies is a particularly important one. The idea of internet neutrality (*net neutrality*) cannot be supported in the context of harmful manifestations that do not only represent deviations from admissible and harmless language, but turn into concrete ways of committing acts of increased gravity.

Social platforms and networks, Cyberspace in general exert a real influence on fundamental rights, that cannot be neglected, and freedom of expression is only one of the relevant aspects. Establishing a balance between freedom of expression and other fundamental rights in this environment is a difficult endeavour, primarily due to the very large number of interested parties and the lack of clearer or more detailed regulations.

Bibliography

1. Benedek, W., Kettemann, M.C., *Freedom of expression and the Internet*, Council of Europe Publishing, 2013.
2. BSR, *Human Rights Impact. Facebook in Myanmar*, October 2018. Available at: https://about.fb.com/wp-content/uploads/2018/11/bsr-facebook-myanmar-hria_final.pdf (accessed March 23, 2023).
3. Civic, M.A., *The Right to Freedom of Expression as the Principal Component of the Preservation of Personal Dignity: An Argument for International Protection Within All Nations and Across All Borders*, University of Pennsylvania Journal of Law and Social Change, Volume 4. Issue 1, 1997.
4. Dror-Shpoliansky, D., Shany, Y., *It's the End of the (Offline) World as We Know It: From Human Rights to Digital Human Rights – A Proposed Typology*, „The European Journal of International Law", Vol. 32 no. 4, https://doi.org/10.1093/ejil/chab087.
5. Fredman, S., *Comparative Human Rights*, Oxford University Press, 2028.
6. Gunatilleke, G., *Justifying Limitations on the Freedom of Expression, Hum Rights Review*, Volume 22, 2021, pp. 91–108, https://doi.org/10.1007/s12142-020-00608-8.
7. Human Rights Committee, *General comment No. 34. Article 19: Freedoms of opinion and expression* (CCPR/C/GC/34), 102nd session, Geneva, July 11-29, 2011. Available at: http://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf (accessed 20 March 2023).
8. Human Rights Council, *Annual report of the United Nations High Commissioner for Human Rights Addendum Report of the United Nations High Commissioner for Human Rights on the expert workshops on the prohibition of incitement to national, racial or religious hatred, A/HRC/22*/17/Add.4, 2013. Available at: https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/SeminarRabat/Rabat_draft_outcome.pdf (accessed on 20 March 2023).
9. Human Rights Council, *Report of the independent international fact-finding mission on Myanmar*, A/HRC/39/64, 12 September 2018. Available at: https://www.ohchr.org/en/press-releases/2019/10/un-independent-international-fact-

finding-mission-myanmar-calls-a-member?LangID=E&NewsID=25197 (accessed 22 March 2023).
10. Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue*, A/HRC/17/27, 2011. Available at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G11/132/01/PDF/G1113201.pdf?OpenElement (accessed 20 March 2023).
11. Human Rights Council, *The promotion, protection and enjoyment of human rights on the Internet*, A/HRC/20/L.13, June 29, 2012. Available at: https:// documents-dds-ny.un.org/doc/UNDOC/LTD/G12/147/10/PDF/G1214710.pdf?OpenElement (accessed 20 March 2023).
12. International Court of Justice, *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (The Gambia v. Myanmar).* Available at: https://www.icj-cij.org/case/178 (accessed March 20, 2023).
13. International Court of Justice, *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (The Gambia v. Myanmar),* Order of 23 January 2020. Available at: https://www.icj-cij.org/sites/default/files/case-related/178/178-20200123-ORD-01-00-EN.pdf (accessed on 20 March 2023).
14. *International Covenant on Civil and Political Rights*, UNGA Res. 2200A (XXI), December 1966, 21 U. N. GAOR Supp. (No. 16), UN Doc. A/6316 (1966), 999 UNTS 171, entered into force on March 23, 1976.
15. Kaplan, S., *When everything is a human right, nothing is*, 2019, https://foreignpolicy.com/2019/09/06/when-everything-is-a-human-right-nothing-is/.
16. Moldovan, C., *Libertatea de exprimare. Garanții și responsabilități. Ghid de standarde internaționale și europene*, Ed. Hamangiu, Bucharest, 2018.
17. Moldovan, C., *Suveranitatea digitală - viitorul spațiului virtual, „*Analele Științifice ale Universității „Alexandru Ioan Cuza" din Iași", Tom LXVII, Supplement 2, Juridical Sciences, 2021, DOI: 10.47743/jss-2021-67-4-19.
18. *Recommendation CM/ Rec(2016)5 of the Committee of Ministers to member States on Internet freedom*, adopted by the Committee of Ministers on 13 April 2016 at the 1253rd meeting of the Ministers' Deputies. Available at: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016806415fa (accessed 20 March 2023).
19. *The Convention for the Protection of Human Rights and Fundamental Freedoms* (known as the European Convention on Human Rights) adopted by the Council of Europe, in Rome, on November 4, 1950, and entered into force on September 3, 1953. Romania ratified the Convention on June 20, 1994, by Law no. 30/1994 (Oficial Gazette no. 135 of May 31, 1994).
20. UNESCO, *Journalism as a public good*, 2021. Available at: https://unesdoc.unesco.org/ark:/48223/pf0000379826.
21. United Nations General Assembly, *Convention on the Prevention and Punishment of the Crime of Genocide,* 9 December 1948, United Nations, Treaty Series, vol. 78.
22. United Nations General Assembly, *Report of the Special Rapporteur on the promotion and protection of the right to freedom* of opinion and expression, A/74/486, 2019. Available at: https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/A_74_486.pdf.
23. United Nations General Assembly, *Situation of human rights in Myanmar*,

A/HRC/RES/34/22, 3 April 2017. Available at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G17/081/98/PDF/G1708198.pdf?OpenElement (accessed March 23, 2023).

24. United Nations Human Rights Office of the High Commissioner, *Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework*, 2011. Available at: https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf (accessed 20 March 2023).
25. United States District Court for the District of Columbia in Application Pursuant to 28 USC § 1782 of The Republic of the Gambia, Petitioner, v. Civil Action No. 20-mc-36-JEB-ZMF. Available at: https://globalfreedomofexpression.columbia.edu/wp-content/uploads/2021/10/In-re-Gambia-v-Facebook.pdf (accessed March 23, 2023).
26. *Universal Declaration on Human Rights*, December 1948, GA Res. 217 A (III), UN Doc. A/810.

Cyber Space and Security in the Cyber Environment. General Considerations

Professor **Carmen Silvia PARASCHIV**[1]

Abstract

The tumult of changes recently encompassed the entire socio-economic field, including information technology, which developed rapidly and sustainably. If in its historical beginnings, information technology represented in society the tool that helped carry out the activity in the field in which it was used, in the sense of optimizing office activities, productive or non-productive, nowadays it is no longer possible to talk about carrying out any activity without the incidence information technology. Defining, in a generous manner, "cyberspace" we can say that it is the entire virtual world around us, the world in which and with which we carry out our entire activity.

Keywords: *cyber space, cyber security, optimization of human resources, virtual world, vulnerability, advantages, digital transformation, information technology, blockchain.*

JEL Classification: K24

1. Introduction

The tumult of changes has recently encompassed the entire socio-economic field, including information technology, which has developed rapidly and sustainably. If in its historical beginnings information technology represented in society the tool that helped to carry out the activity in the field in which it was used, in the sense of optimizing office activities, productive or non-productive, nowadays it is no longer possible to talk about carrying out any activity without the impact of technology the information. Defining, in a generous manner, cyberspace, we can affirm that it is the entire virtual world around us, the world in which and with which we carry out all our activities.

2. It is a real win that we are in cyberspace ?

There are benefits that we haven't thought of, but there are also vulnerabilities and risks in terms of the functioning of the whole space, both at the individual, personal level and at the macro, state level. We are not wrong if we say that cyberspace is currently a real "battlefield".

The authorities signal this aspect, which we find in a statement from the

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

Ministry of Foreign Affairs[2]: "the recent evolution of cyber attacks in our country places the cyber threat among the most dynamic current threats to national security. Romania approaches the field of cyber security as an important dimension of national security, assuming the commitment to ensure the normative framework in the field to face international requirements and to facilitate. on a voluntary basis, bilateral cooperation and the prompt and effective exchange of information between competent authorities to combat the use of Information and Communication Technology/ICT for terrorist or criminal purposes". In the same paradigm is one of the national authorities in the field of cyber security, the Romanian Information Service, which mentions the fact that "at the international level, attacks on computer systems represent a growing phenomenon in recent years, their development often being associated with certain events that they have an impact on nations, communities or groups within society, sometimes becoming the mirror in virtual space of ongoing conflicts in various places in the world".

It is easy to understand the concern shown by the authorities in relation to the field of cyber security, since we cannot affirm and claim that a possible cyber attack would not manifest itself in several areas. Every day comes to confirm the fact that we live in a stage where fields are more and more interdependent, an aspect that is also due to the evolution in the field of information and communication technology.

As I stated before, there are many benefits of technological evolution and the interdependence of fields, but there are also disadvantages that end up being transformed into vulnerabilities that target society as a whole but also individuals in particular. The technological field is a tentacular field that has managed to conquer all social entities. Starting from the fact that we are all dependent on information systems to perform certain activities, (sometimes, in certain fields, most activities) we must prepare to face a new set of challenges that are related, especially to the virtual space , as we all find that the life of each of us, the economic component, as well as the national and international security, depend to a greater or lesser extent on a safe virtual space. All these challenges[3] are included in the concept of cyber security[4] which refers to threats, vulnerabilities and the

[2] *Securitate cibernetică* - htpps://www.mae.ro/node/28364, consulted on 1.03.2022.

[3] Meda Udroiu, *Cyber security – A new dimension of national security*. "Mihai Viteazu" National Academy of Information, article presented at the International Scientific Conference - XXI Strategies with the theme - Complexity and dynamics of the security environment November 24-25, 2015 - Publishing House of the National Defense University "Carol I", Bucharest, 2016, p. 249.

[4] Cybersecurity – the state of normality resulting from the application of a set of proactive and reactive measures that ensure the confidentiality, integrity, availability, authenticity and non-repudiation of information in electronic format, of public or private resources and services in cyberspace. Proactive and reactive measures may include security policies, concepts, standards and guidelines, risk management, training and awareness activities, implementation of technical solutions to protect cyber infrastructures, identity management, consequence management (Appendix no. 1 to Government Decision no. 1.321/2021 regarding the approval of the Cybersecurity Strategy of Romania, for the period 2022-2027, as well as the Action Plan for the implementation of the

need for governments and supranational structures to develop a comprehensive security strategy for their digital network. "Cyber security" in turn is affected by numerous "cyber threats" which, depending on the level they target, can cause damage to various cyber infrastructures. Precisely for this reason, cyber security must represent the object of activity of all those who meet at the level of society, individuals, companies, institutions, private companies and non-profit organizations, but also at the international level between national states, regional organizations and organizations at worldwide, as this aspect concerns the whole society.

All major or minor actors in the use of technology are interested in finding the levers to maintain the security of cyberspace.

At the national level, the legal aspects of cyber security are presented with priority in criminal matters.

Lately we have been witnessing an increase in the phenomenon of computer crime worldwide. It is difficult to stop and equally difficult to censor criminal manifestations due to the fact that there is no standardization of national legislations leading to a unique legislative manifestation for the manifested phenomenon.

It is well known that cyber security has become a particularly important aspect with the phenomenon of globalization of both communication networks, information technology component infrastructures and systems. Economic, political and military that increasingly use cyber systems in the automation of decision-making processes.

Each state is interested and obliged to establish its long-term security policies, as well as the ways to achieve them in order to gain an advantage over other competitors by establishing cyber defense strategies.

In the National Cyber Security Frame Work Manual published in 2012 by the NATO Cooperative Cyber Defense Center of Excellence, it is stated that until the date of publication of this manual "...more than 50 nations have published some form of a cyber strategy that defines what security means for future national and economic security initiatives"[5].

From the content of the manual, but also from the language used, we can see a somewhat permissible association of the terms defense or security with the term cybernetics, in a military context.

Taking into account the fact that a very careful legal regulation is required, especially in criminal matters, in addition to the used notions, specific to the military field, such as "cyber defense" and "cyber security", notions such as "cyber war" are also used, "cyber espionage" even "cyber crime" and sometimes

Cybersecurity Strategy of Romania, for the period 2022-2027, published in the Official Gazette no. 2 of January 3, 2022).

[5] Eugen Valeriu Popa, *Aspecte privind cadrul legal în domeniul apărării cibernetice*, article presented at the International Scientific Conference - XXI Strategies with the theme - Complexity and dynamics of the security environment November 24-25, 2015 - Publishing House of the National Defense University "Carol I", Bucharest, 2016, p. 256.

even "cyber terrorism"[6].

3. Conclusions

The whole range of concepts presented can disturb us and using them without knowing their meaning can give rise to many confusions. Serious and unequivocal legal regulation justifies its presence and usefulness. Law in general and criminal law in particular can be seen primarily as a form of cooperation, the necessary conditions for the existence of an international regulatory framework of cyberspace can only exist in the hypothesis that there are cooperation mechanisms between states when these mechanisms are functional , when a consensus of all those involved in the appreciation of fundamental values is already established, and the cost of lack of participation and involvement is overwhelming.

And here, as in all other social fields, one can support the statement that there is an alignment of individual and collective interests, an aspect that is as natural as possible, since, as is well known, social norms have the ability to generate legal norms; without the existence of these legal norms, society could not exist. The emergence of legal norms and their development leads to the emergence of legal constraints that further support the already existing international legal provisions that ultimately regulate cyber conflict.

The increase in the weight of the cyber component in both military and non-military conflicts leads to the appearance of the initial conditions that generate the emergence of legal norms, but also the desire and the need shown by the subjects involved in the international environment for the integration of these norms into a whole of legal norms that regulate cyberspace[7].

We therefore find that the existence of the cyberspace gives birth, as was natural, to the need for the existence of legal norms that give all participants rights and obligations alike.

I conclude with the initial statement, it is not wrong to say that cyberspace is currently a real battlefield.

Bibliography

1. Dobák, Imre, *Thoughts on the evolution of national security in cyberspace*, „Security and Defence Quarterly", vol. 33, no. 1, 2021, doi:10.35467/sdq/133 154.
2. Government Decision no. 1.321/2021 regarding the approval of the Cybersecurity Strategy of Romania, for the period 2022-2027, as well as the Action Plan for the implementation of the Cybersecurity Strategy of Romania, for the period 2022-2027, published in the Official Gazette no. 2 of January 3, 2022.

[6] Dobák, Imre, *Thoughts on the evolution of national security in cyberspace*, „Security and Defence Quarterly", vol. 33, no. 1, 2021, pp. 75-85. doi:10.35467/sdq/133154.
[7] See Lippert, Kari J., and Robert Cloutier, *Cyberspace: A Digital Ecosystem*, „Systems" 9, no. 3: 48, 2021, https://doi.org/10.3390/systems9030048.

3. Lippert, Kari J., and Robert Cloutier, *Cyberspace: A Digital Ecosystem*, „Systems" 9, no. 3: 48, 2021, https://doi.org/10.3390/systems9030048.
4. Popa, Eugen Valeriu, *Aspecte privind cadrul legal în domeniul apărării cibernetice*, article presented at the International Scientific Conference - XXI Strategies with the theme - Complexity and dynamics of the security environment November 24-25, 2015 - Publishing House of the National Defense University "Carol I", Bucharest, 2016.
5. *Securitate cibernetică* - htpps://www.mae.ro/node/28364, consulted on 1.03. 2022.
6. Udroiu, Meda, *Cyber security – A new dimension of national security*. "Mihai Viteazu" National Academy of Information, article presented at the International Scientific Conference - XXI Strategies with the theme - Complexity and dynamics of the security environment November 24-25, 2015 - Publishing House of the National Defense University "Carol I", Bucharest, 2016.

Profiling Criminals in Cyberspace

Lecturer **Aurel Octavian PASAT**[1]

Abstract

The article deals with issues related to the definition of cybercrime, the ways in which crime manifests itself in cyberspace, types of cybercrime, creating a profile of criminals in cyberspace. As in traditional criminal investigation, cybercrime profiling is a key component in cybercrime investigations as well. One of the components of this model is the theory by which it will be possible to describe, explain and subsequently predict not only criminal professionalism as a social phenomenon, but also the personality of a modern cybercriminal.

Keywords*: cyber space, cyber crime, cyber crimes, cyber profiling.*

JEL Classification: K14, K24

1. Introduction

Cyberspace is still an unknown place and we can say that we know and use only a small part of it. It is a complex ecosystem: if used correctly and controlled, it allows the production and exchange of information from a distance and is a remarkable resource, not only for those who use the Internet for business purposes, but also as a simple means of communication and exchange of views[2].

However, it also offers the possibility of committing, not infrequently, illegal acts, with the perception of the offender remaining unpunished: the screen, besides acting as a filter between the agent and the potential victim of the crime, allows the former to act unmolested wherever he or she is, without the need to be physically at the scene of the crime[3].

Cybercrime differs from traditionally understood crime and is defined in the literature as: "*crime in which the conduct or material object of the crime is linked to a computer or telecommunications system or is committed using such a* system"[4].

Currently, cybercrime is the fastest growing crime compared to other

---

[1] Aurel Octavian Pasat - Transfrontier Faculty, "Lower Danube" University from Galati, Romania, Aurel.Pasat@ugal.ro.

[2] Dodge, M., Kitchin, R. (2001) *Mapping Cyberspace*. London: Routledge, p. 75.

[3] Barak, A. (2008) *Psychological Aspects of Cyberspace*. Cambridge: Cambridge University Press, p. 124.

[4] Cadoppi, A., Canestrari, S., Manna, A., & Papa, M. (2019). *Cybercrime*. Vicenza: UTET Giuridica, p. 48.

crimes. The situation is made more complex by the increasing transnational nature of crime[5]. According to expert forecasts, cybercrime will have overtaken the entire drug market by 2021 and the damage will be six trillion worldwide. An Indian criminologist, Professor Karuppannan Jaishankar reasonably points out that cybercrime is no longer just a hacker attack or an attack on the system, it is an attack on people[6]. Global Cyber Data - 2018 Risk Perception Survey revealed that nearly two-thirds of respondents rated cyber risk as one of the top five risks in their organization[7].

At the same time, it should be noted that the offender who commits crimes in cyberspace has several advantages over the traditional offender:

1) the offender can choose his victim from a very large, global area;

2) the offender may remain unknown to the victim;

3) the offender does not interact directly with the victim, does not use a physical weapon:

4) there is a low risk of the offender's actions being discovered, the offender does not have to flee the scene of the crime.

Crime in cyberspace takes many forms. First, we find cyberstalking, defined as the digital transposition of the crime of stalking. Cyberbullying, an extension of the wider phenomenon called "bullying", consists of any form of pressure, aggression, harassment, blackmail, insult, denigration, defamation, identity theft, alteration, illegal acquisition, manipulation, illegal processing of personal data carried out electronically; as well as the dissemination of online content - which also concerns one or more members of the minor's family - the intentional and predominant purpose of which is to isolate a minor or a group of minors, committing serious abuse, a harmful attack or ridicule.[8]

Staying on the topic of crimes against the person, we find crimes such as sexting, online grooming, revenge porn and the crime of sexual extortion[9].

The Internet is also fertile ground for those who want to commit property crime. Some examples of these illegal activities are fraud, theft, money laundering and illegal trafficking, in which organised crime has its roots, but changes its *modus operandi* by moving from the real world to cyberspace.

---

[5] Greco F., Greco G., *Investigative Techniques in the digital age: Cybercrime and criminal profiling*, „European Journal of Social Sciences Studies", Vol. 5, Issue 3, 2020, p. 4, https://oapub. org/soc/index.php/EJSSS/article/view/821/1403.

[6] Tumalavicius V., Ivanciks J., Karpishchenko O. (2016) *Issues of society security: public safety under globalization conditions in Lithuania*, „Journal of Security and Sustainability", Issues 4(9): 545-573. https://doi.org/10.9770/ jssi.2016.5.4(9).

[7] *Global Cyber Risk Perception Survey 2018*. By the Numbers: Global Cyber Risk Perception Survey. Available at: https://www.marshmma.com/blog/2018-cyber-and-data-security-risk-survey -report.

[8] Greco F, Greco G., *Investigative techniques in the digital age: cybercrime and criminal profiling*, *op. cit*., p. 7.

[9] Nicola, H., & Powell, A. (2016). *Sexual Violence in the Digital Age: The Scope and Limits of Criminal Law*. „Social & legal studies", *25*(4), 397-418.

As far as the economic and financial sector is concerned, cybercrime refers to so-called "*white-collar crime*". This type of crime is the expression used to indicate economic crime, with a particular focus on the perpetrators and their position in the social and productive structure to which they belong. Typologies include: falsification of company financial statements, stock market rigging, direct or indirect corruption of public officials to obtain advantageous contracts and decisions, false advertising, fraud in the exercise of trade, embezzlement and misappropriation of funds, tax fraud, misconduct in the event of failure and bankruptcy.

According to cybercrime statistics by AAG IT Services, in 2022 nearly 1 billion emails were exposed in a single year, affecting 1 in 5 internet users, data breaches cost companies an average of $4.35 million in 2022, approximately 236.1 million ransomware attacks occurred globally in the first half of 2022, 1 in 2 US internet users had their accounts breached in 2021, 39% of UK businesses reported experiencing a cyber attack in 2022, 53.35 US citizens were affected by cybercrime in the first half of 2022, cybercrime cost UK businesses an average of £4200 in 2022, in 2020, malware attacks increased 358% compared to 2019, and the most common cyber threat faced by businesses and individuals is phishing[10].

The RAT guidelines stated that cybercrime occurs when three elements interact in time and space: a motivated cybercriminal, a suitable victim (a suitable target) and the lack of an active and capable defender. Thus, cybercrime occurs when there is a motivated cybercriminal and a suitable victim and there is no one who could prevent a cybercrime[11].

2. Behavioural profile of offenders in cyberspace

One of the differences found between stalking and cyberstalking is that in the former case, the attacker, in order to stalk the victim, will have to follow them, stalk them at home or at work and therefore limit the stalking over time. The cyberstalker, on the other hand, has the possibility to "*torture*" his victim night and day, without having to get up from his chair, but only with the help of a computer or telematics system. In this respect, an attempt has been made to draw up a first behavioural profile of this subject: it appears that the cyberstalker's behaviour develops on the net by sending countless amounts of emails with offensive and demeaning tones, anonymously discloses on the private web material concerning the victim, assumes the victim's identity for malicious purposes and enters without permission the victim's computer system[12].

[10] https://aag-it.com/the-latest-cyber-crime-statistics/, consulted on 1.03.2023.
[11] Zuhri F.A., *The Profile of a Cybercriminal*. Digital Forensic Magazine. Available at: http://digitalforensicsmagazine.com/blogs/wp-content/uploads/2017/05/The-Profile-of-Cybercriminal.pdf.
[12] Ziccardi, G. & Perri, P. (2017). *Tecnologia e diritto*. Milano: Giuffré, pp. 270-275.

Although it may seem reductive, this is a prime example of criminal profiling of a cybercriminal.

Cyberbullying, unlike traditional bullying, uses the net to commit crimes, threats in cyberspace, using photos and videos, threatening emails and instant messages in chat, persistent SMS and MMS, websites and blogs, often violating the Civil Code, or the Penal Code.

What characterises cybercrime is the lack of empathy, but also the lack of real, physical contact with the victim. For example, compared to traditional bullying, cyberbullying completely cancels out the space and distance between people, as well as the emotional dimension. In this sense, Faliva[13] argues that the subject on the other side of the screen is perceived as an individual without a body and emotions, the victim is not perceived as a "*human being*" and any sense of empathy or identification is excluded.

There are many types of attacks on the Internet, some of which are listed below:

- *Bash boards* are "*message centres*" where users can post messages anonymously targeting cyberbully victims;

- *Trolling*, on the other hand, is the dissemination of false information about the victim in order to collect responses from other unaware subjects that can later be used to persecute the victim[14];

- *Outing* is the online sharing of embarrassing secrets and images of the victim[15], *while flaming* is the dissemination of vulgar and violent messages in Cyberspace to provoke real verbal battles[16];

- *Online grooming* - with the development of new technologies, the crime of grooming, which is the luring of minors by an adult for sexual purposes, has become established in today's criminal context. Specifically, the paedophile lures the victim by trying to create a confidential and trusting relationship in order to get the victim to meet the attacker[17].

Also, in this case, an attempt was made to create a kind of profile of the paedophile acting on the web: first of all, it can be seen how the groomer acts mainly on social networks - a channel now used globally - by using fake profiles, designed and created specifically for the person he wants to lure.

In addition to creating a likely credible profile, the paedophile overwhelms the victim with attention, adding "*likes*" to every photo posted by the minor. As we know, among young people it is no longer just the appreciation you receive in person and therefore in real life that matters, but how popular and loved

[13] Faliva, C. (Ed.) (2011). *Tra normalità e rischio. Manuale di psicologia dello sviluppo e dell'adolescenza* (Vol. 65). Maggioli Editore, p. 75.
[14] Fabrizio, L. (2015). *Le nuove forme della devianza.* „Psicologia & Giustizia", *16*(1), p. 87.
[15] Gallina, M. A. (2009). *Dentro il bullismo. Contributi e proposte socio-educative per la scuola: Contributi e proposte socio-educative per la scuola*. Milano: Franco Angeli, p. 76.
[16] Greco F., Greco G., *Investigative techniques in the digital age: cybercrime and criminal profiling, op. cit.,* p. 8.
[17] Ibid.

you are on social media. Once he has gained the victim's attention, the paedophile will start contacting the victim in chat and, after gaining her trust, will start an exchange of photos and videos with a sexual background. What matters most is that the attacker acts unconsciously on the victim; children constantly ask questions about sex but, because it is a social taboo, they do not ask for explanations from parents or teachers - authoritative and reference figures. As a result, they will never reveal to their family that they are having such discussions with a stranger, especially if they are encouraged by the attacker not to say anything, with phrases like "*it's our little secret*".

A 2013 study on cybercrime[18] shows that:

1) offenders, who have committed child pornography offences, are aged between 15 and 73 (average age - 49);

2) 60% of offenders not only saved child pornography material, but also distributed it;

3) one fifth of these offenders were not working (they were retired, unemployed or on some other form of benefit), the rest were working or studying;

4) 42% of offenders lived with a partner and/or child;

5) 4% of all offenders had mental health problems;

6) all offenders identified in the study have carefully hidden their activities from relatives;

7) the average recorded duration of the offence ranged from six months to 30 years.

Revenge porn: is a true "online revenge" and consists of the dissemination and sharing on the web of multimedia material with a sexual background, depicting ex-boyfriends or ex-girlfriends, in order to get revenge. The term itself indicates an act of revenge against an ex-partner at the end of a romantic relationship; this revenge consists of the disclosure and subsequent sharing of intimate material and sexual background.

Sextortion: the phenomenon of sexual extortion has developed in parallel with the use of the internet. In particular, it is attributed to a series of behaviours designed to lure a potential victim "by using instant messaging to the point of inducing them to engage in explicit sexual acts at a distance in order to extort money from them"[19] .

This phenomenon has prompted criminologists once again to try to draw up a profile of these offenders in order to know and contrast sextortion. It is noted, first of all, that *the modus operandi* is almost always the same:

1) the first contact between the attacker and the victim takes place on social media, where the two individuals start exchanging general information about their hobbies, hobbies and jobs;

---

[18] *Comprehensive Study on Cybercrime* (2013) New York: United Nations. https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIMESTUDY_210213.pdf, consulted on 1.03.2023.

[19] Ziccardi, G. & Perri, P. (2017). *Tecnologia e diritto, op. cit.* pp. 279-282.

2) subsequently, the conversations between the two subjects shift to sexual topics. The attacker has to gain the victim's trust, even to the point of sending sexual material (photos, videos);

3) once the victim fully trusts the attacker, the attacker moves from a simple chat conversation to the exchange of sexual material to the video call. It is clear how, at this stage, the victim will go even further with equivocal and increasingly sexual behaviour. The attacker will record and save everything, in order to have as much material as possible;

4) the last phase is blackmail: the blackmailer lets the victim know that she has recorded and saved all the material she sent herself. Blackmail consists of undermining the victim's reputation by convincing her that if she does not pay a certain amount of money, the material collected by the attacker will be shared with the victim's friends, family, employers and partner[20] .

3. Criminal profiling in the digital age

Since cybercrime is a new type of criminal activity, criminologists have been studying the causes of cybercrime and the characterisation of criminals and have come up with new theories.

Cybercrime, like traditional crime, consists of action, action - victim/victim - modus operandi - criminal - harm and loss. From a criminological point of view, cybercrime is a socially legal phenomenon, which also consists of specific elements such as an automated data processing system, cyberspace, an individual, criminal action or inaction. A cybercriminal challenges the values developed by society. A cybercrime is committed because of the cybercriminal's excessive need to express himself in a way that is unacceptable to the public. In addition, it should be borne in mind that in different situations a cybercriminal is more or less likely to commit a crime and that there are circumstances that create a high or low level of risk. This is why cybercriminals are the biggest problem on the global network today[21] .

There are two parts to detecting any cybercrime, both technical and legal. Both the legal and technical circumstances of the crime should be identified in the investigation of crimes in these categories, so it is required that the team carrying out the investigation should be made up of forensic scientists, IT specialists, psychologists, etc.

In the view of the criminal investigation, it can be argued that profiling the offender is largely based on a combination of expert and evidence-based knowledge. Perhaps this may make the profiler more susceptible to cognitive bias and faulty decision-making.

---

[20] Greco F., Greco G., *Investigative Techniques in the digital age: Cybercrime and criminal profiling, op. cit.*, p. 8.

[21] Kipane A., *Meaning of profiling of cybercriminals in the security context*, SHS Web of Conferences 68, 01009 (2019), https://doi.org/10.1051/shsconf/20196801009, p. 10.

The profiler can conclude the age, gender or lifestyle of a criminal based on behaviour during crimes.

The profiler also works with databases to find the relationship between the information recorded in statistical reports and the characteristics of the offender, using data on similar offences and offences detected.

Moreover, it is reasonable to point out that cybercriminal profiling is multidisciplinary in nature. The various types of criminal profiling can be broadly divided into two types: geographical profiling and profiling of the personal characteristics of the offender. The latter is what people most commonly associate with the term offender profiling[22].

Using the locations of an offender's crime as a starting point, geographic profiling attempts to predict the area where the offender lives. Geographical profiling is not just considering the significance of a point on a map. Location must be understood in the context of other aspects of crime that can be used in the inference process.[23] Routine activity theory and pattern theory are relevant to geographic profiling. This suggests that offenders will act in an area with which they are familiar.

One of the directions of profiling is the psychological assessment of certain properties and traits. Cybercriminal profiling combines descriptions of an individual's behaviour and qualities that are created without knowing the identity of the criminal.

Criminal profiling involves identifying an unknown offender using several techniques:

1. crime scene analysis;
2. determining the specifics of the offence;
3. characterising the personality of an offender[24].

Crime scene analysis (behaviour configuration) plays a significant role in the research. Scene analysis (also known as crime scene) is the inspection of the scene and the objects contained therein, if it is carried out after receiving information about the crime committed and if there is sufficient reason to believe that a crime has been committed. Its purpose is to find and record traces indicating that a crime has been committed and to restore the mechanism of the crime. In 1925, Moscow State University professor Ivan Yakimov wrote that "the following stages can be distinguished in the restoration of the crime: detection of a crime, obtaining and evaluation of evidence that helps to discover the alleged perpetrator".[25]

---

[22] Bull R., Cooke C., Hatcher R., Woodhams J., Bilby C., Grant T. (2006) *Criminal psychology*: *A Beginner's Guide*, Oneworld Publications, Oxford, England, p. 84.

[23] Canter D., Youngs D. (2008) *Principles of Geographical Offender Profiling*, New York: Toylor & Francis Group, p. 78.

[24] Kocsis R. N., *Criminal Profiling: Principles and Practice*, 2006, ISBN-13: 978-1588296399 ISBN-10: 9781588296399, p. 57.

[25] Jakimov I. (2003) *Kriminalistika. Rukovodstvo po ugolovnoj tehnike i taktike. Novoje izdanije perepechatonoe s izdanii* 1925, Moskva: LeksEst, p. 67.

Nowadays, in the case of cybercrime, the investigator has to recognise a huge amount of evidence in electronic or digital form. The crime scene, unlike the physical scene, contains computer systems or computer networks. A set of conditions and other investigative data can provide information about the personality, motivation and characteristics of the offender.

Given the diversity of approaches to cybercrime and profiling - the forensic aspect, the psychological aspect, the technical aspect - joint work between specialists is essential. Forms of cooperation may vary during the course of the investigation. Professor Laurence Alison of the University of Liverpool has suggested a number of ways in which a psychologist's expertise could help police and facilitate the work they do. It is important to appreciate that the ways in which psychologists can contribute extend beyond the process of profiling offenders[26].

When predicting and profiling an individual's behaviour, the most significant psychological traits are described - a value system, an emotional state and demographic indicators (biological parents, ethnicity, etc.). At the same time, the type of criminal activity (*modus operandi*) and the type of action are analysed, as well as the place of the crime[27]. Modus operandi reflects the nature of the cybercriminal[28].

The reconstruction of a cybercriminal's *modus operandi* is identified from the assumption that criminal behavior is the aggregate of several aspects, which form the criminal's criminal experience, life experience and events that have influenced his life, professional skills and level of intellectual development[29].

Criminal profiling of an unknown cybercriminal involves three steps:

- a forensic scientist collects the crime scene data and passes it on to the profiler;
- the profiler analyses the data and
- offers predictions about the nature of a potential killer.

A cybercriminal profile can be described by including key elements such as:

1. *Personality characteristics/traits* that are specific to a particular person and that predispose a person to commit a cybercrime. Personality traits are defined as a broad individual psychological dimension that describes the interpersonal, stable and common individual differences in an individual's behaviour, thoughts and feelings.

Traits occur in individual activities in different situations and at different

---

[26] Greco F., Greco G., *Investigative Techniques in the digital age: Cybercrime and criminal profiling, op. cit.,* p. 7.

[27] Knight R., Warren J., Reboussin R., Soley B. (1998) *Predicting rapist type from crime scene variables,* „Criminal Justice and Behavior", 25(1), p. 46.

[28] Lieckiewicz J. (2011) *Cybercrime psychology - proposal of an offender psychological profile*. „Problems of Forensic Sciences", Vol. LXXXVII: 239-252, http://www.forensicscience.pl/pfs/87_Lickiewicz.pdf.

[29] Kipane A., *Meaning of profiling of cybercriminals in the security context, op. cit.,* p. 9.

times. There is a high level of legal nihilism among cybercriminals. The cyber offender has deviations in legal consciousness; the distortion of legal consciousness is caused by an individual's inability to live according to legal norms[30].

It is closely related to the increased internal need to risk breaking the law and to such behaviour to obtain personal gain or to obtain material benefit, profit. The impact of the micro-environment is important. For example, family factors that negatively affect personality formation, thus increasing cybercrime include: deficiencies in the child-rearing process (lack of parents, lack of support and understanding), deforming family relationships (neglect of children, etc.), unfavourable families (addiction problems, financial problems and/or social problems).

2. *Criminal professionalism* - means personality traits that contribute to the safe and effective engagement of cybercrime. Includes four mandatory characteristics: specific personal qualities; knowledge and skills; fearlessness, courage and self-confidence; effectiveness and viability of action; committing a crime and achieving a specific goal[31]. For example, some financially motivated cybercriminals generally have two main goals - login details and user identity to gain access to finances through their acquired identity.

3. *Specialist related technical knowledge and skills in dealing with complex software and devices that enable cybercrime*. Last but not least is the education/profession of the cybercriminal's personality. In criminology, there is a view that digital criminals are highly intelligent and self-educated. However, this does not mean that they have a higher education or work in the field of information technology, but have special knowledge in this field. Special knowledge should be understood as a set of skills that a digital criminal uses to commit a cybercrime.

The cybercrime survey concludes that 65% of crimes committed in cyberspace require relatively simple technical skills, 13% - require medium-level technical skills and 22% - complex technical skills. The most common cyber criminals were students. It is generally recognised that the level of education among cyber criminals may be higher than among other categories of criminals[32]. This is primarily due to the fact that in the age of information technology it is easier for the younger generation to master computer programs than for the older generation. But every year, the age of digital criminals decreases due to the fact that many teenagers master computer technologies from an early age and, because of teenage curiosity, enter security systems.

4. *Social or demographic traits, socio-economic status, moral attributes* are of most practical importance. Socio-demographic characteristics of a digital criminal's personality include gender, age, education/profession. Psychological characteristics of a cyber criminal's personality include psychological health and

---

[30] Greco F., Greco G., *Investigative Techniques in the digital age: Cybercrime and criminal profiling, op. cit.,* p. 7.

[31] Tulegenov V. V. (2014) *Kiberprestupnost kak forma virazheniia kriminalnogo professionalizma. Kriminologiia: vchera, segodnia, zavtra*. 2(33).

[32] *Comprehensive Study on Cybercrime, op. cit.,* 2013.

motive. Based on statistical data, the age of digital criminals is mainly between 18-35 years old. An important role is played by the gender of the cyber criminal. According to scientists, the perpetrators of cybercrime are primarily men, while women act as accomplices. However, it is worth noting that every year there is an increasing trend in the number of women committing this type of crime.

5. In criminology, motivation is understood as a set of subjective bases for action, each of which determines the element of motivation and exists in both the conscious and subconscious mind. Motives are developed and formed under the influence of human emotions and feelings. Motives are internal - chosen by the person and external - driven by others. Research has shown that human behaviour is driven by a range of motives - different internal and external factors[33] . The motive is the driving and facilitating function of the activity (internal psychological encouragement), which, in creating the subject of the activity, directs human activity. The motivation of action is formed from a separate motive or motives.

When cybercriminals are discovered, it is of great importance to create a database, which is done through the internet, and especially applications already embedded in computers and smartphones. Using these applications, IT detectives usually gain access to the phone, i.e., phonebook, photos, videos, calls, messages, geolocation and other useful information that can be stored on a computer. Based on all this information, it is eventually possible to form a certain picture of a digital criminal.

Significant evidence can be collected in this way, for example, using geolocation, the location of a digital criminal can be tracked, and the phonebook can serve as a means of searching for possible accomplices and people close to a cybercriminal, who can then be questioned, and a proper criminal profile drawn up.

One of the well-known cases of catching a cybercriminal is the search for Jeremy Hammond, who hacked into the computers of the Strategic Forecasting Ing. intelligence agency, known as Stratfor, which has clients in the U.S. Department of Homeland Security and the Department of Defense. Jeremy Hammond was accused of hacking into the FBI Virtual Academy, the Arizona Department of Public Safety, the Boston Police Association and the Jefferson County, Alabama Sheriff's Office. When the search operations were implemented, his identity was established with the help of a recruited member of a hacking group, who, during questioning, provided all the information. The next step was to gain access to his data, which contained information about the cyber crimes he had committed.

[33] Ksheti N., (2010) *The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives*, New York: Springer, p. 112.

4. Conclusion

Based on all of the above, we can conclude that the role of information technologies has increased in the course of mankind's evolution, which in turn has given rise to cyberspace crimes committed by cyber criminals. An important aspect in the search for and capture of digital criminals is the formation of a criminological portrait, with its individual characteristics, which in turn can be obtained through the use of the internet, which contains and stores information useful to the bodies that are empowered to carry out investigations.

Bibliography

1. Barak, A. (2008) *Psychological Aspects of Cyberspace*. Cambridge: Cambridge University Press.
2. Bull R., Cooke C., Hatcher R., Woodhams J., Bilby C., Grant T. (2006) *Criminal psychology*: *A Beginner's Guide*, Oneworld Publications, Oxford, England.
3. Cadoppi, A., Canestrari, S., Manna, A., & Papa, M. (2019). *Cybercrime*. Vicenza: UTET Giuridica.
4. Canter D., Youngs D. (2008) *Principles of Geographical Offender Profiling*, New York: Toylor & Francis Group.
5. *Comprehensive Study on Cybercrime* (2013) New York: United Nations. https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIMESTUDY_210213.pdf, consulted on 1.03.2023.
6. Dodge, M., Kitchin, R. (2001) *Mapping Cyberspace*. London: Routledge.
7. Fabrizio, L. (2015). *Le nuove forme della devianza.* „Psicologia & Giustizia", 16(1).
8. Faliva, C. (Ed.) (2011). *Tra normalità e rischio. Manuale di psicologia dello sviluppo edell'adolescenza* (Vol. 65). Maggioli Editore.
9. Gallina, M. A. (2009). *Dentro il bullismo. Contributi e proposte socio-educative per la scuola: Contributi e proposte socio-educative per la scuola*. Milano: Franco Angeli.
10. *Global Cyber Risk Perception Survey 2018*. By the Numbers: Global Cyber Risk Perception Survey. Available at: https://www.marshmma.com/blog/2018-cyber-and-data-security-risk-survey -report.
11. Greco F., Greco G., *Investigative Techniques in the digital age: Cybercrime and criminal profiling*, „European Journal of Social Sciences Studies", Vol. 5, Issue 3, 2020, https://oapub. org/soc/index.php/EJSSS/article/view/821/1403.
12. Jakimov I. (2003) *Kriminalistika. Rukovodstvo po ugolovnoj tehnike i taktike*. *Novoje izdanije perepechatonoe s izdanii* 1925, Moskva: LeksEst.
13. Kipane A., *Meaning of profiling of cybercriminals in the security context*, SHS Web of Conferences 68, 01009 (2019), https://doi.org/10.1051/shsconf/20196801009.
14. Knight R., Warren J., Reboussin R., Soley B. (1998) *Predicting rapist type from crime scene variables*, „Criminal Justice and Behavior", 25(1).
15. Kocsis R. N., *Criminal Profiling: Principles and Practice*, 2006, ISBN-13: 978-1588296399 ISBN-10: 9781588296399.

16. Ksheti N., (2010) *The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives*, New York: Springer.
17. Lieckiewicz J. (2011) *Cybercrime psychology - proposal of an offender psychological profile*. „Problems of Forensic Sciences", Vol. LXXXVII, http://www.forensicscience.pl/pfs/ 87_Lickiewicz.pdf.
18. Nicola, H., & Powell, A. (2016). *Sexual Violence in the Digital Age: The Scope and Limits of Criminal Law.* „Social & legal studies", 25(4).
19. Tulegenov V. V. (2014) *Kiberprestupnost kak forma virazheniia kriminalnogo professionalizma. Kriminologiia: vchera, segodnia, zavtra*. 2(33).
20. Tumalavicius V., Ivanciks J., Karpishchenko O. (2016) *Issues of society security: public safety under globalization conditions in Lithuania*, „Journal of Security and Sustainability", Issues 4(9), https://doi.org/10.9770/jssi.2016.5. 4(9).
21. Ziccardi, G. & Perri, P. (2017). *Tecnologia e diritto.* Milano: Giuffré.
22. Zuhri F.A., *The Profile of a Cybercriminal*. Digital Forensic Magazine. Available at: http://digitalforensicsmagazine.com/blogs/wp-content/uploads/2017/05/ The-Profile-of-Cybercriminal.pdf.

Current Standards for Information Security and Privacy

PhD. student **Tiberiu T. BAN**[1]

Abstract

The last ten years have seen a significant more than 10-fold increase in the number of cyber-attacks worldwide, resulting in an extremely large number of computer records being exposed to unauthorised persons. However, studies by independent international organisations reveal that 95% of these attacks exploiting security breaches could have been prevented. This paper reviews the main international and national standards related to the establishment of security policies and data processing procedures that are able to prevent cyber attacks on personal data, especially in the context of the Internet of Things. The analysis is a qualitative one aimed at highlighting best practices through security policies and processing procedures.

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

JEL Classification*:* K24

1. Introductory recital

The years 2020-2022 brought a profound change in the way society perceived technology. The COVID-19 pandemic context imposed massive changes to the way industry, the economy, the justice system[2], the governmental and non-governmental area operated amidst social distancing. Civil society has found solutions in isolation to carry on business remotely through technology.

Not surprisingly, society has become semi-dependent on the information systems it uses, relying more and more on interconnection and remote communication solutions. Thus, information systems have quite naturally become a critically important node in the way almost all areas of business operate at the moment.

In the course of our daily work, with every action we take, from the most mundane gesture, we generate an impressive amount of computer data - some related to our field of activity, but others being personal user data, of how users use technology to interact with the outside world.

In extenso, often this computer-generated data can be a true reflection of the user's preferences, the way they live their lives and the concerns they have. All of this is hidden in the stream of data stored on computing devices, and the

[1] Tiberiu T. Ban - Faculty of Law, Bogdan Voda" University of Cluj-Napoca, Romania, tiberiu.ban@gmail.com.

[2] Tiberiu 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, volume XIX, 2020, pp. 339-345.

more personal this data is, the more likely it will be personal data rather than data related to the user's area of business.

Social distancing and generous periods of various forms of free movement restrictions (lock-downs) around the world have made users more concerned about their own health, reducing the time they spend on mundane activities such as shopping for essentials and food supplies by turning to e-commerce and food delivery apps, making online payments to comply with recommendations to avoid physical contact with possibly infected banknotes.

It is extremely easy to see why personal smart devices have become essential for a user group that has grown significantly[3] over the last 18 months, and this trend is estimated[4] to continue over the next 5 years.

One particular category of increasing interest[5] in this period is voice-controlled devices, such as personal assistants that receive voice commands in natural language, based on a combination of voice recognition technology and then command processing by artificial intelligence systems.

Although overall there have been massive declines in turnover for a multitude of business areas that have scaled back their operations, the Consumer Technology Goods market is up about 2% globally and about 4-5% in the North American area as well as Europe.

The "smart" product category stands out, with spectacular growth of 24% in the European markets[6]. Given that restrictions on movement have forced education to take place online and that many corporations have encouraged their employees to work from home, it is perfectly explainable why 66% of the fastest growing products in the smart entertainment market were smart gadgets.

Of these, **voice-controlled products saw a 61% increase in sales, placing them as the leader in the best-selling devices category in the tech segment for 2020**, outperforming both the Smart Small Appliances segment such as vacuum cleaners (*"Smart Vacuum"*) and the Smart *Health* monitoring devices segment such as fitness wristbands, devices for measuring body temperature, blood pressure, pulse, oximeters with Bluetooth connectivity.

---

[3] According to the *Worldwide Quarterly Smart Home Device Tracker.* Report by International Data Corporation (IDC), USA, the document is available online at https://www.idc.com/getdoc.jsp?containerId=IDC_P37480, accessed 04.03.2023.

[4] See the findings outlined in the press release by International Data Corporation (IDC), USA, *IDC Worldwide Smart Home Devices Market Grew 11.7% in 2021 with Double-Digit Growth Forecast Through 2026, According to IDC*, the document is available online at https://www.idc.com/getdoc.jsp?containerId=prUS49051622, accessed on 03.03.2023.

[5] See press release of Growth from Knowledge (GfK), Germany, *Smart Home: Consumers show growing interest in voice-controlled products*, available online at https://www.gfk.com/hubfs/website/editorial_ui_pdfs/20210318_GfK_PR_Smart_Home_efin.pdf, accessed 04.03.2023.

[6] See the report by ConPolicy Institut fur Verbaucherpolitik, Germany, implementer of studies and recommendations for the European Commission on consumer protection issues, *Digitalization - Increased demand for smart home devices during pandemic*, published on 18.03.2021, document available online at https://www.conpolicy.de/en/news-detail/increased-demand-for-smart-home-devices-during-pandemic/ accessed on 05.03.2023.

Growth from Knowledge's press release[7] presents the study's conclusion that the surge in popularity of these devices and the overall level of consumer demand for these devices such as smart vacuum cleaners, smart smoke detectors, automated lighting systems and even remote-controlled, connectivity-enhanced, automation-grade cooking appliances is evidence of a trend that cannot be denied and will continue in the coming years.

It has thus become clear that **there is an undeniable motivation for consumers to upgrade their devices, opting for semi-automated versions with connectivity to equip their homes, already convinced of the benefits that can be obtained directly and almost instantly**.

The current trend among both individual and corporate consumers is to migrate from previous generations of devices considered "classic" to an innovative generation of devices that are more intuitive to use and, thanks to automation features, adapt to the owner and their lifestyle habits.

In this context, given the very fact that voice-controlled devices are becoming the lifestyle standard for more and more users, these devices collect an incredibly large amount of computer data, much of which is personal data and data that can be used for automated user profiling, useful in predicting marketing preferences but also valuable in the hands of malicious individuals.

Considering that the trend is clearly to extend the user's physical home with a real "virtual home", the need to take measures to ensure the latter's digital security becomes urgent.

All the online activities of the average user generate personal computer data that any marketing agency and cybercriminal can consider a valuable target, which explains why recent years have brought increasing waves of cyber attacks targeting personal data.

There is an increase in the number of attacks at international level, so if in 2013 it was estimated[8] that the number of computer records exposed to unauthorized persons through cyber attacks was around 823 million, compared to the same indicator in 2018 where the number of computer records exposed was already estimated[9] at 5 billion, so an alarming increase of over 600%.

However, reports by the Online Trust Alliance over the past few years

---

[7] See press release of Growth from Knowledge (GfK), Germany, *Smart Home: Consumers show growing interest in voice-controlled products*, available online at https://www.gfk.com/hubfs/website/editorial_ui_pdfs/20210318_GfK_PR_Smart_Home_efin.pdf, accessed 04.03.2023.

[8] *See the 2014 Data Protection & Breaches - Readiness Guide* report, 07 April 2014, produced by the Online Trust Alliance (OTA) under the sponsorship of The Internet Society Foundation, available online at https://www.internetsociety.org/wp-content/uploads/2019/04/2014-cyber-incident-report.pdf, accessed 01.03.2023.

[9] See *2018 Cyber Incident & Breach Trends* Report - *Review and Analysis of 2018 Cyber Incidents and Key Trends to Address*, 09 July 2019, by the Online Trust Alliance (OTA) under the sponsorship of The Internet Society Foundation, available online at https://www.internetsociety.org/wp-content/uploads/2019/07/OTA-Incident-Breach-Trends-Report_2019.pdf, accessed 02.03.2023.

show a unique conclusion, that **between 89% and 95% of cyber attacks and security breaches each year are preventable**, based on data collected and analysed by The Internet Society Foundation and made public by its Geneva, Switzerland office as part of the dissemination of research grants.

This conclusion is at the same time extremely worrying, but it can also point to a direction of study and concern for the future in terms of increasing the level of information security and privacy by putting in place security policies and data processing procedures that are able to effectively lead to the **prevention of cyber attacks targeting personal data in the ecosystem of smart devices - Internet of Things**.

Unquestionably, such an approach must be taken on two levels. On the one hand, action must be taken with regard to the manufacturers of information systems and software and applications, and stricter controls must be imposed on compliance with the security standards for processing personal data, which is already being carried out by the organisations responsible for control at both national and European level[10].

On the other hand, it is necessary for users - both at individual and corporate level - to be aware of the need to comply with information security policies, the need to follow closely the actual procedures for the secure processing of personal data and the need to actually take reasonable technical measures for the security of information systems.

For all these reasons, there is a clear need to analyse these recommendations, standards and general proposals in a comparative way in order to see to what extent they can be implemented in concrete policies and procedures related to Internet of Things ecosystems. They are part of the new wave of disruptive technologies emerging in the area of information and communication technology.

Furthermore, there is a need for an analysis of the types of cyber threats specifically focused on the area of IoT attacks and the vulnerabilities of these types of devices.

The results of this qualitative analysis are the "lessons learned" from the cases analysed, which will allow, as a future research direction, the development of sets of "best practice" policies and procedures, adaptable to concrete cases of implementation, based on personal data risk impact analyses.

In setting this objective, the working assumption already validated[11] by

[10] See for example a significant fine of €746 million given to the Amazon corporation for violating the provisions of the General Data Protection Regulation on how to obtain valid and informed consent prior to the start of the processing of personal data. The fine was issued by the National Commission for Data Protection in Luxembourg as national supervisory authority on 03.03.2023, *apud* https://industryeurope.com/sectors/technology-innovation/amazon-hit-with-record-%E2%82%AC746m-fine-over-data-protection/ accessed on 03.03.2023.

[11] See Vasiu Ioana, *Prevenirea criminalității informatica*, Hamangiu Publishing House, Bucharest, 2006, pp. 122-124, security policies are compared to laws in the legal field, representing a way of abstraction through which concrete rules to be followed can be defined, being described step by

the literature is that properly designed policies and procedures **can satisfactorily prevent** attacks exploiting known vulnerabilities. However, the mere existence of policies and procedures is not enough; it is also necessary to ensure that they are implemented and applied in the actual reality of the organisation.

It is considered[12] that there are two options for verification, namely an automatic one through the implementation of systems to assess compliance with security measures and continuous assessments, carried out by the human factor to the extent that there are objective criteria established.

2. European Union legislative framework

Given the need to process computer data in the context of inter-connectivity between computer systems belonging to different operators, sometimes located in different countries and perhaps continents, the European Union has placed personal data in a special position, considering that they require a level of protection additional to the usual cybersecurity measures.

The General Data Protection Regulation[13] was adopted in order to bring into line the legislative provisions of the Member States of the European Union on the processing of personal data, and to impose a minimum standard of privacy as the norm in these states.

Prior to the adoption of the GDPR Regulation, EU Member States faced a level of fragmentation in the implementation of personal data protection measures, which strongly affected the economic sector[14] , and with the adoption of the GDPR, the EU has tried[15] to regain the trust of civil society that data controllers are able to process the data that customers entrust to them in a professional and responsible manner, especially in the context of new technologies and the transition to a digital economy.

Viewed from a data security and privacy standard perspective, Regulation (EU) 2016/679 - GDPR introduces an extended level of administrative liability[16] as well as state enforcement tools, namely the implementation of fines with visibly increased amount limits compared to

step through procedures. The set of policies and procedures is considered to be essential for the correct implementation of a level of security of information systems that meets the requirements of the actual reality.

[12] See Adam Theodor Octavian, Găbudean Larisa, Rotaru Vasile Victor, *Risk Management. Personal data protection and information security in the organization. Practical guide*, Evrika Publishing, 2019, p. 75.

[13] 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, the official text is available online at https://eur-lex.europa.eu/eli/reg/2016/679/oj, accessed on 01.03.2023.

[14] See Recital 9 of Regulation (EU) 2016/679 - *General Data Protection Regulation.*

[15] See Recitals 7 and 9 of Regulation (EU) 2016/679 - *General Data Protection Regulation.*

[16] See P. Voigt, A. Bussche, *The EU General Data Protection Regulation (GDPR) - A Practical Guide*, Springer Publishing, Switzerland, 2017, p. 87.

previous regulations in EU member states.

The Regulation imposes a number of organisational requirements on all entities processing personal data, regardless of their role as controller, joint controller, processor or third-party recipient.

The division of responsibility between the associated controllers is provided for in Article 26 of the Regulation, and it is necessary to establish exactly where the dividing line is between the responsibility of each of these controllers in the processing, as long as the exposure of personal data to several controllers and possibly the transfer between several IT data management systems does not result in a lower level of protection[17] than if all the personal data had been processed by a single controller. Basically what is required of the associated controllers is to ensure that the splitting of processing between a number of different IT systems, the transfer of data, the processing carried out on the data - all of these are carried out to comparable standards of security and confidentiality of information, whatever technical measures need to be implemented in order to achieve this.

It is extremely important to note that Regulation (EU) 2016/679 - GDPR is the first legislative framework and still at EU level that imposes such privacy standards at the level of legal obligation. Previously Member States were free to draw their own legislation[18] on the security of information systems[19], but now with the adoption of the Regulation, these two requirements are raised to the level of common intra-EU regulation.

NIS Directive[20] **- Directive (EU) 2016/1148** of the European Parliament and of the Council of 06 July 2016 on measures for a high common level of network and information systems security in the Union was incorporated into national law by Law No. 362/2018[21] on ensuring a high common level of network and information systems security in the Union.

We believe it is extremely important that at the heart of the European

[17] See in this respect also Opinion No. WP169 of the Article 29 Data Protection Working Party, 16 February 2010, document available online at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf, accessed on 01.03.2023.

[18] For example, see Law No. 182 of 12 April 2002 on the protection of classified information, published in the Official Gazette No. 248 of 12 April 2002, available at http://legislatie.just.ro/Public/DetaliiDocument/35209, accessed on 18.03.2023.

[19] For example, see Directive of 12.10.2012 on the security accreditation of information and communication systems (CIS) storing, processing or transmitting classified information - INFOSEC13 issued by the Office of the National Register of State Secret Information, published in the Official Gazette no. 716 of 22.10.2012, www.ilegis.ro accessed on 05.03.2023.

[20] Directive (EU) 2016/1148 of the European Parliament and of the Council of 06 July 2016 on measures for a high common level of network and information security across the Union, available at https://eur-lex.europa.eu/eli/dir/2016/1148/oj accessed on 05.03.2023.

[21] Law No. 362 of 28 December 2018 on ensuring a high common level of security of networks and information systems was published in the Official Gazette No. 21 of 9 January 2019 and entered into force on 12 January 2019. The text of this law is available at http://legislatie.just.ro/Public/DetaliiDocument/209670 accessed on 15.03.2023.

Union's digital evolution are undeniably networks and information systems seen as building blocks of the Internet. This gives EU citizens access to services that have become essential, such as the cross-border movement of goods, services and people.

This is why these very systems can become the target of attacks by individuals who seek to cause major disruptions to the functionality of these services which can result in the entire economic activity of a particular sector of industry being prevented and can lead to catastrophic financial losses.

The NIS Directive recalls that there is a worrying trend of increasing security incidents, both in terms of scale and frequency, and all reports issued by other non-governmental bodies on cyber security incidents unfortunately support this argument.

Although there is already a body within the Union whose main purpose is the analysis of cyber security, ENISA - the European Union Agency for Network and Information Security, it is felt that its role can become more prominent in supporting real strategic cooperation between EU Member States.

The security of networks and information systems can become a permanent priority concern, the aim being to ensure that all Member States have at least a minimum capability and an effective and well-defined national strategy to meet security needs.

At the time of the Directive's entry into force in 2018, it was considered that Member States **were not sufficiently prepared** to respond effectively to cyber attacks against systems and networks. This is mainly due to the fact that Member States have varying levels of preparedness to respond to these types of attacks, which automatically means that economic entities but also citizens are unequally protected across the Union.

Another concern is that digital service operators and digital service providers lack a standard of clear security and notification requirements, a risk management culture and a tendency to minimise the level of danger that attacks against computer networks can pose to the macro economy. This is why at the time of 2018 it was considered almost impossible in the already existing legislative context to implement a *comprehensive and effective EU-wide cooperation mechanism*.

This is the context in which the European Union has decided that it is imperative to implement *a global approach that standardises legal requirements across Member States* and requires the creation of minimum response capabilities, planning standards and procedures for the exchange of information and reporting of major security incidents between essential service providers and digital service providers.

Given that some Member States already have a culture of security of information systems and a corporate culture of protecting digital assets by designing and following effective policies and procedures, the NIS Directive introduces *a* desirable *minimum level* of security and response capability, while

allowing Member States the *right to be able to impose through national transposing legislation a higher level of requirements* in network security, as well as their own superior legislative bodies and channels to ensure the *protection of their essential security interests*, to protect public order and safety and to enable the investigation, detection and prosecution of criminal offences.

A particular concern of the Directive is also the regulation of the **online marketplace** for online sales and service provision between traders and buyers which, in the view of the NIS, should offer more than a mere intermediary role between supply and demand but should be a genuine final destination for **concluding online contracts** with traders and not a mere referral to a preferred trader who traditionally offers physical provision of services or delivery of goods.

Also to be considered as an online marketplace will be the category of **online app stores** which allow the user to purchase the desired applications without going to a physical store and have them **delivered exclusively digitally**, without physical delivery of optical media such as DVDs or boxes, manuals or other documents such as technical or operating specifications. These types of app stores already exist and are widely used by users of devices in the Internet of Things ecosystem, such as the app store on Smart TV, the app store that allows adding functionality to fitness wristbands or Smart Watch and of course not least the classic app stores on Android operating systems (e.g. Google Play) or iOS (e.g. Apple App Store). All of these have become priorities that will be covered by the new mandatory cyber protection standards, which is an absolutely welcome option from the EU legislator.

Other segments of the online sphere are now considered to be of major importance such as **cloud-based IT data storage services** that allow users to store and share data within an organisation that is not physically stored inside equipment located at the organisations' business premises.

The real way in which this information is stored in a disorganized manner across the cloud service provider's storage capacity, but is presented to the user as if they had an online hard drive that they can access from any computing device they log into.

This type of service is becoming more and more attractive to both organisations and private users because it allows data to be stored in absolute security, for example through the use of encryption techniques, regular back-up, systems for keeping recent versions of files, protection against ransomware attacks and more.

Practically, by using cloud data storage services, it is theoretically possible to completely avoid data loss in the event of physical damage to the computer system, as it is sufficient to purchase a new computer, laptop or tablet and log in to the cloud data storage and the user can continue working without any interruption.

An important point to note is that the new perspective brought by the NIS Directive concerns the **transfer of responsibility and accountability for**

ensuring the security of networks and information systems to the operators of essential services and digital service operators.

Previously, these risks and how to respond to these potential security problems were considered to be the sole responsibility of organisational or individual operators, which automatically made it almost impossible to assess the degree of compliance and enforcement of these measures.

The NIS Directive is also concerned with the protection of personal data, as it is expressly stated in Recital 63 that there are extremely frequent situations where **security incidents on information systems and computer networks can lead to the exposure and compromise of personal data**.

This practically justifies the need for cooperation between national reporting and response bodies for security incidents with those for monitoring and reporting security breaches of personal data.

With regard to the way in which the processing of personal data is protected and regulated, the NIS Directive states that it is carried out under Directive 95/46/EC[22] and that the processing of personal data by the Union institutions and bodies is carried out under Regulation (EC) No. 45/2001[23], to which Decision No. 1247/2002/EC[24] also applies.

Of course, in the meantime these regulatory rules have been repealed, which naturally makes the NIS Directive refer to the new regulations updating the aforementioned acts, namely Regulation (EU) 2016/679[25] (GDPR) and Regulation (EU) 2018/1725[26] which establish new standards and regulations updated to current requirements.

Another important point that Directive (EU) 2016/1148 establishes as essential concerns the need for each Member State to define and legislate a

[22] 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, available at https://eur-lex.europa.eu/eli/dir/1995/46/oj, accessed on 15.03.2023.

[23] Regulation (EC) No. 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, repealed, available at https://eur-lex.europa.eu/eli/reg/2001/45/oj, accessed on 18.03.2023.

[24] Decision No. 1247/2002/EC of the European Parliament, of the Council and of the Commission of 1 July 2002 on the regulations and general conditions governing the performance of the European Data Protection Supervisor's duties, repealed, available at https://eur-lex.europa.eu/eli/dec/2002/1247/oj, accessed on 18.03.2023.

[25] 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, available at https://eur-lex.europa.eu/eli/reg/2016/679/oj accessed on 10.03.2023.

[26] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of individuals 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, available at https://eur-lex.europa.eu/eli/reg/2018/1725/oj, accessed on 20.03.2023.

national strategy on the security of networks and information systems, which may go beyond the minimum standards defined by this Directive and for which it is possible and even recommended that Member States seek assistance from the European body ENISA[27] for the concrete development of these strategies that would specifically regulate[28] a response mechanism[29] in case of incidents.

ENISA as an Agency established under the direct supervision of the European Union enjoys Community prerogatives and European legislative support, its tasks as well as the concrete functioning and elements of jurisdiction being regulated by Regulation (EC) No. 460/2004[30], Regulation (EU) No. 526/2013[31] and Regulation (EU) No. 2019/881[32].

ENISA as the Community Agency has a direct role to report on how each of the Member States has agreed to comply[33] but also to provide best practice responses[34] on security incidents.

They must be communicated no later than 3 months after their adoption so that they can be disseminated at Community level, possibly if necessary keeping confidential specific provisions directly related to national security issues which by their nature cannot be made public.

---

[27] See ENISA Guidance - *Strategies for incident response and cyber crisis cooperation*, European Union Agency for Cybersecurity (ENISA), August 2016, available at https://www.enisa.europa.eu/publications/strategies-for-incident-response-and-cyber-crisis-cooperation/at_download/fullReport accessed on 15.03.2023.

[28] See ENISA press statement - *EU Boost against cyberattacks: EU Agency for Cybersecurity welcomes proposal for the Joint Cyber Unit*, European Agency for Cybersecurity (ENISA), June 2021, available at https://www.enisa.europa.eu/news/enisa-news/eu-boost-against-cyberattacks-eu-agen cy-for-cybersecurity-welcomes-proposal-for-the-joint-cyber-unit accessed 18.03.2023.

[29] See ENISA Guide - *EU Member States incident response development status report*, European Union Agency for Cybersecurity (ENISA), November 2019, available at https://www.enisa.europa.eu/publications/eu-ms-incident-response-development-status-report/at_download/fullReport, accessed on 19.03.2023.

[30] Regulation (EC) No. 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency, repealed, available at https://eur-lex.europa.eu/eli/reg/2004/460/2011-06-25 accessed on 15.03.2023.

[31] Regulation (EU) No. 526/2013 of the Parliament and of the Council of 21 May 2013 on the European Union Network and Information Security Agency (ENISA), available at https://eur-lex.europa.eu/eli/reg/2013/526/oj accessed on 14.03.2023.

[32] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (European Union Cybersecurity Agency) and on cyber security certification for information and communication technology, available at https://eur-lex.europa.eu/eli/reg/2019/881/oj accessed on 14.03.2023.

[33] See ENISA Guide - Report on Cyber Crisis Cooperation and Management, European Union Agency for Cybersecurity (ENISA), November 2014 available at https://www.enisa.europa.eu/publications/ccc-study/at_download/fullReport accessed on 21.03.2023.

[34] See ENISA Guidance - *Common practices of EU-level crisis management and applicability to the cyber crisis*, European Union Agency for Cybersecurity (ENISA), April 2016, available at https://www.enisa.europa.eu/publications/eu-level-crisis-man/at_download/fullReport, accessed 19.03.2023.

All these efforts are coupled with initiatives[35] at EU level on new mechanisms[36] for inter-state cooperation that aim to provide concrete and sustainable responses to the new types of cyber attacks launched in recent years.

At the end of 2020, the European Union presented a new EU Cyber Security Strategy[37], on which occasion the European Commission presented a legislative proposal to address both cyber resilience and physical resilience of critical entities and networks. Compared to the text of the NIS Directive (EU) 2016/1148, the new revised Directive (NIS2) aims to address and provide up-to-date solutions to the following vulnerabilities that are said to prevent the NIS Directive from reaching its full potential

In 2016, the European Union regulated Directive (EU) 2016/679 respectively the General Data Protection Regulation (GDPR), and with it Directive (EU) 2016/680[38] was issued as an essential step of the reform that was intended to be implemented in the area of personal data processing, being implemented in national legislation by Law no. 363/2018.[39]

This Directive repealing and updating in the context of the new modern perspective[40] to protect the processing of personal data repeals Framework

[35] See ENISA press statement - *Blue OLEx 2020: The European Union Members State launch the Cyber Crisis Liaison Organisation Network (CyCLONe)*, available at https://www.enisa.europa.eu/news/enisa-news/blue-olex-2020-the-european-union-member-states-launch-the-cyber-crisis-liaison-organisation-network-cyclone, accessed on 10.03.2023.

[36] Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cyber security incidents and crises, available at https://eur-lex.europa.eu/eli/reco/2017/1584/oj accessed on 23.03.2023.

[37] *European Union Cyber Security Strategy for the Digital Decade*, 16 December 2020 proposed by the European Commission and the High Representatives of the Union for Foreign Affairs and Security Policy, Joint Communication to the European Parliament and The Council, JOIN(2020) 18 final, Brussels, available at https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0 accessed on 29.03.2023.

[38] Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, available at https://eur-lex.europa.eu/eli/dir/2016/680/oj, accessed on 19.03.2023.

[39] Law No. 363 of 28 December 2018 on the protection of individuals with regard to the processing of personal data by competent authorities for the purpose of preventing, detecting, investigating, prosecuting and combating criminal offences or the execution of penalties, educational and security measures, and on the free movement of such data, published in the Official Gazette No. 13 of 07 January 2019, available at http://legislatie.just.ro/Public/DetaliiDocument/209627 accessed on 25. 03.2023.

[40] See Report *Directive 2016/680 Personal Data in Law Enforcement*, M. Leiser, ELaw - Center for Law and Digital Technologies Lieden University, conducted in the framework of the European financial support programmes for justice (2014-2020) INFORM - Introduction of the Data Protection Reform to the Judicial System, available at https://www.universiteit leiden.nl/binaries/content/assets/rechtsgeleerdheid/instituut-voor-metajuridica/presentation-leiser-inform.pdf, accessed on 18.03.2023.

Decision 2008/977/JHA[41]. The main stated purpose is to protect individuals in the processing of personal data by competent authorities for the purpose of the enforcement of justice (LED - Law Enforcement Directive) which is a crucial step forward in establishing an EU-wide personal data protection regime.

3. Romania's legislative framework

Fully respecting the tasks laid down by Directive (EU) 2016/1148, Law no. 362 of 28 December 2018[42] on ensuring a high common level of network and information systems security is regulated in order to transpose into Romanian national law the main points laid down in the NIS Directive.

These new legislative regulations are aimed at ensuring the security of networks and information systems that serve key activities for sectors of the economy and society, such as digital infrastructure, energy, transport, health, digital technologies and others.

From an organisational point of view, Law no. 362/2018 establishes the **competent authority at national level for network and information systems security**, a requirement imposed by Directive (EU) 2016/1148, and invests the **National Cyber Security Incident Response Centre (CERT-RO)** as the national authority, which will cooperate in the performance of its concrete tasks, as appropriate, with a number of public institutions such as the Romanian Intelligence Service, the Ministry of National Defence, the Ministry of Internal Affairs, ORNISS, SIE, STS, SPP and others.

Law No. 190/2018[43] is basically the law transposing Directive (EU) 2016/679 GDPR into national law, and clear and adapted regulation by the national legislator is essential. Also, with the entry into force of Law No. 190/2018, an additional set of cumulative appropriate safeguards[44] are provided for the processing of the national identification number taking into account the legitimate interests of the controller.

The new legislative provisions[45] introduced by Law No. 190/2018 relate in particular to genetic, biometric or health data, processing with the declared

[41] Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, repealed, available at https://eur-lex.europa.eu/eli/dec_framw/2008/977/oj, accessed on 19.03.2023.

[42] Law No. 362/2018 on ensuring a high common level of security of networks and information systems, published in the Official Gazette No. 21 of 09 January 2019, available at http://legislatie. just.ro/Public/DetaliiDocument/209670 accessed on 24.03.2023.

[43] Law No. 190 of 18 July 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, published in the Official Gazette No. 651 of 26 July 2018, available at http://legislatie.just.ro/Public/DetaliiDocument/2031 51 accessed on 16.03.2023.

[44] See Article 4 of Law No. 190/2018.

[45] See Article 3 of Law No. 190/2018.

purpose of automated decision-making or based on automated profiling.

The competence according to Article 43 of Regulation (EU) 2016/679 Article 43 has been granted[46] to the Romanian Accreditation Association - RENAR, and accreditations will be performed in accordance with EN-ISO/IEC 17065 or other additional requirements to be established by the national authority (ANSPDCP).

Law No. 365/2002[47] was one of the first efforts made by Romania to implement some of the definitions and regulations specified in the 2001 Budapest Convention on Cybercrime[48], such as information society service, electronic means, service provider, electronic payment instrument, electronic money, remote access payment and others. There are two key aspects regulated by Law No. 365/2002, namely the provision of information society services and the regulation of contracts concluded by electronic means.

It also regulates the concrete conditions of service provision and the strict manner in which the provider is allowed to make commercial communications to recipients, and for the first time expressly establishes the need for express consent (anti-spam policy).

A novel aspect introduced in the Romanian legal paradigm is represented by the **regulation of contracts concluded by electronic means**, which now receive legal recognition, establishing a series of principles, among which we expressly mention. The proof of the conclusion of contracts by electronic means and of the obligations resulting from the assumption of such contracts is subject to the provisions of common law on evidence (from the Code of Civil Procedure[49] and the Code of Criminal Procedure[50]) as well as to the provisions of the Electronic Signature Law No. 455/2001.[51]

An essential aspect regulated by Law no. 365/2002 concerns the **Conditions for keeping or presenting information**, being the first piece of legislation that imposes special conditions for ensuring information security, especially given the non-repudiation nature of contracts concluded under

[46] See Article 11(1) of Law No. 190/2018.

[47] Law No. 365 of 7 June 2002 on electronic commerce, published in the Official Gazette No 959 of 29 November 2006, available at http://legislatie.just.ro/Public/DetaliiDocument/37075, accessed on 17.03.2023.

[48] European Convention on Cybercrime, Budapest, 2011, available at https://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf, accessed on 16.03.2023.

[49] Law No. 134 of 01 July 2010 - Code of Civil Procedure updated to date, republished in the Official Gazette No. 247 of 10 April 2015, available at http://legislatie.just.ro/Public/DetaliiDocument/140271 accessed on 10.03.2023.

[50] Law No. 135 of 1 July 2010 - Code of Criminal Procedure, published in the Official Gazette No. 486 of 15 July 2010, available at http://legislatie.just.ro/Public/DetaliiDocument/120611, accessed on 10.03.2023.

[51] Law No. 455 of 18 July 2001 on electronic signature, published in the Official Gazette No. 429 of 31 July 2001, available at http://legislatie.just.ro/Public/DetaliiDocumentAfis/29903, accessed on 10.03.2023.

electronic signature.

The legal requirements that the information be presented or preserved in its original form are deemed to be met if three conditions are cumulatively met, namely: that there is a *guarantee of the integrity of the information*, ensured by compliance with national standards in the field, from the moment it was generated, that the message is signed using an *extended electronic signature* of the issuer and that the information has the possibility to be *immediately provided* and presented on request.

Decision no. 271/203[52] of the Romanian Government for the approval of Romania's Cyber Security Strategy and the National Action Plan for the implementation of the National Cyber Security System, taking into account the fact that cyberspace is characterized by the existence of almost always foreign elements that generate both opportunities for knowledge and risk situations for the functioning of information systems and information networks, both at individual and organizational level or even at state level.

This Government Decision emphasises that an increase in the capacity to fight cybercrime at national, European and international level implies, among other things:

- increased cooperation and coordination between units responsible for fighting cybercrime, other authorities and experts within the European Union;
- develop a coherent EU regulatory framework on the fight against cybercrime, in coordination with Member States as well as relevant European and international authorities;
- increase awareness of the costs and dangers of cybercrime;

In order to respond to these needs, the Romanian State regulates Romania's Cyber Security Strategy, establishing the following **action directions**[53]: establishment and operationalization of a **national cyber security system**;

This National Cyber Security System (NSCS) is intended to be a general framework for cooperation between public authorities and institutions, with knowledge components, prevention components and cooperation and coordination components as well as counteraction components, with a proactive approach being coordinated at the strategic level by the Supreme Council of National Defence (CSAT) which approves the Security Strategy and constantly adapts it to current needs.

It is expressly regulated in relation to the CSAT Component concretely these tasks are taken over by the Cyber Security Operational Council (COSC)

[52] Government Decision no. 271/2013 approving Romania's Cyber Security Strategy and the National Action Plan for the implementation of the National Cyber Security System was published in the Official Gazette, Part I no. 296 of 23.05.2013 and is available at https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/StrategiaDeSecuritateCiberneticaARomaniei.pdf, accessed on 26.03.2023.

[53] See point III of Romania's Cyber Security Strategy.

which brings together members from MApN, MAI, MAE, MSI, STS, SIE, SPP, ORNISS and the CSAT Secretary. Liaison with the executive is carried out at the level of the Ministry for the Information Society (now the Ministry of Communications and Information Society).

Completing and harmonising the national legislative framework in this area, including the establishment and application of **minimum security requirements for** national **cyber infrastructures**, as well as *developing cooperation between the public and private sectors*, including by stimulating the mutual exchange of information on threats and vulnerabilities as well as on cyber incidents and attacks;

The objectives of this aspect are[54] cooperation at all levels, increasing the level of protection of cyber infrastructures by linking measures taken with available joint public and private sector resources, sharing information on specific threats, vulnerabilities and risks, developing early warning and response capabilities to cyber incidents and attacks, developing educational and research programmes in the field and **developing an organisational security culture** that includes a joint response to major cyber attacks.

It is emphasised that there is a need to implement minimum procedural and security standards for cyber infrastructures at national level to underpin effective protection against cyber attacks and limit the risks of potentially significant incidents.

Prior to the uniform regulations at EU level, prior to Romania's accession to the European Union, Romania acceded to a series of international treaties by which it assumed the fight against cybercrime and the establishment of legislative guarantees regarding the respect of individuals' rights in the processing of personal data.

Thus, in addition to Law No. 677/2001, Romania issued Law No. 506/2004[55] which regulates essential aspects adapted to the context of electronic communications and trying to minimise the risks of unauthorised disclosure of personal data.

An important aspect relates to the *security of the processing of personal data*, thus the provider of an electronic communications service to the public is obliged[56] to take appropriate technical and organisational measures to ensure the security of the processing of personal data, in compliance with express conditions, under the supervision of the ANSPDCP.

Law No. 504/2004 also clarifies[57] issues related to ensuring *the*

[54] See Section V of Romania's Cyber Security Strategy.
[55] Law No. 504 of 17 November 2004 on the processing of personal data and protection of privacy in the electronic communications sector, published in the Official Gazette No. 1101 of 25 November 2004, available online at http://legislatie.just.ro/Public/DetaliiDocument/56973 accessed on 10.03.2023.
[56] See Article 3(1)-(3) of Law no. 504/2004.
[57] See Article 4 of Law no. 504/2004.

confidentiality of communications transmitted over public electronic communications networks and electronic communications services to the public, as well as the confidentiality of related traffic data. Thus, it is expressly stated that listening, recording, storing or any other form of *interception or surveillance of communications and traffic data* is prohibited as a matter of principle.

Law 504/2004 also brings important regulations on important[58] services such as *automatic call forwarding, subscriber registers* and the regulation of *unsolicited communications*, commonly known as "spam" or "mass marketing".

The National Supervisory Authority for Personal Data Processing is established under Regulation (EU) 2016/679 of GDPR as the national authority responsible for monitoring the application of this Regulation in order to protect the fundamental rights and freedoms of natural persons with regard to processing and to facilitate the free movement of personal data within the Union.

Like each of the national authorities of the Member States, the NDPSCA enjoys full independence in the performance of its tasks and in the exercise of its powers and remains independent from any external influence.

The National Supervisory Authority for Personal Data Processing in the performance of the above mentioned duties, issued **Decision No. 128/2018**[59] to regulate a uniform way in which personal data controllers within the meaning of Regulation (EU) 2016/679 of GDPR must fulfil their obligation to notify the Authority if any breach of cybersecurity has occurred.

The ANSPDCP has also issued **Decision No. 133/2018**[60] establishing a uniform national procedure - in compliance with all the legal provisions specified in the above-mentioned normative acts - for receiving and resolving complaints addressed by the individuals concerned to the Authority in the event of a violation of their personal data rights.

Decision 161/2018[61] of the National Authority for the Supervision of Personal Data Processing concerns the regulation of a single procedure for carrying out investigations into the occurrence of a security incident that has been reported in accordance with the procedure specified above in Decision No. 128/2018 to the national authority.

---

[58] See Art. 10, Art. 11 and Art. 12 of Law no. 504/2004.

[59] Decision No. 128 of 22 June 2018 of the National Supervisory Authority for Personal Data Processing on the approval of the standard personal data breach notification form in accordance with the provisions of Regulation (EU) 2016/679 GDPR published in the Official Gazette No. 557 of 03 July 2018, document available online at http://legislatie.just.ro/Public/DetaliiDocument/202190 accessed on 17.03.2023.

[60] Decision No. 133 of 3 July 2018 of the National Supervisory Authority for Personal Data Processing on the approval of the procedure for receiving and resolving complaints, published in the Official Gazette No 600 of 13 July 2018, available online at http://legislatie.just.ro/Public/DetaliiDocumentAfis/202633, accessed on 18.03.2023.

[61] Decision No. 161 of 9 October 2018 of the National Supervisory Authority for Personal Data Processing on the approval of the Procedure for conducting investigations, published in the Official Gazette No. 892 of 23 October 2018, available at http://legislatie.just.ro/Public/DetaliiDocumentAfis/206155 accessed on 17.03.2023.

Decision 174/2018[62] of the ANSPDCP brings an absolutely necessary regulation, given that Regulation (EU) 2016/679 requires[63] that where necessary, the controller will carry out an analysis to assess whether the processing takes place in accordance with the data protection impact assessment, especially in the situation where a change in the risk posed by the concrete processing operation occurs. Thus, the controller is obliged to carry out the Data Protection Impact Assessment (DPIA) in some situations considered to present a high level of risk to the security and confidentiality of the personal data being processed.

4. Conclusions and best practices

The main elements constituting good practice both at cross-border, state and organisational level or even at individual level, depending on the case, most of these have the rank of principles:

- a *global and unified level of response between states* is needed, we need to be able to anticipate exactly what each state's ability to respond and be resilient to attacks that can have a significant disruptive impact;

- we need to raise the *security of information systems and networks and the* way information systems are interconnected, both in terms of the equipment used and the algorithms and software tools used, to the *level of a national priority;*

- it is a priority to provide *both legislative and practical cyber protection to protect online services*, online app stores, cloud computing data storage services;

- it is imperative that *every state develops a response and resilience capacity to cyber attacks*;

- it is absolutely necessary to have at state level, at organisational level but also at individual level where we are not referring to home users but to small and micro enterprises (as defined by the new revised NIS Directive2) *response capacity, policies and procedures to ensure resilience*, reporting and adequate response to information security attacks that are designed to compromise the security of information systems and information networks;

- it is a priority for *digital service operators and operators of essential services to take on the task of ensuring the security of the IT infrastructure*, without leaving this responsibility to the home or organisational user who has neither a culture of information and information systems security nor the know-how and financial resources to cover the vulnerabilities that often arrive on the supply chain, the responsibility not being clearly established in this situation;

- we need to develop *much closer cross-border and international*

[62] Decision No. 174 of 18 October 2018 of the National Supervisory Authority for Personal Data Processing on the list of operations for which it is mandatory to carry out the personal data protection impact assessment, published in the Official Gazette No. 919 of 31 October 2018, available at http://legislatie.just.ro/Public/DetaliiDocument/206331 accessed on 19.03.2023.

[63] See Article 35 of Regulation (EU) 2016/679.

cooperation mechanisms on cyber security and attack prevention;

- **a national strategy on network and information systems security** is absolutely necessary, it must clearly define who the responsible actors are, the transparent way in which they communicate incidents and the individual response mode established for each situation, as well as the response scenarios (in a multiple use case scenario analysis) in the event of a significantly disruptive incident;

The most important conclusion, supported both by Romania's Cyber Security Strategy refers to the implementation of the National Cyber Security System - it should be flexible, adaptive, have capabilities for identification, anticipation, resources and operational procedures for prevention, response and counteraction, as well as tools for documenting and sanctioning perpetrators of cyber attacks.

Romania's Cyber Security Strategy as well as all regulations at European level recognise that at both individual and organisational level, **it is also necessary to implement concrete** and effective **security policies and procedures**, designed on the same considerations of the NSCS but adapted at a micro level.

From the whole analysis of all the elements of legislation as well as the guidelines covered, the starting hypothesis of the main study contained in the thesis is validated, namely that **security policies are necessary and effective. They can protect and prevent cyber attacks. A minimum level of security is required to be implemented.**

Bibliography

1. Ban, Tiberiu 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, volume XIX, C.H.Beck Publishing House, Bucharest.
2. ConPolicy Institut fur Verbaucherpolitik, Germany, implementer of studies and recommendations for the European Commission on consumer protection issues, *Digitalization - Increased demand for smart home devices during pandemic*, published on 18.03.2021.
3. Cyber Crisis Cooperation and Management, European Union Agency for Cybersecurity (ENISA), November 2014.
4. ENISA - *Blue OLEx 2020: The European Union Members State launch the Cyber Crisis Liaison Organisation Network (CyCLONe).*
5. ENISA - *EU Boost against cyberattacks: EU Agency for Cybersecurity welcomes proposal for the Joint Cyber Unit*, European Agency for Cybersecurity (ENISA), June 2021.
6. ENISA Guide - *Common practices of EU-level crisis management and applicability to the cyber crisis*, European Union Agency for Cybersecurity (ENISA), April 2016;
7. ENISA Guide - *EU Member States incident response development status report*, European Union Agency for Cybersecurity (ENISA), November 2019.

8. ENISA Guide - *Strategies for incident response and cyber crisis cooperation*, European Union Agency for Cybersecurity (ENISA), August 2016.
9. Growth from Knowledge (GfK), Germany, *Smart Home: Consumers show growing interest in voice-controlled products.*
10. International Data Corporation (IDC), USA, *IDC Worldwide Smart Home Devices Market Grew 11.7% in 2021 with Double-Digit Growth Forecast Through 2026, According to IDC.*
11. Octavian, Adam Theodor; Găbudean, Larisa; Rotaru, Vasile Victor, *Risk Management. Personal data protection and information security in the organization. Practical guide*, Evrika Publishing, 2019.
12. Opinion No. WP169 of the Article 29 Data Protection Working Party, 16 February 2010.
13. Report *Directive 2016/680 Personal Data in Law Enforcement*, M. Leiser, ELaw - Center for Law and Digital Technologies Lieden University, conducted in the framework of the European financial support programmes for justice (2014-2020) INFORM - Introduction of the Data Protection Reform to the Judicial System.
14. The *2014 Data Protection & Breaches - Readiness Guide* report, 07 April 2014, by the Online Trust Alliance (OTA) under the sponsorship of The Internet Society Foundation.
15. The *2018 Cyber Incident & Breach Trends* Report - *Review and Analysis of 2018 Cyber Incidents and Key Trends to Address*, 09 July 2019, by the Online Trust Alliance (OTA) under the sponsorship of The Internet Society Foundation.
16. The *Worldwide Quarterly Smart Home Device Tracker* report, conducted by International Data Corporation (IDC), USA.
17. Vasiu, Ioana, *Preventing computer crime*, Hamangiu Publishing House, Bucharest, 2006.
18. Voigt, P., Bussche, A., *The EU General Data Protection Regulation (GDPR) - A Practical Guide*, Springer Publishing, Switzerland, 2017.

ARTIFICIAL INTELLIGENCE THROUGH THE LENS OF TODAY'S LAW

New Technologies are Shaping Arbitral Proceedings

PhD. student **Andrada-Laura TARMIGAN**[1]

Abstract

The aim of this article is to analyze the impact and changes brought by new technologies in international arbitration procedures, what are the prospects for the future development of these tools in a fast-paced environment and how participants are expected to adapt in these off-the chain disputes. The results obtained through the comparative method are relevant for professionals involved in international arbitration. Furthermore, we will analyze the potential disputes arising out of the technology itself and how are these technologies going to shape decision making on a short, medium and long term. We will refer to the manner in which the leading institutions in arbitration and dispute resolution services position themselves. Lastly, we will refer to the potential issues of the parties' acceptance of the "digital justice" and the prospect of autonomous enforceable arbitral awards.

Keywords: *technology law, international arbitration, innovation, digital justice.*

JEL Classification*:* K33

1. Introduction

In this era of globalization and technological absorption, improvement tools have been introduced in arbitration, which anticipate notable "*disruptions and opportunities.*"[2]

This paper will analyze the impact of emerging technologies on international arbitration proceedings on short and medium term. Firstly, we will discuss how stakeholders are going to use artificial intelligence ("*AI"), either* as support for increasing speed and efficiency or even as a decision-making tool.

Secondly, we will approach the subject of new platforms used by different arbitration institutions and touch upon others matters of concern, such as increasing sustainability of dispute resolution or the obstacles that are technologies could create for parties involved in international arbitration proceedings.

---

[1] Andrada-Laura Tarmigan - Doctoral School of Law, Bucharest University of Economic Studies, Romania, andrada.tarmigan@drept.ase.ro.

[2] Kiran Nasir Gore, *International Disputes and Digital Disruption, in Conversation with Claudia Salomon, President of the ICC International Court of Arbitration*, 2022, "Kluwer Arbitration Blog", the document is available online at https://arbitrationblog. kluwerarbitration.com/ 2022/09/ 30/international-law-talk-podcast-and-arbitration-international-disputes-and-digital-disruption-in-conversation-with-claudia-salomon-president-of-the-icc-international-court-of-arbitration/ (last accessed 14 April 2023).

2. Use of technology in international arbitration

New technologies such as blockchain or machine learning have entered the world of dispute resolution and are simplifying the procedures and cutting costs. International arbitration seems to be the perfect fit, since it highly promotes confidentiality, flexibility and a straightforward enforcement procedure. Moreover, new technologies will generate disputes and arbitration seems best suited for resolving them.[3]

Videoconferencing, multimedia presentations, real-time electronic transcripts, cloud-based storage, artificial intelligence *("AI")* (data analytics, technology-assisted document review) are tools that are already used in arbitral proceedings[4].

Virtual hearings are the most popular, having acknowledged advantages such as cost-efficiency, flexibility, greater availability of dates for hearings, more sustainable. They made international arbitration available for more users and these advantages generally overcome the inevitable flaws: difficulty of accommodating multiple time zones, difficulty of assessing witnesses' credibility, screen fatigue etc.[5]

Confidentiality is one of the main obstacles for new technologies in the context of arbitration. For example, using data analytics tools[6] or the Internet of things *("IoT")*[7] in arbitration could be less efficient compared to national courts, since there are not as many public databases with arbitral awards for access.[8]

Machine-learning tools are used for automated fact checking in submitted documents, in cross-examination or in witness's testimony and alert counsels

[3] Gauthier Vannieuwenhuyse, *Arbitration and New Technologies: Mutual Benefits*, Journal of International Arbitration, 2018, Issue 1, pp. 119-129, https://kluwerlawonline.com/journal article/Journal+of+International+Arbitration/35.1/JOIA2018005.

[4] Łągiewska, M., *Chapter 11 The New Landscape of Arbitration in View of Digitalization*, in Shaheeza Lalani and Steven G. Shapiro (eds.), *The Impact of COVID on International Disputes*. Leiden, The Netherlands: Brill | Nijhoff, 2022, pp. 208–217doi: https://doi.org/10.1163/ 97890045 14836_013.

[5] Use of Technology: The Virtual Reality, White and Case, 2021, the document is available online at https://www.whitecase.com/sites/default/files/2021-05/quml-use-technology.pdf (last accessed 17 April 2023).

[6] For example, Context, a tool developed by Lexis Nexis, that can analyze the likelihood of winning or losing a motion.

[7] Internet of things technology is essentially the communication of data between one device or platform to another over the internet or other communications networks.

[8] Nasser Ali Khasawneh, Maria Mazzawi, Ricardo Christie, *Arbitration and the Advent of New Technologies*, "Global Arbitration Review", the document is available online at https://global arbitrationreview.com/guide/the-guide-telecoms-arbitrations/first-edition/article/arbitration-and-the-advent-of-new-technologies (last accessed 10 April 2023).

and the arbitral tribunal[9] to the possible inconsistencies.[10] Practitioners could use similar natural language processing *("NLP")* systems when generating the narrative of events for the tribunal.[11]

Other relatively recent tools tested in arbitration are the metaverse, with holograms for participants or with a mix of video participants and virtual reality avatars. Tech-enthusiasts expect the metaverse and smart contracts to lead to autonomous arbitration and self-executing arbitral agreements.

Moreover, several soft law instruments promoting fairness, transparency and secure use of technology emerged. For example, some entities drafted rules for the resolution of digital asset disputes[12].

The UK Jurisdiction Taskforce *("UKJT")* issued the United Kingdom's first Digital Dispute Resolution Rules *("DDRR").* The *DDRR* may be included in any contract by stating, "*Any dispute shall be resolved in accordance with UKJT Digital Dispute Resolution Rules".*

Another notable feature consists of the fact that, if not chosen by the parties, the DDRR allows the arbitrators to be appointed by the Society for Computers and Law *("SCL"*), *which* also administers the arbitration.

Parties will provide evidence of their identity to the reasonable satisfaction of the tribunal, who is obliged not to disclose the identification details unless disclosure is "necessary for the fair resolution of the dispute, enforcement, protection of the tribunal's own interests, or if required by law, regulation or court order". Furthermore, rule no. 15 permits the tribunal to provide the award in an anonymized form.[13]

Another important step in this direction was the CIArb's[14] *Framework Guideline on the Use of Technology in International Arbitration*, which seeks to introduce a number of guiding principles on the use of technology in arbitration.

---

[9] For example "*Squash"* is an automated real-time fact-checker, developed by Politifact and Duke University.

[10] Leonardo F. Souza-McMurtrie, *Arbitration Tech Toolbox: Will ChatGPT Change International Arbitration as We Know It?*, "Kluwer Arbitration Blog", 2023, the document is available online at https://arbitrationblog.kluwerarbitration.com/2023/02/26/arbitration-tech-toolbox-will-chatgpt-change-international-arbitration-as-we-know-it/ (last accessed 2 April 2023).

[11] Robert Bradshaw, *Arbitration Tech Toolbox: Cross Examination? There's an App for That*, "Kluwer Arbitration Blog", 2023, the document is available online at https://arbitrationblog.kluwerarbitration.com/2023/02/06/arbitration-tech-toolbox-cross-examination-theres-an-app-for-that/ (last accessed 9 April 2023).

[12] Digital Dispute Resolution Rules ("*DDRR"),* created by the UK Jurisdiction Taskforce; JAMS Rules Governing Disputes Arising out of Smart Contracts; tech dispute resolution mechanisms, such as Kleros and Codelegit.

[13] Peter Smith, Arbitration Tech Toolbox: Arbitrating Digital Asset Disputes, "Kluwer Arbitration Blog", 2022, the documents is available online at https://arbitrationblog.kluwerarbitration.com/2022/04/27/arbitration-tech-toolbox-arbitrating-digital-asset-disputes/ (last accessed 13 April 2023).

[14] Chartered Institute of Arbitrators.

Another AI tool suitable for complex arbitration cases, especially for presenting expert evidence, refers to data visualization. Data visualization tools can assist in presenting the data and damages models by consolidating various Excel spreadsheets and calculations into a single platform, allowing experts to incorporate more sophisticated charting and presentation functions.[15]

3. Digital justice

New technologies have the ability to improve speed and quality of a decision, but accepting digital justice could be difficult for unsatisfied parties.

Parties are accustomed to select trusted arbitrators, which makes the acceptance of the finality of the award easier. Moreover, the involvement of national courts in the action for annulment or the procedures for the recognition and enforcement of arbitral awards, offers a feeling of comfort. However, this may no longer be the case for future arbitrations.

Despite the sharp decline of the cryptocurrency and NFT market, arbitration is the expected decentralized and neutral dispute resolution method for most contracts in this area of expertise, mostly targeting those arbitrators with experience in investments, financial transactions, supply of services, or intellectual property.

In many jurisdictions such as Russia, Greece, China, Qatar, cryptocurrency-related disputes were not considered arbitrable, which also excludes their recognition and enforcement on these territories, on public policy grounds.

Other issued could relate to the necessity of class actions or anonymous parties and the volatile nature of assets, that may require interim measures, adopted through the intervention of emergency arbitrators, difficult to enforce, unless automated.[16]

On 28 May 2021, a Mexican court indirectly enforced an arbitral award relying on a blockchain arbitration protocol *("Blockchain Arbitral Award")*[17], by incorporating a reference into a traditional arbitral award.

The clause mentioned a hybrid process, where the arbitrators had to draft

[15] Tigran Ter-Martirosyan, *Christopher Lim, Arbitration Tech Toolbox: Damages Expert Evidence Using Sensitivity Analysis, Scenario Modelling and Data Visualization*, Kluwer Arbitration Blog, 2021, the document is available online at https://arbitrationblog.kluwerarbitration.com/2021/08/27/arbitration-tech-toolbox-damages-expert-evidence-using-sensitivity-analysis-scenario-modelling-and-data-visualisation/, (last accessed at 13 April 2023).

[16] Edward Taylor, Jennifer Wu Zach Li, *Crypto Arbitration a Survival Guide*, "Kluwer Arbitration Blog", 2022, the document is available online at https://arbitrationblog.kluwerarbitration.com/2022/09/29/crypto-arbitration-a-survival-guide/ (last accessed 4 April 2023).

[17] Mauricios Virues Carrera, *Accomodating Kleros as a Descentralised Dispute Resolution Tool for Civil Justice Systems: Theoretical Model and Case of Apllication*, the document is available online at https://ipfs.kleros.io/ (last accessed 30 March 2023).

a procedural order addressed to the decentralized justice platform *Kleros*[18], which would then issue a decision based on its blockchain arbitration protocol**.**

After running its blockchain arbitration protocol the platform communicated to the arbitrator, the decision reached by the three jurors selected for the case. As a next step, the sole arbitrator rendered an arbitral award incorporating the decision from *Kleros* and the Mexican courts enforced the decision.

Smart contracts are self-executing instruments that involve automatically rendering the award, in the form of a code. However, parties may have to approach state courts for recognition and enforcement based on the New York Convention. The New York Convention was not updated for the technological era, but is still applicable, especially considering its pro-enforcement spirit. This means that parties still have a safety net, since an off-chain tribunal confirms the award. [19]

4. Platforms

There are several platforms, provided by well-known arbitral institutions, to help case users with overall communication and document sharing in a secure and easily accessible environment[20].

In October 2022, the ICC[21] launched its new digital case management platform, "*ICC Case Connect*", where users can e-file their Request for Arbitration and any other documents access their case library and communicate with each other.

In 2021, the HKIAC[22] also launched the "*HKIAC Case Connect*, which parties can use to communicate and "*track deadlines and dates on a case-specific calendar".* Similarly, AAA[23] offers its "*WebFile*" platform to its users, which includes the same features as the others, as well as additional features such as the option to pay invoices online.[24]

---

[18] A decentralized application deployed on Ethereum which provides its users with decentralized arbitration services.

[19] Arijit Sanyal, *Arbitration Tech Toolbox: Can the New York Convention Stand the Test of Technology Posed by Metaverse Awards?*, "Kluwer Arbitration Blog", 2022, the document is available online at https://arbitrationblog.kluwerarbitration.com/2022/12/20/arbitration-tech-toolbox-can-the-new-york-convention-stand-the-test-of-technology-posed-by-metaverse-awards/ (last accessed 9 April 2023)

[20] See Cristina Elena Popa Tache, *Adapting an Efficient Mechanism for Resolving International Investment Disputes to a New Era. Vienna Investment Arbitration and Mediation Rules,* „International Investment Law Journal", Volume 1, Issue 2, July 2021, pp. 91-101.

[21] International Chamber of Commerce.

[22] Hong Kong International Arbitration Centre.

[23] American Arbitration Association.

[24] Marc Labgold, Megan Labgold, *Arbitration Tech Toolbox: ICC Case Connect – A User Perspective*, "Kluwer Arbitration Blog", 2023, the document is available online at https://arbitrationblog.kluwerarbitration.com/2023/02/21/arbitration-tech-toolbox-icc-case-connect-a-user-perspective/ (last accessed at 4 April 2023).

The SCC[25] also has its own platform since 2019, which facilitates secure communications. Moreover, it uses a calendar with deadlines to inform the parties on the arbitral proceedings and includes an archiving service.

Such platforms can also facilitate other arbitration processes, for example the selection and appointment of arbitrators.[26] The *Arbitrator Intelligence* platform[27] collects data on legal professionals and optimizes the selections of arbitrators by providing their linkage with the nature of the case. [28]

Lastly, Web 3.0 is a future version of the internet based on public blockchain, a record-keeping system used for cryptocurrency transactions. Its main advantage is that it is completely decentralized, meaning that rather than users accessing the internet through services like Google, they will own sections of the internet. State authorities and intermediaries are excluded.

5. New technology and greener arbitration

The transition to a low-carbon future influences all fields of activity. Arbitration seems to be more easily adaptable than the state courts system, since sustainability became a fact of consideration for most supervising institutions.

The behavioral changes associated with the usage of new technologies are reducing the carbon footprint of arbitral proceedings. Virtual and hybrid meetings have the most positive impact, since they dramatically decrease case user's international flight agenda.

Using electronic rather than hard copy communications that are sent around the globe from parties to counsels and then to institutions, is an important step in mitigating the environmental impact of arbitration as well.

6. Obstacles in using technology in arbitration

The arbitral tribunal should ensure that the use of technological tools does not interfere with the parties' right to equal treatment, to free access to a court of law, procedural fairness and to the opportunity to fully present their case.

Parties could encounter barriers in accessing a certain technology, for example due to a lack of IT literacy, a language barrier, time-zone discrepancies, financial reasons or regulations in their state that limit new technologies.

---

[25] Stockholm Chamber of Commerce.

[26] Michelle Bernier, *Technology and Arbitration: New Trends in Law*, 2023, the document is available online at https://www.econlib.org/technology-and-arbitration-the-new-trends-of-law/ (last accessed 14 April 2023).

[27] The platform can be accessed online at https://arbitratorintelligence.com/ (last accessed 14 April; 2023).

[28] https://ciarglobal.com/arbitrator-intelligence-anuncia-la-disponibilidad-de-sus-informes-sobre-arbitros/.

7. Conclusion

Artificial Intelligence can manifest itself in international arbitral proceedings in three different ways: as a support for the automation of procedural acts (reducing time and costs), as an interpretative tool for consultation or as a judging entity.

The compromise of semi-automation that involved automating those elements of the arbitral procedure that involve repeat processes, while leaving arbitrators to address decision-making is an acceptable solution for short and medium term.

As a number of new technologies have emerged and will undoubtedly continue to advance, the future of technology arbitration seems promising.

Arbitration has many advantages for emerging technology disputes. Currently, it is not completely independent from national court's interference, especially in the action for annulment and recognition and enforcement phases. Basic level, *'off-the-chain'* disputes that imply web 3.0 will still need to engage with traditional dispute resolution methodologies, including contract interpretation and application of the law.

In a few years from now, even the concepts we consider novel today will become outdated. Arbitration has the potential to become a private procedure, fully independent of geographic limitations and off-chain interventions, moving towards an entirely neutral and non-state based forum of dispute resolution, finalized with an automatically enforceable award, compatible with most decentralized platforms.

Bibliography

1. Arijit Sanyal, Arbitration Tech Toolbox: *Can the New York Convention Stand the Test of Technology Posed by Metaverse Awards?* "Kluwer Arbitration Blog", 2022.
2. Cristina Elena Popa Tache, *Adapting an Efficient Mechanism for Resolving International Investment Disputes to a New Era. Vienna Investment Arbitration and Mediation Rules,* „International Investment Law Journal", Volume 1, Issue 2, July 2021.
3. Edward Taylor, Jennifer Wu Zach Li, *Crypto Arbitration a Survival Guide*, "Kluwer Arbitration Blog", 2022.
4. Gauthier Vannieuwenhuyse, *Arbitration and New Technologies: Mutual Benefits,* „Journal of International Arbitration", 2018, Issue 1.
5. Kiran Nasir Gore, *International Disputes and Digital Disruption, in Conversation with Claudia Salomon, President of the ICC International Court of Arbitration*, "Kluwer Arbitration Blog", 2022.
6. Łągiewska, M., *Chapter 11 The New Landscape of Arbitration in View of Digitalization,* in Shaheeza Lalani and Steven G. Shapiro (eds.), *The Impact of COVID on International Disputes*. Leiden, The Netherlands: Brill | Nijhoff, 2022, pp. 208–217doi: https://doi.org/10.1163/ 97890045 14836_013.

7. Leonardo F. Souza-McMurtrie, *Arbitration Tech Toolbox: Will ChatGPT Change International Arbitration as We Know It?*, "Kluwer Arbitration Blog", 2023.
8. Marc Labgold, Megan Labgold, *Arbitration Tech Toolbox: ICC Case Connect – A User Perspective*, "Kluwer Arbitration Blog", 2023.
9. Michelle Bernier, *Technology and Arbitration: New Trends in Law*, 2023.
10. Nasser Ali Khasawneh, Maria Mazzawi, Ricardo Christie, *Arbitration and the Advent of New Technologies*, "Global Arbitration Review".
11. Peter Smith, Arbitration Tech Toolbox: *Arbitrating Digital Asset Disputes*, "Kluwer Arbitration Blog", 2022.
12. Robert Bradshaw, *Arbitration Tech Toolbox: Cross Examination? There's an App for That*, "Kluwer Arbitration Blog", 2023.
13. Tigran Ter-Martirosyan, Christopher Lim, *Arbitration Tech Toolbox: Damages Expert Evidence Using Sensitivity Analysis, Scenario Modelling and Data Visualization*, Kluwer Arbitration Blog, 2021.
14. Use of Technology: The Virtual Reality, White and Case, 2021.

Implications of ChatGPT Technology on Criminal Law

Lecturer **Silviu Gabriel BARBU**[1]
PhD. student **Vasile COMAN**[2]

Abstract

The scientific community has been discussing for a long time about the potential of creating an artificial, non-biological, impartial machine with human intelligence, considering that such an innovation with emotional - and not only computational - intelligence could bring many benefits to society, including the legal world. Recently introduced (November 2022) in a more publicly accessible form, the ChatGPT (Chat Generative Pre-trained Transformer) technology is one such artificial intelligence application, part of the OpenAI project, and is essentially built as a conversational interface with the potential to deliver results in a human-like manner. As an artificially intelligent chat-bot, ChatGPT has several functions subsumed to its use and performance, that are rather extensive, and there is a concern whether the ChatGPT technology may be used for judicial decision-making, in which context arises the question whether it can also be hijacked in order to commit criminal offences. The answer is positive, but accepting this fact raises some possible issues in criminal law enforcement practice such as establishing the guilt, the dialogue with the personal nature of the criminal liability, adapting the criminal sanction system to the specific environment of commission, and others, discussed in this article. ChatGPT is certainly the chat-bot of the moment and perhaps even of the year 2023. Formal artificial intelligence (AI) is still in its infancy, but despite its limitations, the ChatGPT technology can already be considered impressive in its timeliness and evolution compared to other automated chats or applications of robotics, as it has the capacity to communicate credibly and convincingly, as a human interlocutor and in real time.

Keywords*: ChatGPT, OpenAI, artificial intelligence (AI), criminal law, criminal offence.*

JEL Classification: K14, K24

1. Introduction

The scientific community has long discussed about the potential of creating an artificial, non-biological, impartial machine with human intelligence, considering that such an innovation with emotional - and not only *computational* - intelligence will have a large-scale echo in terms of use cases and will also better help humans understand their selves and solve the problems they face.

[1] Silviu Gabriel Barbu - Faculty of Law, University „Transylvania" of Brasov, Romania, silbarg70@gmail.com.
[2] Vasile Coman - Faculty of Law, „Titu Maiorescu" University of Bucharest; judge at Prahova Tribunal, Romania, v.comann@yahoo.com.

The goal created around artificial intelligence (AI) has, ultimately, the ideal of creating a machine that is indistinguishable from a human in terms of its thought process for the benefit of the latter, a goal which is difficult to achieve, however, considering that most people do not understand their own thinking mechanism

Recently introduced (November 2022) in a more publicly accessible form, the Chat-GPT (*Chat Generative Pre-trained Transformer*) technology is one such application of artificial intelligence that has sparked the world's interest, but also concern about a tool that interferes with what is the pride of our human species: intellectual capabilities. This fact is seen by some members of the community as a danger for the human, with an existing risk of losing control over his evolution as forms of artificial intelligence and computer programs are perfected towards greater and greater autonomy, to the detriment of the human[3].

Conceptually, Chat-GPT is a member of the family of pre-trained generative transformative language models and has been designed to deliver results in a human-like manner. As a form of intelligence it uses both supervised learning and reinforcement learning in a process called Reinforcement Learning from Human Feedback (RLHF), i.e. comparing some features with their human[4].

Chat-GPT is essentially a *chat interface* that can be queried following the creation of a user account, being designed in such a way that it can intelligently answer a wide variety of questions and even give the impression that a meaningful dialogue can be carried out with it. The technology is based on an algorithm called „Large Language Modeling”[5] which aims to understand the structure of human language and, more importantly, to predict the next word in a sentence in order to generate coherent texts[6]. However, this type of algorithm requires very long training phases, similar to learning a foreign language.

At the origin of Chat-GPT is the OpenAI project that had started in 2015[7],

---

[3] See Ricardo Pedro, *Artificial intelligence on public sector in Portugal: first legal approach*, „Juridical Tribune - Tribuna Juridica”, Volume 13, Issue 2, June 2023, pp. 150-154.

[4] The Chat-GPT technology uses probability to guess which word should appear at a certain point in a sentence, mimicking human speech and writing patterns. With access to so many parameters and words, ChatGPT is able to use a vast amount of vocabulary, information and context to produce meaningful and engaging responses to queries on a seemingly unlimited number of topics.

[5] The modeling learning algorithm is not foreign to other related disciplines, such as psychology, where the concept of NLP (neuro-linguistic programming) exists, also known as the psychology of excellence through knowledge modeling. The current version of Chat-GPT, however, is much more advanced, being built with the help of a large language model (also known as LLM) called GPT-3, one of the largest and most powerful LLMs developed to date, with about 175 billion parameters and access to 300 billion words.

[6] However, although it has been tested, the technology does not yet have the ability to predict the future, but this capability is likely to be developed in the future depending on the pool of information made available to the application.

[7] Since its founding in December 2015, the start-up has been endowed with $1 billion in funding, subsequently attracting Google as an investor, with which it competes. Besides, Google has developed its own prototype of AI chatbot "Bard", which will be able to access updated information both on the internet and in Google's own (and enormous) database. So there are other chatbots under

dedicated to pushing artificial intelligence research very far, and its founder Sam Altman has contributed to many high-tech companies: he has co-founded Airbnb and helped finance other projects such as Reddit, Twitch, Dropbox. Chat-GPT is not OpenAI's first spectacular creation. The company, which is jointly run and financed by American businessman Sam Altman and Elon Musk, is also behind DALL-E, an image generator based on keywords[8].

The purpose of the OpenAI software is to assess their effectiveness and potential to create an artificial, non-biological machine with human intelligence. The resulting findings may better guide researchers in creating more human-intelligent models, not only helping humans as an unbiased data source, but also helping the machine create its own data, views, beliefs and opinions autonomously.

2. Uses and limitations of the Chat-GPT technology

Among the basic uses of this artificial intelligent chat-bot, we may evoke the following basic functions or uses:

a) The first function of Chat-GPT is that of a conversational interface (*chatbot*). During various tests, it was subjected to a wide variety of questions: encyclopaedic information, cooking recipes, filmographies, etc. Each time, Chat-GPT produced summaries of an honourable quality.

Chat-GPT also remembers the questions previously asked by the interlocutor, and is even able to correct itself, having the capacity to learn from its own mistakes.

b) Chat-GPT can also be used to create content, a surprising use, as the application is able to create even viable code for a Wordpress site, to elaborate comments - accompanied by emoticons - to controversial articles. Chat-GPT has also managed to create Facebook "posts", comments on controversial articles, tips for negotiating the price of a used car, suggestions for image editing software, and more. On the other hand, Chat-GPT has been much less inspired in the realms of art (e.g., poetry), or humor management.

c) Among the amazing capabilities of Chat-GPT is the ability to summarie ideas, articles, studies or to develop analyses[9]. For example, it has been

development, which suggests that the ChatGPT technology is just the first general example in a market that may soon be competitive enough. Anis Benabed, Lucica Tudoran, *Artificial Intelligence Towards International Regulations, Frameworks and Laws in the World of Globalization: Implications and Challenges*, „Perspectives of Law and Public Administration", Volume 12, Issue 2, June 2023, p. 269.

[8] DALL-E is an AI system that can create realistic images and art from a natural language description, but it lacks the emotion, "realness" and expression behind the art it created itself.

[9] Not only that, but the technology has also been able to provide users with well-developed professional e-mails, essays and other literature that would otherwise require an application of the mind. - Gagan Anand, The Revolutionary Chat GPT And Its Legal Policies, 1st of 2023, www.mondaq.com.

asked "Can you write a 500-word discussion on this topic?" and the program complied and the result was much appreciated. Chat-GPT software can respond to all written requests by generating texts that look as if it was written by a human, and is able to simulate truly credible discussions, which is explained by the fact that its learning algorithm is based on ingesting an astronomical amount of data, be it literature, television, online public forums, news articles or movie scripts, and more. This is, however, at the same time a limitation of its own because for now Chat-GPT technology does not search for information outside the database.

d) Can Chat-GPT technology be used *for judicial decision-making*? This has already been tested and, it seems, yes. In one case[10], in order to to make a decision in one of the cases he had to decide (concerning medical insurance for a child suffering from autism and whose parents, due to financial difficulties, could not afford to cover the costs of treatment and transport), a judge in the Colombian city of Cartagena used an unusual tool - the artificial intelligence program Chat-GPT. The judge asked the Chat-GPT program whether, under Colombian law, a minor suffering from autism is exempt from paying for treatment, and the answer was yes. The news, reported by The Guardian, has caused controversy between those who argue that the latest technology should be used to streamline the justice system and those who reject the idea that artificial intelligence can make decisions for humans.

Can Chat-GPT be used *to create laws*? It seems so. For example, ChatGPT was used experimentally to produce a 14-page law article in an hour.

Are there any limitations in Chat-GPT technology? The current version of ChatGPT is subject to several critical limitations, originating in the finite corpus of information from which it derives its answers, which makes it vulnerable to "hallucinations", i.e. content invention[11].

Although it is a revolutionary step in the artificial intelligence sphere and is nevertheless accompanied by a vast knowledge base, the Chat-GPT technology is far from being infallible because, first of all, its answers may contain many errors[12]. However, Chat-GPT seems to resolve them over time as it expands its knowledge base. Thus, in early January 2022, in a question about Descartes, he claimed that this philosopher lived in South America, which is not correct. A month later, he no longer displays this error. However, it would be necessary for Chat-GPT to cite its sources, as Wikipedia does, so as not to conflict, as we shall see, with the copyright on the information accessed and processed.

---

[10] *Lumea* Magazine, no. 3/2023, p. 6.

[11] That is, it will fabricate facts and sources it does not have access to through sufficient data. For example, there are interactions where ChatGPT has repeatedly fabricated scientific studies in response to the queries of users, displaying the same level of confidence as providing a factually correct answer.

[12] This also results from the description of the application on Open AI's official website, which states that "We've trained a model called ChatGPT which interacts in a conversational way. The dialogue format makes it possible for ChatGPT to answer follow-up questions, admit mistakes, challenge incorrect premises and reject inappropriate requests".

Chat-GPT also tends to generate long, deliberately watered-down sentences with certain formulas that it likes to repeat (with only one or two variations)[13]. Very often, for lack of knowing what to answer in the moment, the application calls for several unnecessary or inconclusive sentences regarding the expected answer.

Even though Chat-GPT can respond to all written requests by generating texts that look as if they were written by a human, and is able to simulate truly credible conversations, this is explained by the fact that its learning algorithm is based on ingesting a huge amount of data[14].

Because it lacks experiences with different people, the Chat-GPT chatbot cannot provide highly personalized responses, noting that the program cannot access past conversations to inform its responses.

Another limitation that is difficult to compensate for - regardless of the amount of knowledge and information made available to it - is the role of human consciousness and awareness of social values in a given historical moment, elements that in the field of law acquire an essential role[15].

3. The use of Chat-GPT in legal services, particularly in the profession of lawyer

The neglected advantages of AI have determined various law firms to start initiating processes to introduce artificial intelligence systems into their functioning by accessing generative AI developed specifically for the complicated legal problems that law firms face in their caseloads.

On the other hand, legal professionals around the world have questioned whether a new existential threat has emerged in OpenAI's much-discussed AI chatbot, Chat-GPT, whose rise in popularity and large number of users in a short time was meteoric[16]. Therefore, there are concerns about job security in the legal profession, with existential fears attributed to the ChatGPT's seemingly miraculous ability to produce, almost instantaneously, compelling written work on a wide range of topics, including answers to legal questions and drafts of legal

[13] This can also include the fact that ChatGPT will often write answers that sound plausible and convincing, but incorrect or nonsensical, and this is because it does not encompass all the knowledge in the world or on the internet and does not currently include any resources beyond the year 2021.

[14] ChatGPT sets responses that are maintained at the language level, but which lose their meaning and are often false. This happens even on fairly simple general knowledge topics.

[15] This can include the ability to agree, disagree, judge and continue debates on subjects even when all parties have the same information. See Macey-Dare, Rupert, *ChatGPT & Generative AI Systems as Quasi-Expert Legal Advice Lawyers - Case Study Considering Potential Appeal Against Conviction of Tom Hayes* (January 30, 2023). Available at SSRN: https://ssrn.com/abstract=4342686 or http://dx.doi.org/10.2139/ssrn.4342686.

[16] For example, Netflix took 3.5 years to reach its first million users. For Spotify, five months and Instagram 2.5 months. ChatGPT reached this milestone in just five days.

documents. So should lawyers around the world be worried or excited about the future of AI in the legal profession?

There are a number of potential benefits for legal practitioners and consumers of legal services that can be achieved through the adoption of generative AI technologies, such as ChatGPT, including improved productivity and efficiency, reduced costs and improved communication.

Therefore, ChatGPT seems to have the capacity to quickly generate answers to simple legal questions, quickly prepare preliminary drafts of legal documents, such as draft contracts, and can quickly find relevant information referenced in large legal documents such as case law. If these types of answers are shown to be reliable, over time, lawyers may be able to resolve clients' simple legal questions more quickly and also get a head start on matters that are more complex and strategically valuable to clients.

From the perspective of improving communication as it continues to evolve, ChatGPT may also be able to assist lawyers by quickly drafting clear and concise communications to stakeholders such as clients, opposing lawyers and courts.

ChatGPT can also reduce costs incurred by law firms and in-house counselors by automating and reducing the need for human activity in upfront tasks on matters.

The access to a wider range of expertise is another utility of Chat-GPT, subject to granting access to a wider dataset than the current GPT-3 corpus, thus becoming capable of helping lawyers to gain access to a wider range of legal sources (articles, manuals, professional statutes, etc.) than human lawyers would typically do.

It should be noted, however, that for the moment users will still need to carefully check the quality of Chat-GPT results for the accuracy and relevance of the facts contained in them, to avoid the trap of "hallucinations" - made-up answers[17], or potential biases[18]. For example, ChatGPT responses do not currently take into account any changes to legislation from 2021 onwards, and this may cause the application to favour outdated interpretations of legal principles due to the fact that such interpretations are more commonly associated with the existing dataset[19].

[17] When asked if he ever fabricates sources or information, ChatGPT replied, "As a language model, I don't have the capacity to fabricate sources or information, I can only generate text based on models from the data I've been trained on. However, my answers may not always be accurate or appropriate given the context of a user's question." This suggests that ChatGPT does not see a "hallucination" as equivalent to "fabrication", but rather a side-effect of the way it generates answers, i.e. by replicating text based on patterns derived from its training data.

[18] Such prejudices might include racist and gender views.

[19] When asked if he is biased towards certain points of view, Chat-GPT answered: "As a machine learning model, I am not capable of having opinions or biases. However, the data that I have been trained on might contain biases, which might be reflected in my answers. OpenAI is actively

From a privacy and legal professional privilege perspective, law firms and other organizations intending to access Chat-GPT licenses for their use will need to clarify whether the data they enter into Chat-GPT will be retained and used by OpenAI or by the Chat-GPT software and security controls that OpenAI has in place[20].

4. Chat-GPT technology and criminal law

Can Chat-GPT software technology be used to commit crimes? Definitely yes, and some examples are enlightening.

a) Since it has the ability to communicate as a human interlocutor and to derive *context* from the interactions in which it participates, the Chat-GPT technology could contradict the criminal rules that protect the consent of the holders of the exchanged information, associated with copyright observance.

Therefore, the information stored in the Chat-GPT database is usually copyrighted, and its use in the process of forming the response to the user's replies remains protected, at least under European law, against any unauthorized use[21]. As the communication process may involve more than one source of information from perpetrators in more than one country, the question of concurrence of applicable criminal laws may also arise.

In Romania, for example, art. 13 of Law no. 8/1996 on copyright provides that the use of a work gives rise to distinct and exclusive economic rights of the author to authorize or prohibit, inter alia, „a) the reproduction of the work;" and art. 14 states that *reproduction*, for the purposes of this law, means "the making, in whole or in part, of one or more copies of a work, directly or indirectly, temporarily or permanently, *by any means and in any form, including* the making of any sound or audiovisual recording of a work, as well as the *permanent or temporary storage thereof by electronic means*".

The legal protection and limitation of the risk of copyright infringement is also achieved through criminal law means, as reflected in the incriminations contained in Law no. 8/1996, in art. 194 („It is a criminal offence and punishable by imprisonment from 6 months to 3 years or a fine *to make available to the public, including via the internet or other computer networks, without right,* works or products bearing related rights or sui generis rights of database manufacturers or copies thereof, regardless of the support, so that the public can

working on ways to detect and mitigate these biases in our models". ChatGPT is clearly aware of the risk of a response containing bias, a risk that could be mitigated as the technology develops.

[20] In political activity, the idea of a regulating organisation is promoted, aligning private and public interests through a decentralised and fluid rebalancing of functions. See Diana Dănișor, *The Explosion of Network Techniques and the Myth of the Network between Science and Democracy. Legal Implications,* in „Perspectives of Law and Public Administration", Volume 12, Issue 2, June 2023, p. 224.

[21] From this perspective, the question has sometimes been asked whether this is the end of copyright as we know it?

access them at any place or at any time individually chosen"), art. 195 („It is a criminal offence and punishable by imprisonment from 6 months to 3 years or a fine the *unauthorized reproduction* on computer systems of computer programs in any of the following ways: installation, storage, running or execution, display or transmission on an internal network"), art. 196 [„(1) Shall constitute offences and shall be punishable by imprisonment for a term of one month to one year or by a fine the following acts committed without the authorization or consent of the holder of the rights recognized by this law: a) the *reproduction of works* or products bearing related rights; (...); e) making derivative works"], art. 197 [„(1) It shall be an offence and punishable by imprisonment for a term of six months to three years or a fine for a person who appropriates, without right, in whole or in part, the work of another author and presents it as his own intellectual creation"], and others.

On the other hand, with regard to the violation of copyright or other intellectual property when using Chat-GPT, it was objected that this form of artificial intelligence must obtain the necessary information from a particular source, due to the nature of machine learning, and that the company is aware of the possibility of such violation and has provided a clause stating that, after being notified of any alleged violation, it may delete or disable the content in question[22].

b) Also, starting from the premise of the real character of good faith in the elaboration of the answers to the requests addressed, one can enter the realm of offences against the protection of the social value of trust. For example, giving the wrong answer may lead to certain decisions being taken which may subsequently lead to other actions which give rise to offences such as false statements, intellectual fraud, deception, and others.

c) The potentially illegal or abusive access to and then use of user data, especially since recent use of the app, which has been widely published on various social media apps, has revealed that individuals have been adding information about their employers, college professors, assignments, and even their clients in order to cause the app to redact emails, research papers, exam answers and various other documents that might otherwise be designated confidential and would have raised issues of violation of non-disclosure agreements in certain cases. E.g. art. 361 of the Criminal Code (RO) on the illegal interception of a transmission of computer data, art. 364 of the Criminal Code on the unauthorized transfer of computer data.

It is important to note that one of the main features of the application is that it studies the user's behaviour in order to provide them with the most appropriate results, which further raises the question of the extent to which the application can access personal information held in the user's account, and this access could conflict with certain legal provisions on the right to privacy and

[22] Another aspect of the intellectual property issues is Chat GPT's right to the information originally received by the chatbot, which has been specifically mentioned as being the property of Open AI, the unlawful use of which may again open the user to infringement actions by the company.

access in the IT environment.

The use of social networks has always been affected by the misuse of users' personal information by leading companies. Conglomerates such as Meta Inc, Twitter Inc and even ABC Inc have faced international and national scrutiny over the illegal use of this information for monetary and popularity gains. This abuse has grown to such an extent that these companies have even been periodically summoned by the U.S. Senate to face hearings in the Congress[23].

d) Chat-GPT is an artificially intelligent application capable of making optimal use of personal information for the benefit of the application and to the detriment of the user, and where the privacy policy requires "unlimited" use of the user's information, so that it becomes obvious that the threat of privacy violation may increase substantially, raising the question of the incidence of the offence of violation of private life under art. 226 of the Criminal Code, under the conditions of this incriminating text, possibly adapted to the new challenges of AI.

Chat-GPT's privacy policy states that Open AI may share the user's personal information with third parties without prior notice, unless such notice is required by law. It also states that the exchange of information may also be without limitation in cases where it is shared with vendors and service providers to help Open AI meet "operational needs" and perform "certain services and functions." It is thus noted that because the platform does not define the terms "operational business needs" or "certain services and functions", the extent and reasons for sharing data become unclear and may come into real conflict with the law.

At the same time, Chat-GPT's privacy policy further specifies that the user's personal information may also be used for "conducting research", which may be either internal, shared by third parties or even published or made generally available.

A simple examination of this clause provides a clear conclusion of a considerable increase in the scope of public sharing of information. By including the term of publication or any generally available information, coupled with the fact that the company has required an unlimited approach to information in undefined circumstances, will greatly enhance the vigilance of the user. The need for such caution is amplified by the fact that the policy requires a collection of data on service usage, type of content viewed, device information and other relevant information of the user.

However, the legislations still need to provide protection to artificial intelligence or other self-generated computer programs under the law, in order to

[23] Even the Competition Commission of India (CCI) initiated its own case against Meta Inc. for abusing its market dominance by updating the terms of use of its messaging app "Whatsapp" and allowing the sharing of user data on Facebook Inc. While the CCI in this case named "In Re: Updated Terms and Conditions and Privacy Policy for Whatsapp Users" deemed that WhatsApp contravenes the law.

make the technology more economically feasible and accessible to users[24].

In case of crimes committed by or through the use of Chat-GPT technology, some *possible problems may arise in criminal law enforcement practice*:

a) Who will be the active subject of the offence in this case and how does this reconcile with personal criminal liability? Staying in the cyberspace sphere, one could make an analogy with criminal liability for cyber attacks directed from other states' territories by non-state entities, but for the preservation of the necessary human – machine control link, in the first case the ability to decide correctly and the mistake itself should be provided by humans.

At the time being, the Chat-GPT technology is, however, a generic program in an experimental phase, so it should be "empowered" to decide ("think") for itself what is right and wrong and have its own source of derived data, it should have several selection mechanisms (*input*) such as temperature sensors, sensors for detecting change in facial expressions, feelings besides the visual component and audio inputs.

Experiences and decisions are shaped by many things - their inputs (what we see, hear, feel, smell, taste and believe), the person/agent, previous knowledge experiences with the person/agent, the situation they react to, the history of knowledge of the situation.

Also, responses and opinions should all be independent of the human interlocutor, just as it is with humans, but with consideration of different experiences for different people - for understanding humanity, logic and rationality alone is not enough.

That is, although he is left to be influenced by certain opinions, the decision itself should be the choice of the program based on his personal inputs, experiences and not something that is complexly encoded in him or taken from public sources.

Therefore, if AI is ever to achieve the same kind of intelligence that humans have, it should first be able to have its own system of opinions independent of any human input; this means that the system must receive, experience and process everything as humans do[25].

b) Criminal law enforcement in space? The Chat-GPT technology is developed by the US-based Open AI company, and the access and use of accounts is done in the virtual environment, so the classic principle of ubiquity of criminal law should be reconfigured and adapted to the new challenges of the virtual environment.

c) How can guilt be proven? As an essentially subjective aspect, the evidence in this case should still be concentrated in the ex re sphere of traditional

[24] See Cristina Elena Popa Tache**,** *Public International Law and FinTech Challenge*, „Perspectives of Law and Public Administration", Volume 11, Issue 2, June 2022, pp. 218.

[25] Ahmed, Bin Khalid, *Making machines more human (studye*), 2022, https://www.research gate.net.

criminal law, by reference to certain physical manifestations of the system (e.g. repeated errors of execution with close legal consequences), with the mention that in this case one could speak of a specific objective component in the content of the subjective side of the offence.

d) Should the system of criminal sanctions be (re)adapted to the specific environment of the offence? It is argued that the application of a criminal fine is inappropriate and the application of a prison sentence is excluded. In the case of Romanian criminal law, however, it would be possible to use the current complementary penalties, such as the suspension of the activity of the Chat-GPT programme together with the imposition, as a complementary penalty, of the remediation of the system and its reintroduction into the circuit after an expert verification authorized by certain competent authorities specifically created for this purpose.

5. Conclusions

Chat-GPT is certainly the chatbot of the moment and perhaps even of the year 2023. Official artificial intelligence (AI) is still in its infancy, but the technology under review can already be considered impressive by the degree of timeliness and evolution compared to other automated chats or robotics applications.

The Chat-GPT technology has the ability to communicate credibly and convincingly, like a human interlocutor, spontaneously and in real time. With all its popularity and expansion, the debate about the use and misuse of data by various web-based applications such as Chat-GPT, is still relevant and requires a change in legislation so that any violation of the criminal law or intellectual property law (copyrights and trademarks) by these applications can be dealt with appropriately.

The potential benefits need to be balanced against the potential risks, which include Chat-GPT's overestimation of legal knowledge, "hallucinations", bias, copyright and data privacy.

On the other hand, as with any item in the virtual world, one must remain vigilant against the risks of over-reliance on Chat-GPT and other AI chatbots like it. These include:

Overestimating legal knowledge - ChatGPT can only generate text based on patterns it has learned from the data it has been trained on. Therefore, if its training dataset does not contain sufficient resources in the specific area of law in which it is being queried, the chatbot may produce a lucid and understandable response, but one based on an incomplete or outdated picture of the law[26].

[26] When asked about the potential risk of users overestimating their knowledge of the law, ChatGPT responded, "As a language model, I am able to understand and respond to natural language input, but it is important to note that my knowledge is based on the text that I have been trained on and may not be accurate or up-to-date -to date. In addition, I am not a substitute for legal advice from a

Whether the technology will adequately and comprehensively address all areas of law in all jurisdictions is both unlikely and difficult to verify, given its size, plus the general limitation of training this application only on data available until June 2021.

Bibliography

1. Ahmed, Bin Khalid, *Making machines more human (study)*, 2022, https://www.researchgate.net.
2. Anis Benabed, Lucica Tudoran, *Artificial Intelligence Towards International Regulations, Frameworks and Laws in the World of Globalization: Implications and Challenges*, „Perspectives of Law and Public Administration", Volume 12, Issue 2, June 2023.
3. Cristina Elena Popa Tache**,** *Public International Law and FinTech Challenge*, „Perspectives of Law and Public Administration", Volume 11, Issue 2, June 2022.
4. Diana Dănișor, *The Explosion of Network Techniques and the Myth of the Network between Science and Democracy. Legal Implications,* in „Perspectives of Law and Public Administration", Volume 12, Issue 2, June 2023.
5. Gagan Anand, *The Revolutionary Chat GPT And Its Legal Policies*, 1st of March 2023, www.mondaq.com.
6. *Is your next lawyer a chatbot?* Study available on www.allens.com.au.
7. *Lumea* Magazine, no. 3/2023.
8. Macey-Dare, Rupert, ChatGPT & Generative AI Systems as Quasi-Expert Legal Advice Lawyers - Case Study Considering Potential Appeal Against Conviction of Tom Hayes (January 30, 2023). Available at SSRN: https://ssrn.com/abstract=4342686 or http://dx.doi.org/10.2139/ssrn.4342686.
9. Open AI, Introducing ChatGPT, available on https://openai.com/blog/chatgpt.
10. Ricardo Pedro, *Artificial intelligence on public sector in Portugal: first legal approach*, „Juridical Tribune - Tribuna Juridica", Volume 13, Issue 2, June 2023.

qualified professional." This response demonstrates that while ChatGPT itself does not recognize the risk of users overestimating their ability to advise on the law (and would not give such a warning when asked a legal question), when asked, ChatGPT recommends that users consult qualified practitioners in connection with legal questions.

The Robot as a Natural or Legal Person. Another Perspective on the Concept of Person

Researcher **Cristina Elena POPA TACHE**[1]
Student **Marius Vasile BÂRDAN**[2]

Abstract

The word you will find in the interface is to understand the concept of a person and what skills a being must have to be a person. This material also examines the religious perspective on the issue announced in the title. Manufacturers and computer scientists involved in building and training robots for consumers will need to consider the distribution market sector and by implication, the beliefs of the people who are to use this type of artificial intelligence as a tool. In the biblical account of man, it is said that man was created by God by a triumphant counsel: 'Let us make man in our image, after our likeness', and by making a person capable of communication, it means that he is a person, because communication makes you a person, but a freely consented communication. The concept of a person has evolved over time so that in the Greek period the man who was not free could only express himself behind a mask, as in the performance of a character in a play today, then in the Roman world, as a man who was not free could only express himself by having a patron who gave social witness for the man to express himself freely. So, freedom of expression was an ability of the human person, of a natural person in the legal sense. The article tries to expose the chosen topic from the perspective of two authors with their particular opinions: the professor of law in communications and new technologies who sees the objective whole of things and the eminent student, Orthodox priest who comes up with particularly interesting arguments. In the preparation of this material, we used an introspective method with qualitative and quantitative values.

Keywords: *robot, religion, legal personality, new technologies.*

JEL Classification*:* K15, K24, O14, O33, Q55

1. Introduction

In recent decades, and quite acutely in recent years, technological developments in the field of robots and artificial intelligence in general have raised interesting and complex questions about the legal and even moral status of robots. One of the modern debates concerns the recognition of robots as "persons" - either as natural persons, with rights and responsibilities similar to those of human beings, or as legal persons, with limited rights and obligations within specific legal and economic systems. In this context, our article explores the idea of viewing

[1] Cristina Elena Popa Tache - researcher at CIRET - Center International de Recherches et Études Transdisciplinaires Paris, France, cristinapopatache@gmail.com.
[2] Bârdan Marius Vasile - Faculty of Psychology, Behavioral and Legal Sciences, "Andrei Șaguna" University of Constanta; Orthodox priest, Romania, nifonmariusvasile@gmail.com.

robots as natural persons or as legal persons. We will attempt to analyse the pros and cons of recognising robots as persons and collect the legal, ethical and social implications of this approach from various religious, ethical and cultural perspectives on the status of robots within human society. Throughout history, the concept of personhood has evolved and undergone certain mutations, and rapid technological development has brought with it new and complex issues in defining the status of robots, especially as we are only now discussing the development of the most comprehensive laws on artificial intelligence in different regions of the world. Slowing down or suspending the adoption of regulations of this kind is not a solution because law, now removed from the social sciences, will not be able to keep pace with the latest technological or social developments, which brings to mind the classic defacement of the normative that becomes clear only towards the end of an era, symbolised suggestively by the owl in the hand of the goddess Minerva taking flight at sunset[3]. From autonomous robots in industry and medicine, to virtual assistants in everyday life and social robots in the care of the elderly or children, robotic technology has become increasingly present in our lives, and is expected to be increasingly common, which has brought to light some profound questions about how we should have regulated the legal status of these artificial entities. Today, it is no wonder that there are various technological investments, maritime, airborne, space or land-based, building and launching satellites, building renewable power plants, building and exploiting blood plasma fractionation and many more[4].

Thus, this article aims to examine some of the debates, arguments, legal, ethical, social and cultural implications of these needs for legal regulation generated by the inevitable emergence of robots.

2. Some legal issues and questions to consider

Given the novelty of the issue, which comes against the backdrop of a project currently underway in the European Union to draft a legislative act on artificial intelligence, we shall point out certain differences that will be evident both if this act is adopted and if it fails[5].

Although the draft we are discussing considers that it is "appropriate for a particular natural or legal person, defined as a supplier, to take responsibility for the placing on the market or putting into service of a high-risk AI system, irrespective of whether that natural or legal person is the person who designed or

[3] The owl, her sacred animal, is the ancient symbol of thought, education and brotherhood. The goddess of wisdom, Minerva was therefore chosen, not by chance, by the members of the Romanian Academic Society at the unanimous proposal of George Barițiu to appear on its seal in 1867.

[4] Cristina Elena Popa Tache, *Editorial*, in „International Investment Law Journal", Volume 1, Issue 1, February 2021, p. 4.

[5] This is the *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 acts*, com/2021/206 fInal.

developed the system", there are nevertheless certain regulatory gaps that will subsequently need to be addressed. One of the aspects that is not mentioned is that of considering artificial intelligence as an extension of the human person, a kind of medical prosthesis, in which case we can no longer treat it as a separate tool, but will discuss it as a complement to the physical or mental abilities of the human person. The future is probably on the side of international "bio" law, which also includes that part intended for human enhancement.

However, the EU may not have the legal basis in the Treaties on which to base new regulations such as this one, since Article 114 of the Treaty on the Functioning of the European Union (TFEU) provides for the adoption of measures to ensure the establishment and functioning of the internal market. It is only the possibility of regulating certain aspects that relate solely to the EU internal market, more specifically the digital single market[6] . But let us bear in mind one of the great merits of the Court of Justice of the European Union, namely the enunciation of the principle that the Treaties should not be interpreted rigidly, but should be considered in the context of the stage of integration and the objectives they have set. This principle has allowed the EU to legislate in areas that are not subject to specific provisions in the Treaties, for example the fight against pollution (in a judgment of 13 September 2005 - case C-176/03 - in which the Court actually authorised the EU to take measures related to criminal law when they are considered "necessary" to achieve the objective pursued in terms of environmental protection).

However, what regulations at international level could be drawn up and adopted urgently with regard to the situation described? How will the concept of *human enhancement* through artificial intelligence[7] be regulated internationally? This is just one of many regulatory shortcomings.

Another question is: if these technologies are also used for *animal enhancement*, what will be the legal regime since the legal status of animals remains a notion left behind, if not completely neglected in favour of the obsessive focus

[6] The draft provides that "certain specific rules on the protection of individuals with regard to the processing of personal data, in particular restrictions on the use of AI systems for 'real-time' remote biometric identification in publicly accessible premises for law enforcement purposes, it is appropriate to base this Regulation, as regards those specific rules, on Article 16 TFEU".

[7] For an understanding of this concept, see Julian Savulescu and Nick Bostrom (eds.), *Human Enhancement*, Ed. Oxford University Press, 2009, p. 18 which starts from the premise: "To what extent should we use technology to try to make better human beings? (...) Human enhancement aims to increase human capacities above normal levels. Many forms of human enhancement are already in use". See also Bakken, Borge, *The Exemplary Society: Human Improvement, Social Control, and the Dangers of Modernity in China*, Oxford University Press, 2000, pp. 12-19, https://EconPapers.repec.org/RePEc:oxp:obooks:9780198295235. Also, Seckington, Ian, *The Exemplary Society: Human Improvement, Social Control and the Dangers of Modernity in China. By Børge Bakken*. [Oxford: Oxford University Press, 2000. xiii 516 pp. ISBN 0-19-829523-5.], in The China Quarterly, 167, pp. 790-791, 2001, doi:10.1017/S00 0944390140043X.

on the legal status of the robot[8] . Man becomes the victim of his own disinterest in the effectiveness of legal regulations. If man will not be able to apply technological improvements on his own person, then he will seek other avenues, including their application on animals. There are theoretical debates on different concepts that refer to technological modification of animals, used indiscriminately and referring to animal enhancement, animal uplift, animal breeding and animal dismemberment[9]. These discussions are not new. They have been going on for over ten years.

In one of my papers in 2022 I strongly proposed that the legal status of animals should be urgently established as similar to the legal status of a minor[10]. Previously, in a 2009 paper, it was analysed that "Given, however, that enhanced intelligence is a benefit to (some) animals, as it is to humans, then the reasons we have for enhancing the intelligence of a human child may also apply to creating similar obligations to enhance these animals. In other words, we have a *prima facie* obligation to enhance both chimpanzee and human."[11]

The robot can be considered an extension of man in several cases, depending on how it is designed, used and integrated into both human activities and its attributes. Starting from manufacturing and industry, robots were initially designed to be extensions of human capabilities that can perform repetitive, dangerous or heavy tasks such as assembly, welding or material handling. It was intended that they could be controlled by humans who could program, monitor and control them in real time, in this case using them as extensions of the human workforce to increase efficiency and accuracy in production processes. This has been followed by the development of the healthcare field, where robots can be used as extensions of the skills and knowledge of doctors and nurses: in minimally invasive operations, such as robot-assisted surgery, where a human surgeon controls a robot to perform complex and precise surgery.

In these situations, robots become an extension of the doctor's hands and skills, allowing them to perform more precise and safer procedures[12]. The third

---

[8] See Cristina Elena Popa Tache, *Vers un droit de l'âme et des bioénergies du vivant*, Ed. L' Harmattan, Collection: Logiques Juridiques, 2022, preface by Jean-Luc Martin-Lagardette, pp. 27-105.

[9] Gayozzo, Piero, *Animal Enhancement, Uplift or Augmentation? Clarifying concepts*, in „International Journal of Social Sciences and Humanities Invention", 8(09), 6542-6547, 2021, https://doi.org/10.18535/ijsshi/v8i09.02.

[10] See the full reasoning in Cristina Elena Popa Tache, *op. cit.*, 2022, pp. 27-105.

[11] Chan Sarah, *Should we enhance animals*, in „Journal of Medical Ethics", 2009 Nov;35(11):678-83. doi: 10.1136/jme.2009.029512. PMID: 19880704; PMCID: PMC4829097.

[12] In the studies, a fragmented notion of care and a relationship between two independent entities (a man and a machine), but also a more complex understanding of social action and technical-scientific assemblies of care have been reported. Using the notion of interpretive repertoires, we identify two repertoires that are mobilised in citizens' perspectives on robotics: a repertoire of well-being, associated with inter-human relations and the notion of 'good care', and a repertoire of responsibility, associated with individual and collective responsibility for facilitating the smooth running of the system and guaranteeing care in a context of health pressures. Starting from the mobi-

stage has seen the emergence of robots that can be extensions of skills irretrievably lost by people with disabilities, to help them improve their autonomy and independence. We refer here to people with reduced mobility, especially for some daily tasks such as cleaning, cooking, or interacting with the environment. The fourth stage was the emergence of robots, also used as extensions of human capabilities in space exploration and scientific research, such as remotely controlled space rovers, such as those sent to Mars, which can be seen as extensions of researchers on Earth, extending their ability to explore and study inaccessible environments. Consideration of the legal personality of autonomous systems comes with the question of whether (and if so, under what conditions) these systems should be granted the status of legal subjects, capable of acting in law and/or being held liable in law?[13] Is this possible in the cases mentioned here, or should we consider another legal institution? Would granting legal personality to robots solve the problem of private law liability for damage caused by semi-autonomous systems?

We see that the sophistication of artificial intelligence is increasing and integrating into various aspects of human society. In the context of virtual and augmented reality, robots can be used as extensions of human movements and actions to interact with virtual or augmented worlds. Even a teacher's capabilities can be extended through robots that can be programmed to provide explanations, perform demonstrations or provide feedback, thus extending a teacher or instructor's capabilities in teaching complex concepts or developing students' skills.

Turning to the health and human enhancement side, we find that robots can be used as human prostheses in cases where they are designed and used to replace or supplement a person's lost or impaired biological functions: as prostheses for amputated limbs such as arm, hand, leg or lower leg prostheses, controlled via electrical signals generated from the remaining muscles or nerves, allowing the amputee to regain certain functionalities and improve their quality of life. Robots can be used as prostheses for people with motor impairments, such as paraplegia or tetraplegia, which can be controlled by electrical signals from the brain or other parts of the nervous system, so that those affected by various motor impairments can regain certain movement abilities and have greater autonomy in

---

lisation of different interpretative repertoires by citizens, robots are virtual entities that acquire different meanings through the debates around them. These analyses are extensively presented in Vallès-Peris N, Barat-Auleda O, Domènech M., *Robots in Healthcare? What Patients Say*, in „International Journal of Environmental Research and Public Health", 2021, Sep 21;18(18):9933, DOI: 10.3390/ijerph18189933, PMID: 34574861; PMCID: PMC8466583. Also see details in Gilbert G.N., Mulkay M., *Opening Pandora's Box: A Sociological Analysis of Scientists' Discourse*, Cambridge University Press; Cambridge, 1984, p. 75 et seq.

[13] Hildebrandt, Mireille, *Legal Personhood for AI?, Law for Computer Scientists and Other Folk* (Oxford, 2020; online edn, Oxford Academic, 23 July 2020), pp. 237-250, https://doi.org/10.1093/oso/9780198860877.003.0009; and Bryson, Joanna J., Mihailis E. Diamantis, and Thomas D. Grant., *Of, for, and by the People: The Legal Lacuna of Synthetic Persons*, „Artificial Intelligence and Law", 25 (3) 2017, pp. 273-291, https://doi.org/10.1007/s105 06-017-9214-9.

everyday activities. In the presentation, we will also look at robot prostheses that can be applied to animals. Such prostheses include: hearing and visual prostheses, such as: cochlear implants for people or animals with hearing impairments or artificial eyes for people (or animals) with visual impairments; or cognitive prostheses for people or animals with cognitive impairments, such as neurological conditions or traumatic brain injury.

These robotic prostheses for human or animal use are still in the development and research phase, but this does not mean not creating regulatory levers now for when they all become widely available and accepted in medical and social practice. As one author relatively recently put it, "But why stop at restoration? Motors in prosthetics can be more powerful than human muscles; indeed, a major goal of exoskeleton research is to develop exoskeletons that greatly enhance human capabilities"[14]. Indeed, robotic prostheses raise ethical and legal issues arising from the sensitive boundary between therapy and enhancement, an issue that arises in philosophical debates and underpins policy and regulation. Academic debates have noted a distinction between *restitutio ad integrum* (the reconstitution of human integrity) and *transformatio ad optimum* (the reformation of the human being in a better way)[15]. The question remains: how will it be possible for humankind to be ready for such a completion and enhancement of its personality if even today humans do not have a regulation regarding the ownership of their own body?

The law (rights) concerning the human body in particular is studied in major university centres in the form of courses[16]. Different national legal systems have developed legal rules governing the transfer of organs or other tissues taken from human bodies, which are similar in part. Despite intensive studies, if we proceed to analyse our own national system, each with its own law, we will find that we will not find a clear provision stating that the individual has ownership of his own body in the full sense of: *jus possidendi, jus utendi, jus fruendi, jus abutendi*. We will note that, for example, we find few countries where the individual can fully decide what to do with his body, such as the case where his suffering is

[14] Ronald Leenes, Erica Palmerini, Bert-Jaap Koops, Andrea Bertolini, Pericle Salvini & Federica Lucivero, *Regulatory challenges of robotics: some guidelines for addressing legal and ethical issues*, „Law, Innovation and Technology", 9:1, 1-44, 2017, DOI: 10.1080/17579961.2017.1304 921. The authors note that some characterizations such as unnaturalness, fairness, unfairness, and dignity overlap with many other considerations, adding complexity to the resolution of such issues.

[15] Federica Lucivero and Anton Vedder, *Human Enhancement: Multidisciplinary Analyses of a Heated Debate* in Federica Lucivero and Anton Vedder (eds.), *Beyond Therapy v. Enhancement? Multidisciplinary Analyses of a Heated Debate*, Pisa University Press, 2014; and Urban Wiesing, *The History of Medical Enhancement: From Restitution Ad Integrum to Transformatio Ad Optimum?* in Bert Gordijn and Ruth Chadwick (eds.), Medical Enhancement and Posthumanity, Springer, 2010, pp. 9-24.

[16] See University of Southampton, available at: https://www.southampton.ac.uk/courses/modules/laws3141, accessed 01.09.2021.

to be ended by active euthanasia: Argentina, Belgium[17], Canada, Chile, Colombia, Denmark, Finland, Japan, Luxembourg, Mexico, South Korea. In other countries, passive euthanasia is allowed (Great Britain, Israel, Germany, Spain, India or Ireland); in Uruguay, for example, "mercy killing" was adopted in 1933.

Most countries prohibit euthanasia; in Romania, for example, euthanasia is punishable by 1 to 5 years in prison and is not allowed. We deduce from this that we have a form of possession over our bodies, but we do not have full ownership, we do not have a *jus utendi* and neither do we have a *jus abutendi*. Even today there is not enough regulation of what is meant by ownership of the body, the right to dispose of this property and its control. Many questions remain. At the international level, regulations could be subject to human rights or the rights of nature, but at the level of national law, nothing prevents the process of adequate regulation of everything that is a form of life, and here we note how certain legal concepts discussed and treated as modern legal controversies are lagging behind others such as those that are the subject of our theory. Experts remain of the opinion that the development of clear legal principles is necessary to protect the rights of individuals, referring in particular to the use of these materials in medical research[18].

Despite the existence of regulations in the domestic law of some countries, they do not contain sufficient detail to distinguish the set of rights that the person himself may have over his body. We have mentioned that dictionaries have begun to include in the definition of the natural person details such as the fact that legal systems can attribute rights and duties to natural persons without their express consent (in Cornell Law School), and that this concept extends in some legislation to the whole of nature and animals, in particular their protection. This is also where the danger of non-regulation lies. These issues have the potential to trigger certain fears and lead us to consider the concept of quasi-slavery.

World dictionaries define slavery as the human condition of people (slaves) who work for a master without pay and *have no rights over their own person*. Therefore, what substantially differentiates the free man from the slave is having rights over his own person. By an exercise in legal logic, it follows that

[17] In Belgium, this right has been legalised by Parliament since 2002. For minors suffering from terminal illnesses, the Senate extended the law in 2013. The child's parents and a medical team must make a request in such cases. The first minor was euthanised under this law in Belgium in 2016.

[18] For a comparative analysis of some systems of law on these issues, see Rohan Hardcastle, *Law and the Human Body. Property Rights, Ownership and Control*, ed. Hart Publishing, 2007. The analysis demonstrates that, although property rights and other matters relating to human tissue (the legal regime of human body parts is dealt with here) are recognised in limited circumstances, no principled basis (in common law or by statute) for the recognition of these rights and interests has been accepted. These observations have also been developed in my book: *Vers un droit de l'âme et des bioénergies du vivant*, Ed. L'Harmattan, Paris, 2022, Collection: Logiques Juridiques. Render also observed that the doctrine has criticized the distributive consequences of a regime in which we cannot - at any point in our lives - "own" our own bodies (or its constituent parts), but other persons can, and therefore what has been missing is a conceptual basis for understanding the living human body as property.

not to have freedoms over one's person is to be free and different from a slave, but only to have rights. Slavery has also been defined as "a state of total political, social and economic dependence in which a country, a social group or an individual is held[19]". The Slavery Convention, signed in Geneva on 25 September 1926, which entered into force on 9 March 1927, contains the following definition: "1) Slavery is the status or condition of a person over whom any or all of the powers attaching to the right of ownership are exercised".

In reality, to take away someone's rights is to take away their freedom, an assumption that cannot be formulated in reverse: taking away someone's freedoms cannot mean taking away their rights because rights did not exist *ab initio*. Freedoms have a lower legal status than rights. As there is no law without institutions, scholars have argued that law is *de facto* a system of rules and that the creation and implementation of these rules regulating a certain behaviour is achieved through social or governmental institutions[20].

3. The human person through the lens of the world's religions in general

The vision of the human being can be said to have been tried in all religions and traditions of the world. Hinduism, Buddhism, Confucianism and Taoism have been observed to have in general common the human person as a social being endowed with a spiritual element - a soul - and open to transcendence and in harmony with the natural environment, perceptions which have generated to this day values or models of good behaviour, hence a certain legal custom given by certain aptitudes but also by the possibility of acting morally. Domènec Melé and César González Cantón have noted very well that the three great Abrahamic monotheistic religions - Judaism, Christianity and Islam - share the belief that the human being has a spiritual soul and that there is only one God, the personal Supreme Being and Creator of the universe. Thus, the human being is seen as dependent on God, but endowed with free will, the capacity for moral discernment and responsibility[21]. Without entering into the detailed realm of these debates, we will try to extract the necessary essence of our arguments and observations. An interesting appropriation of Islam is that all people are understood to be

[19] *Explanatory Dictionary of the Romanian Language*, Romanian Academy, Ed. Univers Enciclopedic, 1998 edition.
[20] Geoffrey Robertson (Author), Kenneth Roth (Introduction), *Crimes against humanity: The Struggle for Global Justice*, revised and updated edition, Paperback - January 31, Ed. New Press, 2007, p. 90.
[21] Domènec Melé and César González Cantón, *Views of the Human Being in Religions and Philosophies*, in: Human Foundations of Management, IESE Business Collection. Palgrave Macmillan, London, 2014, pp. 68 ff., https://doi.org/10.1057/9781137462619_5.

born Muslims and that it is the (cultural) environment that changes their essentially Muslim nature into "something else"[22]. If the cultural environment can shape human nature, then we have a different perspective, in which more possibilities can arise proportionally equal to the possibilities that society can confer, including through technological developments. This view is complemented by the views of other theorists who have observed that Advaita Vedanta, Vaishanava Hinduism, Buddhism, Abrahamic faith and materialist faith present humans as complex material organisms[23]. Or, can adaptation to the characteristics of robots fall within this sphere of complexity?

Each of these religions has proposed rules of conduct, with a well-defined set of minimum standards and virtues necessary for good behaviour. Monotheistic faiths: In monotheistic religions, such as Christianity, Islam and Judaism, the human person is often considered a creation of one God and is seen as a unique and special being created in the image or likeness of God. The human person is considered to have a soul and is often subject to moral and ethical rules established by God.

Polytheistic religions, such as Hinduism, Greek mythology or indigenous religions, consider that this concept of the human person can be more diversified. The human person can be seen as an individual being with his or her own abilities, but can also be related to a system of deities, spirits or divine entities that can have influence over human life and destiny. It is useful to bear in mind that Buddhism, Taoism or Hinduism see the human person as a complex being, made up of different levels of consciousness and energy. The concept of self and identity is explored in depth, and the individual can be seen as an entity in search of enlightenment and liberation from the cycle of rebirth. We can see that traditional and cultural religions and beliefs see the human person as being able to play an important role in community and society. Religious values and practices can be closely linked to the daily life of the human person, such as rites of passage, family ceremonies, healing practices or the relationship with ancestors and nature.

These categories may vary according to the specific interpretations and practices of different religions and cultures, and this is a general description of how the human person may be understood in a religious context in various world religions. None of these views took into account the emergence of robots. The question is: given that the majority of the world's population belongs to the three major religions, how will they perceive the artificial creation called robot? Is there any real possibility of limiting the robot to the status of a mere tool? If so, then how will this quality be applied if the robot is absorbed by the human person as an extension of him or her, or if it is used in a way that exceeds these limits?

The debates and arguments on the recognition of robots as natural or legal persons are complex and varied. Among the "pro" arguments are: the ability of

[22] On *Human Nature, Religious and Philosophical Aspects*, in Encyclopedia of Science and Religion, accessed March 23, 2023 at: https://www.encyclopedia.com.
[23] Ward, Keith, *'Introduction', Religion and Human Nature*, Oxford, 1998, pp. 8,9.

robots to have consciousness, intelligence, emotions and autonomy; the possibility of robots developing a form of autonomy and moral responsibility, which would lead to rights and obligations similar to those of human beings; and the potential of robots to actively contribute to society through their work, innovation and other forms of social participation, an argument for their recognition as natural persons with rights and privileges.

Conversely, the "against" arguments claim: the absence of real consciousness and autonomy in robots; the risk of creating confusion regarding the legal and moral status of robots, as they do not have the same characteristics and attributes as human beings; and the potential negative consequences of recognising robots as natural persons, such as legal and moral responsibility for their actions, or the possibility of being subject to excessive restrictions or obligations.

If we consider the granting or recognition of a legal personality, then we will have at the centre of the debate some elements such as: Recognition of robots as legal persons could facilitate the proper regulation and protection of their interests and the attribution of legal responsibility for their actions; the ability of robots to own property and enter into contracts; the potential of robots to contribute to the economy and technological development; the fact that robots have no real consciousness, emotions or autonomy - issues that affect their recognition as legal persons inadequately; the risk of setting a dangerous precedent by granting legal rights and privileges to artificial entities; the potential abuses and exploitation that could arise from recognising robots as legal persons, such as using them for commercial purposes without respecting their rights or welfare.

Perspectives on recognising robots as individuals or legal entities vary according to the cultural, social, ethical and legal context of each society: some cultures and communities may be more open to the idea of recognising robots as individuals or legal entities, while others may be more reserved or reject the idea altogether.

However, the crux of the debate, on which it would be interesting to have more research, is: from a religious point of view, can man be creative and what would be the limits allowed by the Bible, for example?

Without delving into the religious rules of each religion, we will note that man, as God's creation, has the power of creation. The Bibles are full of examples where man builds settlements, works the land or performs various activities[24] . Technology is just another activity to enhance our spiritual evolution, it is a new challenge that man must treat with respect for people, nature and the whole universe from the design phase. There is no religious text that imposes any limits on

[24] The Orthodox Bible contains several texts in which people do various works. For example: "the son of a widow of the tribe of Naphtali and a father of Tyre, who worked in the Aramaic. Hiram was full of wisdom, skill and knowledge in doing all kinds of plowing work. He came to Emperor Solomon and did all his work for him" (1Ki.7:14): or "and he made some braids in the form of a net, and some tassels made with staves, for the roofs on the top of the posts, seven for the first roof, and seven for the second roof (1Kings 7:17)".

the power of creation other than observance of the "commandments". In other words, man is free to create unlimitedly because that is his structure, but he must respect the divine laws, i.e. those perceptions that require him to behave honestly. We will note that all these rules provide for divine punishments if man has done what is universally evil.

Of all the evils the creation of idols seems to be the greatest. We understand from this that from a religious point of view, under no circumstances and never, should a robot have an "idol" status. By following this path, man can directly create inspired by his divine power and can access these capacities mostly for the common good, based on that principle of utilitarianism of not being harmful. Recall that Jeremy Bentham (1748-1832), the English jurist and philosopher considered the founder of utilitarianism, and an ardent promoter of major legal reforms in 18th century England, sought to transform law into an empirical science, not focused on philosophical speculations about natural rights and other appealing fictions, but oriented towards enhancing public happiness[25].

4. A robot: what is a robot, what is a robot?[26]

In high school I was called a "cyborg" because I was strong and legal in my actions, like a robot. I've been called a robot, but I'm not, I'm human. The word human comes from the Latin word humus, which means earth, which represents one of the five main elements, and the science that studies humanity is called anthropology, another word, in Greek this time, which means an thropos - looking at the sky, man who seek their Creator, God. *Fecisti nos ad Te Domine et inquietur est cor meum donec requiecat in Te.* (Blessed Augustine)

The main problem of this research came to my mind during the Law of Communication and New Technologies class, when my teacher told us that in the European Union there is a current topic of discussion in favor of the case where a robot, as an intelligence artificial entity can be called a natural or legal person.

My thoughts flew back then, 20 years ago at the Faculty of Theology when I spoke and discussed the concept of Person, which is a topicality in this age, when the word and concept of person are depersonalized, because we humans do not have clearly in mind that we are God's creation, we are the image of our God, we are the likeness of God.

We are called by name - Basil - and we respond to God's call, we received that name at our baptism, we are meant to be gods by grace, not by being (essence). We are created by God through triune counsel, not like God's other creations, through the word: "Let it be". When God created man he looked at His Son,

[25] See Monica Florentina Popa, *What the economic analysis of law can't do - pitfalls and practical implications,* in „Juridical Tribune - Tribuna Juridica", Volume 11, Issue 1, March 2021, pp. 81-94.

[26] This chapter reflects the opinion of the author M.V. Bârdan who is an Orthodox monk priest and law student. The exposition is personalized to add originality, ethos and realism to this material.

Jesus Christ, and we all have the image of Christ, whether we believe it or not, we are created by the same God, regardless of creed, skin color or nation, the image of God in man it represents: reason, will, feeling and freedom, and the resemblance to God is in a continuous dynamic, through a participation in God's grace. Through our good, beneficial, unconditional actions, through the fact that we give birth to children, we become gods, taking part in the creation of the world, which has not stagnated, God is not a Deus absconditus. The creation of a robot is a production, it is a "counsel between men", not a council between God and men, as in the creation of a man, for example. The true birth of a human being is done by the child's mother and father together with God, without selfish reasoning as a foundation. When we are selfish, we take God out of the equation of life. Believe it or not, we are created by God himself with *humus*, but we are *anthropos*.

A robot has no freedom. A man has freedom and has the attribute of God's existence in him, that is, Self-Existence, but without dependence on anyone. God exists.

I don't think there is any religion - *modus cognoscendi et deum*[27] that is about robots. However, the reality remains that laws are either derived from social traditions or from the dominant religion in society and both are identified from the dominant social culture[28] .

5. Conclusions

The debates remain complex and controversial**.** This is an issue that will continue to be explored in the future as technology and society evolves, and requires careful and balanced legal regulation to ensure the protection of the rights and welfare of both humans and robots. One of the arguments for recognising robots as natural or legal persons is that they can be created with advanced artificial intelligence, allowing them to have cognitive and emotional abilities similar to humans. If we think about the significant impact on the economy and society in general, and the contribution of robots to production, services, research and innovation, then we can also imagine the hypothesis that they could be subject to legal rules and responsibilities, such as paying taxes, complying with regulations and protecting consumer rights. Certainly, complex legal issues have already

[27] The expression belongs to Vicentiu de Lerin.

[28] Mohammad Ali Mahdavi Sabet, Sajjad Mazloumi, *Bio-ethical principles of medical law with an emphasis on the law of Iran*, in „Juridical Tribune - Tribuna Juridica", Volume 6, Issue 2, December 2016, p. 322. The authors conclude in their study: "Therefore, religious principles and guidelines define the solutions to medical ethical dilemmas, and valid legal sources underlie the legislation. But two things are noteworthy, the first is that contemporary scholars will comment on some issues where circumstances require a revision of past procedures, with respect for the principle of nonharm and the philosophy of utilitarianism which means that an action must be totally useful and have positive results and not be harmful to the body or mind."

been opened up, such as legal liability for damages, safety and security regulations, and intellectual property rights over innovations created by robots.

The question of whether a robot could be considered a person raises various ethical, philosophical, legal and technical issues. At present, robots are not recognised as persons, but are treated as objects or property from a legal perspective. Of course, we can consider some technological developments so significant that in the future, a robot could be considered a person if it had a form of consciousness and autonomy similar to that of humans, namely if it had the ability to feel, to have intentions, to exercise its will and to choose its own actions, if it had advanced cognitive abilities, such as abstract thinking, complex problem solving and decision making based on values and principles, or, if we go further in our imagination, if the robot had the right to legal protection, property, privacy and other fundamental rights, but was also subject to legal responsibilities such as compliance with laws and regulations[29].

Ultimately, it is possible that the similarities and differences between humans and robots underlie these types of legal regulations[30]. However, the human person remains the true creator, a biological being, with a complex and varied nature, while robots are artificial, human-made creations, each with a specific design and functionality, operating on the basis of programmes and instructions set by humans, without having an ethics or morality of their own. The personality of a robot refers to the distinct characteristics, behaviours and traits it displays in its interaction with its environment and with humans.

In conclusion, man without robot is possible, while robot without man remains impossible.

Bibliography

1. Bakken, Borge, *The Exemplary Society: Human Improvement, Social Control, and the Dangers of Modernity in China*, Oxford University Press, 2000, https://EconPapers.repec.org/RePEc:oxp:obooks:9780198295235.
2. Bryson, Joanna J., Mihailis E. Diamantis, and Thomas D. Grant., *Of, for, and by the People: The Legal Lacuna of Synthetic Persons*, „Artificial Intelligence and Law", 25 (3) 2017, https://doi.org/10.1007/s105 06-017-9214-9.
3. Chan Sarah, *Should we enhance animals*, in „Journal of Medical Ethics", 2009 Nov; 35(11). doi:10.1136/jme.2009.029512. PMID: 19880704; PMCID: PMC

[29] There are already examples of regulations that are starting to set some trends. In 2017, the European Parliament adopted a report recommending the creation of a separate legal status for robots, including specific rights and obligations. The following year, the US state of California passed a law requiring a certain degree of ethical autonomy for robots and artificial intelligence systems used in autonomous vehicles. Other jurisdictions and international organisations have also begun to explore the possibility of recognising robots as distinct legal entities.

[30] Both humans and robots have the ability to function autonomously, to make decisions and act according to their environment, to learn from experiences, to adapt to changes in their environment, to interact with the world around them using various modalities such as movement, communication and perception.

4829097.
4. Cristina Elena Popa Tache, *Editorial*, in „International Investment Law Journal", Volume 1, Issue 1, February 2021.
5. Cristina Elena Popa Tache, *Vers un droit de l'âme et des bioénergies du vivant*, Ed. L' Harmattan, Collection: Logiques Juridiques, 2022, preface by Jean-Luc Martin-Lagardette.
6. Domènec Melé and César González Cantón, *Views of the Human Being in Religions and Philosophies*, in: Human Foundations of Management, IESE Business Collection. Palgrave Macmillan, London, 2014, https://doi.org/10.1057/9781137462619_5.
7. *Explanatory Dictionary of the Romanian Language*, Romanian Academy, Ed. Univers Enciclopedic, 1998 edition.
8. Federica Lucivero and Anton Vedder, *Human Enhancement: Multidisciplinary Analyses of a Heated Debate* in Federica Lucivero and Anton Vedder (eds.), *Beyond Therapy v. Enhancement? Multidisciplinary Analyses of a Heated Debate*, Pisa University Press, 2014.
9. Gayozzo, Piero, *Animal Enhancement, Uplift or Augmentation? Clarifying concepts*, in „International Journal of Social Sciences and Humanities Invention", 8(09), 2021, https://doi.org/10.18535/ijsshi/v8i09.02.
10. Geoffrey Robertson (Author), Kenneth Roth (Introduction), *Crimes against humanity: The Struggle for Global Justice*, revised and updated edition, Paperback - January 31, Ed. New Press, 2007.
11. Gilbert G.N., Mulkay M., *Opening Pandora's Box: A Sociological Analysis of Scientists' Discourse*, Cambridge University Press; Cambridge, 1984.
12. Hildebrandt, Mireille, *Legal Personhood for AI?, Law for Computer Scientists and Other Folk* (Oxford, 2020; online ed., Oxford Academic, 23 July 2020), https://doi.org/10.1093/oso/9780198860877.003.0009.
13. Julian Savulescu and Nick Bostrom (eds.), *Human Enhancement*, Ed. Oxford University Press, 2009.
14. Mohammad Ali Mahdavi Sabet, Sajjad Mazloumi, *Bio-ethical principles of medical law with an emphasis on the law of Iran*, in „Juridical Tribune - Tribuna Juridica", Volume 6, Issue 2, December 2016.
15. Monica Florentina Popa, *What the economic analysis of law can't do - pitfalls and practical implications,* in „Juridical Tribune - Tribuna Juridica", Volume 11, Issue 1, March 2021.
16. On *Human Nature, Religious and Philosophical Aspects*, in Encyclopedia of Science and Religion, accessed March 23, 2023 at: https://www.encyclopedia.com.
17. *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 acts*, com/2021/206 fInal.
18. Rohan Hardcastle, *Law and the Human Body. Property Rights, Ownership and Control*, ed. Hart Publishing, 2007.
19. Ronald Leenes, Erica Palmerini, Bert-Jaap Koops, Andrea Bertolini, Pericle Salvini & Federica Lucivero, *Regulatory challenges of robotics: some guidelines for addressing legal and ethical issues*, „Law, Innovation and Technology", 9:1, 2017, DOI: 10.1080/17579961.2017.1304 921.
20. Seckington, Ian, *The Exemplary Society: Human Improvement, Social Control*

and the Dangers of Modernity in China. By Børge Bakken. [Oxford: Oxford University Press, 2000. xiii 516 pp. ISBN 0-19-829523-5.], in „The China Quarterly", 167, 2001, doi:10.1017/S00 0944390140043X.

21. Urban Wiesing, *The History of Medical Enhancement: From Restitution Ad Integrum to Transformatio Ad Optimum?* in Bert Gordijn and Ruth Chadwick (eds.), Medical Enhancement and Posthumanity, Springer, 2010.
22. Vallès-Peris N, Barat-Auleda O, Domènech M., *Robots in Healthcare? What Patients Say*, in „International Journal of Environmental Research and Public Health", 2021, Sep 21;18(18):9933, DOI: 10.3390/ijerph18189933, PMID: 34574861; PMCID: PMC8466583.
23. Ward, Keith, *'Introduction', Religion and Human Nature*, Oxford, 1998.

Adapting Non-Contractual Liability Rules to Artificial Intelligence

Associate professor **Vasile NEMEȘ**[1]
Assistant professor **Gabriela FIERBINȚEANU**[2]

Abstract

Current national liability rules are not adequate to deal with liability claims for damage caused by AI-based products and services. The specificity of AI systems, their complexity and especially their autonomy and opacity (the so-called "black box" effect) make it difficult for victims to identify who is liable and to prove liability claims. The European Commission's AI policies propose a holistic approach to liability, aiming at adaptations of product liability under the Product Liability Directive and specific harmonisation under the Proposal for a Directive on the adaptation of non-contractual liability rules to artificial intelligence. These two initiatives complement each other to form an effective global civil liability system. They respond to the scenarios in which the risks envisaged by the general framework provided by the Proposal for a Regulation laying down harmonised rules on artificial intelligence (AI Act) materialise. This paper proposes a first incursion into the liability frameworks for damage caused by AI systems as set out in the Proposal for a Directive of the European Parliament and of the Council on the adaptation of the rules on non-contractual civil liability to artificial intelligence (the AI Liability Directive).

Keywords: *artificial intelligence systems, burden of proof, holistic liability system, level of harmonization.*

JEL Classification: K15, K24, K33

1. Background and objectives of the Proposed Directive

The objective of the proposal is to promote the implementation of a trusted AI in order to reap its full benefits for the internal market, ensuring that victims of AI injuries obtain protection equivalent to that afforded to victims of product injuries in general. The issue of AI systems is not a recent concern at EU level. In the White Paper on AI of 19 February 2020[3], the European Commission

[1] Vasile Nemeș - Faculty of Law, „Nicolae Titulescu" University of Bucharest, Romania, nemes@nemes-asociatii.ro.
[2] Gabriela.Fierbințeanu - Faculty of Law, „Nicolae Titulescu" University of Bucharest, Romania, gabriela.fierbinteanu@gmail.com.
[3] White Paper "Artificial Intelligence - A European approach focusing on excellence and trust", 19.2.2020, COM(2020) 65 final.

addressed the risks of using such systems by elaborating, in the AI Liability Report[4], on the challenges of AI for existing liability rules. The public consultation that underpinned the impact assessment of the proposal also confirmed stakeholders' views, on the difficulty of applying tort principles in actions concerning damage caused by AI systems, due to the specificity of their behaviour. Why does such intervention become necessary in practice? At EU level the EU liability frameworks have worked well. They are based on the application of the Product Liability Directive (Directive 85/374/EEC), which harmonised producer liability for defective products, and on non-harmonised national liability regimes.

The Product Liability Directive provides a level of protection that could not be ensured by national fault-based liability provisions alone. It introduces a system of strict liability of the producer for damage caused by a defect in his products. In the case of physical or material damage, the injured party is entitled to compensation provided that he proves the damage, the defect in the product (the fact that it did not provide the safety that consumers could expect) and the causal link between the defective product and the damage. The non-harmonised national regimes provide for fault-based liability rules under which, in order for a claim to be accepted, the victim of the damage must prove the fault of the person responsible, the damage and the causal link between the defect and the damage.

At national level, there are also strict liability regimes under which the legislator assigns liability for a risk to a specific person, without the need for the victim to prove fault/defect or the causal link between fault/defect and the damage. Under national liability regimes, victims of damage caused by products and services may submit several claims for compensation in parallel, based on either fault or strict liability. Often these claims are brought against different liable persons and under different conditions. The victim of a car accident may, for example, rely on strict liability against the owner of the car, fault-based liability against the driver, and will be able to claim compensation from the manufacturer under the Product Liability Directive if the car was defective. However, the characteristics of emerging digital technologies such as AI have raised questions about some aspects of national and EU liability frameworks. Some features could complicate the detection of the causal link between the injury and human conduct on which a fault-based claim should be based under national rules, making it difficult and costly to provide evidence to support claims. If we consider an autonomous cleaning robot operating in a public space and injuring a person, it becomes difficult to prove fault, unlike if a cleaning device were handled by a human operator. An accident of this type can have numerous causes such as, an image segmentation error by the robot's artificial intelligence based perception system, a failure of the intelligent vision component vendor to provide an available software update or a failure of the user (cleaning company) to install it, a failure of

[4] Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee on the safety and liability implications of artificial intelligence, the internet of things and robotics, 19.2.2020, COM(2020) 64 final.

the remote human operator to properly monitor the operation of the robot or even a deliberate jamming of its system. In order to substantiate the claim, however, the victim will need to establish the relevant actions/actions or, given the autonomous mode of operation of the robot as well as the opacity and complexity of the various artificial intelligence components, this process may prove extremely difficult. Assuming that guilt can be established, proving the causal link between the act and the injury will require decoding the information and reactions of the AI system, and it is unlikely that a clear causal link can be inferred between these technical elements and the injury caused[5].

The situation becomes even more difficult if the algorithm regarded as the main suspect in causing the damage has been modified by an AI system built on machine learning techniques. In all of these examples, the requirements embedded in such AI systems, designed to drive the management of data collection and analysis and not least, decision-making, appear not to be simple to understand, often requiring analysis that can be costly[6]. There is thus a risk of inadequate compensation, or it is important that victims of accidents caused by products and services incorporating emerging digital technologies, such as AI, are afforded a level of protection that is no less than that offered for other similar products and services for which they would obtain compensation under national tort law, otherwise there is a risk that emerging technologies will be less accepted by users. In addition, if the challenges to national liability frameworks were to be solved at national level only, the fragmentation of national legal regimes would increase, which would increase the cost of bringing innovative AI solutions to market.

There is also a need to ensure predictability for businesses, which need to know the liability risks they are exposed to throughout the value chain, be able to mitigate or prevent them and effectively insure against them. Consequently, this legislative intervention should not be seen in isolation, but as part of a package of complementary measures which also includes the legislative proposal for horizontal rules on artificial intelligence systems (the AI Act)[7] and the proposal for a Directive on product liability[8] (the latter also revising Council Directive

[5] Ada Lovelace Institute (2022), *AI liability in Europe: anticipating the EU AI Liability Directive*, available at https://www.adalovelaceinstitute.org/wp-content/uploads/2022/09/Ada-Lovelace-Institute-Expert-Explainer-AI-liability-in-Europe.pdf.

[6] See Expert Group on Liability for New Technologies. (2019). *Liability for Artificial Intelligence*. European Commission, available at https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=63199.

[7] Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) (COM(2021) 206 final).

[8] Proposal for a Directive Of The European Parliament And Of The Council on product liability (COM(2022) 495 final).

85/374/EEC[9]). In relation to civil liability only, an injured person will thus be able to claim damages under contractual liability or non-contractual liability which does not relate to the defectiveness of a product, e.g. latent defect liability or fault-based liability, in the latter case, the present legislative proposal establishing common rules on disclosure and burden of proof in the context of fault-based claims for damages caused by an AI system.

2. Introduction to the architecture of the Proposed Directive

As stated in the explanatory memorandum accompanying the proposal, the direction of action envisaged is phased, the first of these steps preferring to achieve the objectives through a minimally intrusive approach, limited to the use of relative legal presumptions in the context of the approach to reduce the burden of proof. However, in order not to hamper innovation, the option of reducing the burden of proof was not chosen. The second step, retained by the proposal in the form of Article 5 of the proposal (Specific assessment and review) aims at assessing the adequacy of strict liability rules for claims for damages against operators of certain AI systems, as long as they are not already covered by other Union liability rules, and the need for insurance cover, while taking into account the effect and impact on the introduction and take-up of AI systems, in particular for SMEs.

The scope concerns non-contractual civil law claims for damages caused by an AI system, where such claims are brought under fault-based liability regimes[10]. The Directive does not define concepts such as "fault" or "damage", since the determination of the extent of their meaning is a matter for national regulatory systems, the meaning established by these rules varying from one Member State to another. Being constructed as an instrument aiming at minimum harmonisation, the text allows claimants affected by damage caused by AI systems to invoke more favorable rules of national law. According to Article 1(3), the proposal does not affect the rules of Union law governing the conditions of liability in the field of transport or the rights that an injured person may have under national rules implementing Directive 85/374/EEC. The definitions used by the Directive in Article 2(1) to (4) (AI system, high-risk AI system, provider and user respectively) are referred to the provisions of the AI Act for consistency. Claims for compensation may be brought, in accordance with Article 2(6)(a) and (b), by the person injured by an outcome of an IA system or by the failure of such

[9] Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products (OJ L 210, 7.8.1985, p. 29).

[10] See Karner/Koch/Geistfeld, „Comparative Law Study on Civil Liability for Artificial Intelligence" 2021, https://op.europa.eu/ro/publication-detail/-/publication/8a32ccc3-0f83-11ec-9151-01aa75ed71a1.

system to produce an outcome where such an outcome should have been produced, and by the person who succeeded or subrogated to the rights of the injured person under the law or a contract. In order to allow victims of damage caused by AI systems to exercise their rights in relation to this Directive through representative actions, Article 6 amends Annex I to Directive (EU) 2020/1828[11].

In order to achieve the objective of the proposal, as also noted in its preamble (recital 16), access to information on certain high-risk AI systems suspected of being the element causing the damage is an important factor in determining whether compensation should be claimed and it is therefore appropriate to introduce rules on the disclosure of relevant evidence by those in possession of it for the purpose of establishing liability. Thus, Article 3(1) of the Directive provides that a court may order the disclosure of relevant evidence in relation to certain high-risk AI systems which are suspected of having caused damage. Requests for disclosure of evidence are addressed to the provider of an AI system or a person subject to the provider's obligations under the AI Act. The court, according to paragraph 4 of the said rule, may order such disclosure only to the extent necessary and proportionate to support the claim for compensation. Courts shall take into account the legitimate interests of all parties, including third parties concerned, in particular with regard to the protection of trade secrets within the meaning of Directive (EU) 2016/943[12] and confidential information, such as information related to public safety or national security. But why are we only talking about high-risk systems? Limiting disclosure of evidence in relation to high-risk AI systems is aligned with the provisions of the AI Act, which has retained specific documentation, record-keeping and information obligations for operators involved in the design, development and implementation of such systems. Such consistency also ensures the necessary proportionality, avoiding situations where operators of lower or no risk AI systems would have to document information to a similar level as required for higher risk AI systems. Given the complexity and opacity of the new digital technologies, victims may find themselves in a weaker position to establish causation than in other tort liability scenarios, where the actions that led to the injury may be easier to analyse, but courts were identifying ways to ease the burden of proving causation if the plaintiff's position is considered weaker than in typical cases, even before this proposition arises[13].

What is involved in activating the relative legal presumption of causation in cases of fault? National courts presume, for the purpose of applying liability rules in a claim, causation between the defendant's fault and the result produced

[11] Directive (EU) 2020/1828 of the European Parliament and of the Council of 25 November 2020 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC, OJ L 409, 4.12.2020, p. 1-27.

[12] Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against unlawful acquisition, use and disclosure, OJ L 157, 15.6.2016, p. 1-18.

[13] See CJEU, Case C-621/15 Sanofi Pasteur, ECLI:EU:C:2017:484.

by the AI system or the inability of the AI system to produce a result, if all the following conditions are met: the plaintiff has proved, or the court has presumed, the fault of the defendant or of a person for whose conduct the defendant is responsible, consisting of a breach of a duty of care laid down in Union or national law directly designed to protect against the damage caused; it can reasonably be considered likely, based on the circumstances of the case, that the result produced by the AI system or the inability of the AI system to produce a result was influenced by fault; the plaintiff has proved that the result produced by the AI system or the inability of the AI system to produce a result gave rise to the damage. It should also be noted that where, according to the legislative proposal, the defendant does not comply with an order issued by a national court in a claim for damages to disclose or preserve evidence available to it, the national court will presume a breach of a relevant duty of care by the defendant. Thus, in the case of a claim for compensation in relation to a high-risk AI system, a national court will not apply the presumption if the defendant demonstrates that the claimant has reasonable access to sufficient evidence and expertise to prove the causal link. In the case of a claim for compensation in relation to damage caused by a non-high-risk AI system, the presumption will apply only if the national court considers it excessively difficult for the claimant to prove the causal link. As can be seen, the proposed approach does not imply a reversal of the burden of proof, according to which the victim no longer bears the burden of proof and the person liable bears the burden of proving that the specific conditions for liability are not met. Such a categorical step has been ruled out to avoid exposing providers, operators and users of AI systems to greater liability risks, which could hamper innovation in AI-based products and services.

3. Instead of conclusions

In order not to anticipate, given the recent publishing of the proposed Directive but at the same time to optimistically highlight the impact of the legislative initiative, we paraphrase its very recitals, considering that the proposed adaptations have the potential to contribute to increasing societal and consumer confidence, promoting the introduction of AI and at the same time ensuring a robust legal framework that has the vocation to guarantee that victims of damage caused with the involvement of AI will receive the same effective compensation as victims of damage caused by other technologies.

Bibliography

1. Ada Lovelace Institute (2022), *AI liability in Europe: anticipating the EU AI Liability Directive*, available at https://www.adalovelaceinstitute.org/wp-content/uploads/2022/09/Ada-Lovelace-Institute-Expert-Explainer-AI-liability-in-Europe.pdf.
2. CJEU, Case C-621/15 Sanofi Pasteur, ECLI:EU:C:2017:484.

3. Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products (OJ L 210, 7.8.1985, p. 29).
4. Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against unlawful acquisition, use and disclosure, OJ L 157, 15.6. 2016.
5. Directive (EU) 2020/1828 of the European Parliament and of the Council of 25 November 2020 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC, OJ L 409, 4.12.2020.
6. Expert Group on Liability for New Technologies (2019). Liability for Artificial Intelligence. European Commission, available at https://ec.europa.eu/newsroom /dae/document.cfm?doc_id=63199.
7. Karner/Koch/Geistfeld, "Comparative Law Study on Civil Liability for Artificial Intelligence" 2021, https://op.europa.eu/ro/publication-detail/-/publication/8a3 2ccc3-0f83-11ec-9151-01aa75ed71a1.
8. Proposal for a Directive of the European Parliament and of the Council on liability for defective products (COM(2022) 495 final).
9. Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) (COM(2021) 206 final).
10. Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee on the Safety and Liability Implications of Artificial Intelligence, the Internet of Things and Robotics, 19.2.2020, COM(2020) 64 final.
11. White Paper "Artificial Intelligence - A European approach focusing on excellence and trust", 19.2.2020, COM(2020) 65 final.

Artificial Intelligence and the Legal Responsibilities in Public Financial Administration

Associate professor **Olga SOVOVA**[1]
Associate professor **Zdenek FIALA**[2]

Abstract

New digital technologies, especially tools for gathering information about persons and legal entities, are inevitable in modern public administration. State financial services and the tax administration represent one of the most critical parts of the administrative bodies, creating vast databases of personal and economic data. The exploitation of various software tools, including artificial intelligence for collecting, grouping and evaluating data sets, poses questions about the legal responsibility of the public administration when using such efficient but also assailable tools to intrude into personal and business privacy and space. The paper examines the new trend in the European Union for utilising digital technologies for public financial services. Based on the Czech tax control experience, the paper highlights the procedure's possible risks and weak spots. The paper points out possible benefits both for addressees and public authorities. The paper focuses on the responsibility of the public authority for the accuracy, completeness, and protection of registered data. The authors underline the specifics of the legal responsibility for introducing artificial intelligence into state financial services. The paper concludes with business and legal practice proposals when interacting with public financial administration. The authors examine the mentioned challenges through desk research and analyses of European and national legal regulations. In their considerations and proposals, the authors also lean on their practical experience with public administration.

Keywords: *financial administration, digitalisation, artificial intelligence, privacy, legal responsibility.*

JEL Classification: K24, K34

1. Introduction

The 21st century-called very often the century of the global information society and new technologies- brought in the last decade the need for new approaches in public administration.[3] The mentioned period, especially the SARS-COVID-19 pandemic and current disruptive times, needed and still requires an

[1] Olga Sovova - Police Academy of the Czech Republic, sovova@polac.cz.
[2] Zdenek Fiala - Police Academy of the Czech Republic, fiala @polac.cz.
[3] Sovová, O., Fiala, Z. *Challenges of Public Administration in the Global Digital Era*, in Cazala, J., Zivkovic, V. (eds.), *Administrative Law and Public Administration in the Global Social System* (Contributions to the 3rd International Conference „Contemporary Challenges in Administrative Law from an Interdisciplinary Perspective", October 9, 2020, Bucharest). ADJURIS - International Academic Publisher, Bucharest, Paris 2021, p. 138–146, available online at: http://www.adjuris.ro/editura_en.html, accessed March 4, 2023.

entirely new approach to communication between the public administration and its addressees.

State financial services, which create funds for state functions and accomplish the tasks of the modern European welfare state, should be on the top for up-to-day state services. Taking into consideration the general requirements of the European Union (EU) principles, as well as the national regulation in one of the EU member states- the Czech Republic - and the professional experience, the authors argue the main challenges of the public financial administration transition into the technology-based, user - friendly and accessible service. The authors focus on the state financial administration using digital technologies and artificial intelligence to evaluate and enforce addresses' obligations.

Remote digital tools and artificial intelligence (AI) increasingly penetrate our everyday life. Many systems work autonomously to a large extent based on machine learning. They generate not just output based on specific instructions but also on formulas they have derived. The consequence is that the behaviour of these systems in some situations cannot be fully predicted or explained by their creator or operator. Therefore, neither is the question of determining who should be responsible for any damage caused by artificial intelligence. Is it supposed to be the author of the software making up the artificial intelligence system that caused the damage? Or should it be the company that created the artificial intelligence product? Or should the user who applied the product in the specific situation where the damage occurred be responsible? Considerations about the responsibility of the so-called electronic person also appeared.

All these development trends represent a considerable challenge for legal practice and science. The paper aims to highlight the possibilities, risks and benefits of technologies the public finance administration uses. The authors argue the necessity of a clear delineation for responsibility when using digital tools and artificial intelligence in public finance services and administration.

2. State financial services and the digitalisation

Automation and digitalisation have become essential parts of financial processes in the private sector in the last decade. The pandemic and the need to speed up remote access and communication significantly helped the onset of digitalisation and the use of AI in the daily management of financial flows and operations. Also, communication with clients, especially in bank services, has moved to virtual reality. The development of smartphones and the entry of a new generation accustomed to the online world and services to the labour and financial markets have accelerated this progression even more.

The requirements for modern technological services, originally intended primarily for the business market, due to the protection of public health during the pandemic and with the onset of the energy crisis and the legislation on measures against the legitimisation of crime proceeds and the war situation at the

borders of the EU, are gradually becoming the standard of public services. The management of public finances, the evaluation of risks, and the collection of taxes and other levies based on public budgets following the principles of the rule of law requires that state bodies also use modern technologies. The state financial authorities need access to relevant data within the national state. They also need to be prepared for cooperation with any other tax and finance authorities in a globalised world. Finally, the state's financial services must be user-friendly and enable domestic and cross-border user access.

Financial public administration and services form an integral part of public administration.

All the requirements for public administration in the rule of law apply to financial administration, too. It is necessary to comprehensively address the use of new technologies and artificial intelligence, including responsibility for their failure or misuse, for the entire public administration. The proponent of all public administration systems will guarantee that the addressees can satisfy their requirements in one place, either in person or by remote access. At the same time, the public administration will have an overview of the addressees' activities without burdening them with excessive bureaucracy. The costs of public administration and its services will decrease.

3. Liability for digitalised services

In general, the legal regulation distinguishes two types of liability: personal liability, where the pest is examined, and objective liability, where the culpability of the responsible person or entity is irrelevant.

The basic principle in establishing liability based on fault across European regulations is that the person who caused the damage is responsible. However, the harmer can exculpate if she proves it was not a culpable act. In such a case, the pest bears the burden of proof.

The usual legal construction is assumed or presumed fault for this liability for damage. Negligence suffices to infer liability.

Thus, for example, the Czech Civil Code, Act No. 89/2012 Coll.[4], in the provisions of § 2911, introduces the presumption of negligence, according to which it is considered that anyone who causes damage to the victim by violating a legal obligation is acting negligently. Furthermore, according to Section 2912 of the Civil Code (CC), if the tortfeasor does not reasonably act as expected from a person of average qualities in private intercourse, she is acting negligently. The presumption of negligence also applies when the tortfeasor exhibits special knowledge, skill or care or undertakes to perform an activity requiring special knowledge, skill or care and does not apply these unique qualities. At the same

[4] English version available online at https://www.cak.cz/assets/pro-advokaty/mezinarodni-vztahy/civil-code.pdf, accessed March 4, 2023.

time, in Section 4 of the CC, it is assumed that every legally capable person has the mind of an average person and the ability to use it with ordinary care and caution and that everyone can reasonably expect this from them in legal dealings. The principle of personal responsibility, culpability with an intentional, direct violation of legal obligations, or negligence forms the core of private law.

As a follow-up to issues related to artificial intelligence, it will therefore be necessary to consider special requirements for the care or supervision of both the user and machine controlled by AI.

A particular legal regulation Act. No. 82/1998 Coll., on Liability for Damage Caused in the Exercise of Public authority by a Decision or Incorrect Official Procedure, provides for damage caused by public administration. Responsibility for the performance of a public administration is an objective liability for the result, regardless of whether it was intentional or negligent. The finding of a specific official as the culprit of the damage is also irrelevant to a victim. The decisive factor is whether the authority or the court establishes an unlawful decision or incorrect official procedure. However, even this type of liability closely links with private law. If the administrative authority does not comply with the claim for compensation or grants it in part, the injured party must sue under civil law.

In each context, the choice of a specific type of responsibility depends on the level of maturity of artificial intelligence and the inputs of a human factor. In general, the more autonomous the artificial intelligence is, the lower the requirements should be placed on its users. While in a non-automated system, the user takes full responsibility, in an automated system where many tasks, functions and operations occur independently of the user's will, the responsibility should shift to the side of artificial intelligence.

Therefore, it is suggested to consider the concept of objective responsibility in the case of fully automated systems. The emphasis on objective liability in the case of the use of artificial intelligence is a consequence of the fact that the injured party will usually not be able to prove the fault of a specific person, who often may not be present, and, therefore, she would not be able to claim compensation.

The report of the Expert Group on Liability and New Technologies[5] proposes that the objective responsibility for specific artificial intelligence systems that are operated in public spaces and can thus cause significant harm should be borne by the so-called operator. The operator should be the person or a legal en-

[5] Bertolini, A., Episcopo, F., *The Expert Group's Report on Liability for Artificial Intelligence and Other Emerging Digital Technologies: a critical assessment*. Cambridge University Press, 2021. Available online at: https://www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/expert-groups-report-on-liability-for-artificial-intelligence-and-other-emerging-digital-technologies-a-critical-assessment/45FD6BB0E113E7C4A9B05128BC710589#, accessed March 4, 2023.

tity who controls the risk associated with the operation of the respective technology. However, the mentioned report mainly focuses on the operation of autonomous vehicles and drones. The report draft also emphasises these general postulates mentioned earlier in European directives. The principle of absolute or objective responsibility should concern artificial intelligence applications. At the same time, however, an approach based on risk management is also applied, aimed at a person who, under certain circumstances, can minimise risks and solve the harmful effects of technology.

4. Proposal for an EU Directive on the tightening of non-contractual liability for culpability in the use of artificial intelligence

From the above, within the framework of personal responsibility, when applying compensation for damage caused by an artificial intelligence system, the injured party will have to prove the fault of the pest. The proposed EU regulation helps her a little through the so-called evidentiary presumption.

In the area of non-verbal liability for fault, the European Commission intends to introduce simplified evidence in connection with artificial intelligence systems. In general, a credible claim of the injured party is assumed. An information obligation to present relevant facts about the system is introduced for the so-called high-risk artificial intelligence systems. Violation of this obligation is associated with using the presumption of fault. However, it needs to be clarified from the draft directive what information should be submitted. Whether all that is relevant to the occurrence of damage or only the information for which the obligation to register them according to the regulation on artificial intelligence arises. The Artificial Intelligence Act - the so-called AI-Act - has yet to be adopted by the EU bodies[6].

In addition to the claimant's credibility, the plaintiff must prove that the defendant probably influenced the "output" of the artificial intelligence system and violated the duty to protect against the damage. The so-called presumption of causality must be proven. However, the presumption relates exclusively to the relationship between fault and results from the system. The standard rules for the burden of proof still apply to decide whether the system caused the damage.

The proposal's effects will largely depend on the general standard of hearing evidence and the regulation of the burden of proof in each EU member state. The pitfalls of such harmonisation are that the legal systems of individual EU member states do not always understand uniformly the terms "causality" and "culpability". Some countries place the problem of proportionality and other in-

[6] Proposal for a Regulation of the European Parliament and the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts. 21.04.2021. Available online at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206, accessed March 4, 2023.

stitutes of attribution in causality or the problem of damage to goods and protective purpose to the concept of culpability. Moreover, the difficulty of the causality test also differs in individual legal systems.

Generally, while the importance of fault liability will decrease as automation progresses, harmonised product liability will increase.

One of the critical questions of the proposal of the AI Liability Directive[7] related to automation is whether software should also be considered a product. According to the draft directive, the software as a cloud service falls under the intended regulation. It is, therefore, not decisive whether the software materialises on a data carrier. At the same time, the software manufacturer's responsibility for updating it is introduced because it keeps the product under the manufacturer's control[8].

In connection with product defects, the proposal further constructs legitimate expectations, emphasising the product's ability to learn and its use by other products. However, the EU bodies must explain the overall approach in more detail.

Artificial intelligence is a tool that allows the processing of large data amounts. AI facilitates repetitive tasks and organises and sorts data collections. Finally, it optimises and speeds up management and control processes. Deep learning AI imitates human work but cannot replace it, especially in creative activities[9]. AI also has no ethical and legal awareness but works based on information fed into it by the creator.

5. Considerations on digital and artificial intelligence - based financial services - a Czech example

Financial administration authorities in EU member states use many digitised databases of taxpayers and other economic entities. The Czech Republic has adopted the Act on the Right to Digital Services No. 12/2020 Coll. This law allows the addressees to perform their activities towards the public administration electronically. Public administration, including financial administration, must ensure the technical conditions, including cloud computing.

The Czech Ministry of Finance offers an open data web as a public service and information. An overview of economic subjects registered in the Czech

[7] Proposal for the Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive). 28.09.2022 Available online at: https://commission.europa.eu/system/files/2022-09/1_1_197605_prop_dir_ai_en.pdf, accessed March 4, 2023.

[8] See Article 4 of the AI Liability Directive Proposal.

[9] Vošalíková, A.: *Jsme připraveni žít s robotem*? „Mlada fronta Dnes", a Czech daily, 29.10.2023, p. 9. Available online at: https://www.idnes.cz/technet/technika/komentar-vosalikova-umela-inteligence-robot-kreativita-hrozba.A230127_173752_domaci_kadlwww.idnes.cz, accessed March 4, 2023.

Republic is available on the websites.[10] The registry is an informative source that displays data from particular registers of the state administration, so-called source registers, in which the data concerned are kept. Furthermore, the user can find financial information about the state budget, state grants or macroeconomics predictions, public procurement, and contracts concluded by the Ministry of Finance.

Robotic technology processes the majority of registered big data. The primary problem is that aggregated data are recorded and processed without their originator being able to influence them in any way. A wrong record can only be corrected if the authority responsible for the entry in the source register cooperates.[11] Sometimes, the data holder needs help finding such a public authority. The Ministry of Finance is thus publishing data for the correctness of which it often could not be responsible.

Thus, whether such registers form an accurate public financial service is questionable. Could artificial intelligence processing the data be liable for faults, even if it has access to source registers? Or, should the published data remain only informative, without any legal binding?

The current information concerning the register of economic subjects explicitly states that the registry is just an information source. However, most accounting systems of business corporations link to this register. Thus, they verify the existence and credibility of a potential business partner in the list of economic subjects and value-added taxpayers. The entrepreneur may lose business opportunities if the public financial service does not work correctly.[12]

If the public administration databases are not connected, should artificial intelligence be able to overcome this error by itself? Does a person have to program it? Is it possible to entrust artificial intelligence with such a learning process that will remove errors that humans have caused in the system?

The taxpayers' evidence, especially of VAT payers, forms the most challenging issues of public financial services. The state financial administration acquires and processes enormous data amounts. The data consist of sensitive personal information about the taxpayer's identity and assets.

The system of tax identification numbers in the Czech Republic differs. Legal entities use their identity business number. The birth identity number (birth ID) identifies persons. Anyone can derive from it a gender and the precise date of birth, including a specific identifier for each Czech citizen or another Czech tax resident. Generally, all public authorities and private entities must protect the birth ID if they need it according to the legal requirements.[13] However, if the

[10] Available online at: https://wwwinfo.mfcr.cz/ares/ares.html.en., accessed March 4, 2023.

[11] See the list of registration authorities. Available online at: https://wwwinfo.mfcr.cz/ares/ares.html.en. Accessed March 4, 2023.

[12] Examples from the author Sovova's attorney's practice.

[13] Article 6 of the Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 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

person is a VAT payer, her tax identity, composed of the prefix CZ and the birth ID, is publicly available in the VAT payers register.[14]

The person can demand the tax authority to get the unique identifier, a computer-generated number.[15] Nevertheless, before the new identification is valid, the tax administration publishes the birth ID. AI could solve this issue. It could transform the birth ID as an identification into a unique identifier during a short period without extra costs and thus help to protect the data according to General Data Protection Regulation.

According to the authors, faults in the mentioned evidence could spoil images of the state and the taxpayers without a proper solution for modern technologies. Deficiencies in the records may result in the taxpayer being considered unreliable. Such a case has both tax, legal and personal consequences. According to Section 106a of the Czech VAT Act, No. 235/2004 Coll., a so-called unreliable taxpayer, is excluded from the quarterly tax return, and her VAT registration could be cancelled for one year. The unreliable taxpayer is a dangerous business partner because the other contractual parties guarantee the VAT levy.

Considering that the EU's new system for the identification of cross-border online payments connected with the mandatory VAT levy should start on January 1, 2024[16], the issues of AI interference and responsibility for any deficiencies must be solved before the CESOP system will be valid.

The authors argue that the legal regulation of maladministration responsibility should be extended to using AI in the execution of state power. The Czech legal regulation in the Act on Liability for Damage Caused in the Exercise of Public Power by a Decision or an Incorrect Official Procedure, No. 82/1998 Coll., creates the necessary prerequisites for the mentioned liability. However, according to the authors' knowledge, the courts have yet to deal with the responsibility for using digital technologies in public or financial administration.

6. Conclusion

Digitalisation has immensely changed financial services, working with the private finance sector's financial flows, risk evaluation, accountant, and tax records. Legislation and case law have ceased to a delay after the technical development.

Regulation). Available online at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN, accessed March 4, 2023.

[14] Available online at https://adisspr.mfcr.cz/adis/jepo/epo/dpr/apl_ramce.htm?R=/dpr/Dph Reg?ZPRAC=FDPHI2%2526poc_dic=2%2526OK=Zobraz, accessed March 4, 2023.

[15] Available online at: at https://www.ey.com/cs_cz/tax/tax-alerts/2021/moznost-pozadat-o-zmenu-dic-fyzicke-osoby/en, accessed March 4, 2023.

[16] Central Electronic System of Payment information, CESOP. Available online at: https://taxation-customs.ec.europa.eu/taxation-1/central-electronic-system-payment-information-cesop_en, accessed March 4, 2023.

However, it must be more questionable whether the public finance services and the administration can withstand the ever-accelerating scientific and technical progress. Bureaucratic apparatus and cumbersome procedures, unfortunately often required by the legal regulation of the public sphere, slow down and often even make it impossible to administer public finance services effectively.

AI allows for gathering extensive data, analysing them, and thus making sound public policy decisions. It is inevitable for public sector organisations to learn about these technologies and develop the necessary skills and competencies to help their organisations stay competitive. AI and other digital technologies are not only tools for public sector organisations to enhance existing capabilities in public administration. The new technologies demand a complete revisit of the existing administrative systems and processes.[17]

The possibilities of digitisation and artificial intelligence, together with the clearly defined accountability of public finance officers, will contribute to the discussion on bringing financial management closer to the requirements of the 21st century.

Given the rapid pace of technical development, creating isolated rules for different automated systems seems unreasonable. The authors consider it more appropriate to apply objective liability in the case of risk to avoid gaps in protection and inconsistencies in assessment. The breach of duty of appropriate care by risk adjustment should always lead to reversing the burden of proof.

Regardless of the above, every rule of law state must also ensure adequate services to those who, for whatever reason, cannot or do not want to use technology when communicating with the state. There must be no discrimination or exclusion from certain services. Otherwise, it would impact human rights and the rule of law as the EU Commissioner for Human Rights D. Mijatović stated: *"artificial intelligence-driven technology is entering more aspects of every individual's life, from smart home appliances to social media applications, and it is increasingly being utilised by public authorities to evaluate people's personality or skills, allocate resources, and otherwise make decisions that can have real and serious consequences for the human rights of individuals. Therefore, finding the right balance between technological development and human rights protection is urgent."*[18]

Bibliography

1. Bertolini, A., Episcopo, F. *The Expert Group's Report on Liability for Artificial Intelligence and Other Emerging Digital Technologies: a critical assessment*.

[17] Tan, E. *The new digital era governance.* Chapter 2: *The role of big data, AI and blockchain technology in digital public governance*. p. 51. Available online at: https://www.wageningenacademic.com/doi/abs/10.3920/978-90-8686-930-5_2, accessed March 4, 2023.

[18] Available online at: https://www.coe.int/en/web/commissioner/-/unboxing-artificial-intelligence-10-steps-to-protect-human-rights, accessed March 4, 2023.

Cambridge University Press, 2021. Available online at: https://www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/expert-groups-report-on-liability-for-artificial-intelligence-and-other-emerging-digital-technologies-a-critical-assessment/45FD6BB0E113E7C4A9B05128BC710589.

2. Czech Civil Code Act. No. 89/2012 Coll., https://www.cak.cz/assets/pro-advokaty/mezinarodni-vztahy/civil-code.pdf.
3. Liability for Artificial Intelligence Report from the Expert Group on Liability and New Technologies-New Technologies Formation. Available online at: https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=36608.
4. 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. Available online at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206.
5. Proposal for the Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive). 28.09.2022 Available online at: https://commission.europa.eu/system/files/2022-09/1_1_197605_prop_dir_ai_en.pdf.
6. Regulation (EU) 2016/679 Of The European Parliament And Of The Council of April 27 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). Available online at: https://eur-lex.europa.eu/legalcontent/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN.
7. Sovová, O., Fiala, Z. *Challenges of Public Administration in the Global Digital Era*, in Cazala, J., Zivkovic, V. (eds.), *Administrative Law and Public Administration in the Global Social System* (Contributions to the 3rd International Conference „Contemporary Challenges in Administrative Law from an Interdisciplinary Perspective", October 9, 2020, Bucharest). ADJURIS - International Academic Publisher, Bucharest, Paris 2021, p. 138–146, available online at: http://www.adjuris.ro/ editura_en.html.
8. Tan, E., *The new digital era governance. Chapter 2: The role of big data, AI and blockchain technology in digital public governance*. Available online at: https://www.wageningenacademic.com/doi/abs/10.3920/978-90-8686-930-5_2
9. *Unboxing artificial intelligence*.10 steps to protect human rights, available online at: https://rm.coe.int/unboxing-artificial-intelligence-10-steps-to-protect-human-rights-reco/1680946e64.
10. Vošalíková, A*., Jsme připraveni žít s robotem?* "Mlada fronta Dnes", a Czech daily, 29.10. 2023, available online at: https://www.idnes.cz/technet/technika/komentar-vosalikova-umela-inteligence-robot-kreativita-hrozba.A230127_173752_domaci_kadlwww.idnes.cz.

LEGAL INTERFACE OF THE CURRENT STANDARDS IN DIGITALIZATION

Brief Considerations Regarding the Work on Digital Platforms

Associate professor **Ana VIDAT**[1]

Abstract

The European Commission's recent concerns include measures to improve working conditions for working on platforms and to support the sustainable growth of digital work platforms in the EU. There is a need to regulate the area of work on digital platforms – ensuring that people working through digital work platforms can enjoy their employment rights and social benefits. Workers will also benefit from additional protection for the use of algorithmic management (i.e., automated systems that support or replace managerial functions in the workplace). A common set of EU rules will provide greater legal certainty - enabling digital work platforms to fully benefit from the economic potential of the single market and a level playing field.

Keywords*: individual employment contract; digital platforms; work; European Union acts; comparative law.*

JEL Classification*:* K24, K31

1. Introductory aspects

Digitisation results in innovative services, new business models, new ways of organising work; artificial intelligence (AI), digitisation connects the world, increasing international cooperation and streamlining the way organisations operate and workers are managed[2].

New technologies are automating much of daily work and repetitive tasks – enabling workers to focus on more creative, analytical and strategic activities[3].

Digitalisation is making remote and hybrid working viable options for more and more employers, leading to more flexible work organisation and increased productivity. Digital work platforms can effectively match labour supply and demand and create opportunities for those involved in the legal employment relationship.

Digital transformation also brings with it several challenges. Working

---

[1] Ana Vidat - Faculty of Law, Bucharest University of Economic Studies; lawyer, member of the Bucharest Bar Association, Romania, ana.vidat@drept.ase.ro.

[2] *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Better working conditions for a stronger social Europe: reaping the full benefits of digitalisation for tomorrow's work*, COM/2021/761 final, available here: https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:52021DC0761 (accessed on 28.06.2022). See also Nina Gumzej, *Data protection for the digital age: comprehensive effects of the evolving law of accountability*, „Juridical Tribune - Tribuna Juridica", Volume 2, Issue 2, December 2012, p. 83.

[3] *Communication from the Commission to the European Parliament, the Council, ..., op. cit.*

conditions in the EU are among the best in the world. Minimum requirements on working time, health and safety at work, social protection, and equal treatment of people (including equal pay for men and women) are part of the European social model. However, the advent of digitalisation is affecting the labour market in ways that call this model into question. New forms of work organisation do not automatically translate into quality jobs[4].

Therefore, the principles underlying the European social market economy should not be taken for granted and should be protected. Some people are increasingly disadvantaged – including those working through digital work platforms and working in precarious working conditions. New ways of organising work in the form of platform working make it more complex to properly qualify those who work as workers or self-employed. This leads to situations where some people are unfairly deprived of access to the protection conferred by worker status; others cannot enjoy real autonomy of self-employed status. As algorithmic tools become more widespread in the labour market, issues of supervision, data use, equality and discrimination (*e.g.*, gender bias embedded in the design of algorithmic tools) and enforcement of algorithmic management are increasingly emerging.

Recent concerns of the European Commission include measures to improve working conditions for platform work and to support the sustainable growth of digital work platforms in the EU.

There is a need to regulate the area of work on digital platforms – ensuring that people working on them can enjoy the rights conferred by labour law and the social benefits due to them. Workers will also benefit from additional protection for the use of algorithmic management (*i.e.*, automated systems that support or replace managerial functions in the workplace).

A common set of EU rules will provide greater legal certainty – creating the possibility for digital work platforms to fully benefit from the economic potential of the single market and a level playing field. One of the Union's objectives is to promote the well-being of its peoples and the sustainable development of Europe, based on a highly competitive social market economy, aiming at full employment, social progress[5].

The right of every worker to working conditions which respect his or her health and safety at work, dignity, and the right of workers to information and consultation are enshrined in the Charter of Fundamental Rights of the European Union. The European Pillar of Social Rights states that "irrespective of the type or duration of the employment relationship, workers have the right to fair and equal treatment as regards working conditions and access to social protection"[6].

Digital transformation is driving rapid change, affecting the labour market – find it necessary to identify "ways to improve the working conditions of

[4] *Communication from the Commission to the European Parliament, the Council....., op. cit.*
[5] Article 3 of the European Union Treaty.
[6] Principle 5 of the European Pillar of Social Rights.

workers on online platforms"[7].

The economy of digital platforms is growing fast[8]. Currently, more than 28 million people work through digital work platforms in the EU. By 2025, this number is expected to reach 43 million. Most of them are genuinely self-employed. However, an estimated 5.5 million are incorrectly classified as self-employed. Between 2016 and 2020, revenue from the platform economy increased almost fivefold, from around €3 billion to around €14 billion. Digital work platforms create opportunities for businesses, workers and the self-employed and provide improved access to services for consumers. However, new ways of working also bring new challenges. It is becoming increasingly difficult to qualify people's professional status correctly – leading in some cases to inadequate workers' rights and social protection. In addition, the use of algorithms in the work of platforms can raise issues of accountability and transparency. The Commission has resorted to presenting: a Communication setting out the approach and measures at EU level on working on platforms; work on future global standards for high quality work on platforms; a proposal for a Directive on improving working conditions for working on platforms.

The proposal includes measures to correctly establish the professional status of people working through digital work platforms and new rights for both workers and self-employed persons in relation to algorithmic management; draft guidelines clarifying the application of EU competition law to collective agreements of self-employed persons without employees who wish to improve their working conditions. The guidelines include people working through digital work platforms.

In its Communication "Better working conditions for a stronger social Europe: reaping the full benefits of digitalisation for tomorrow's work"[9], the Commission invites Member States, social partners and all relevant stakeholders to present concrete measures to improve working conditions for platform working. Its aim is to reap the benefits of digital transformation and safeguard the social economy. The EU also wants to lead by example and contribute to future global standards for high quality work on platforms. Platforms operate across borders and warrant a cross-border regulatory approach.

---

[7] Political guidelines for the next European Commission 2019-2024 "A more ambitious Union - My Programme for Europe" – Document available online.

[8] https://romania.representation.ec.europa.eu/news/propunerile-comisiei-de-imbunatatire-conditiilor-de-munca-pentru-persoanele-care-lucreaza-prin-2021-12-10_ro (accessed on 28.06.2022).

[9] *Communication from the Commission to the European Parliament, the Council, the European Economic and Cocial committee and the Committee of the regions better working conditions for a stronger social europe: harnessing the full benefits of digitalisation for the future of work*, com/2021/761 final, available here in english: https://eur-lex.europa.eu/legal-content/en/txt/?uri=celex:52021dc0761, accessed on 28.06.2022.

2. Working on digital platforms

It enables many people to earn a living or supplement their income, including those who find it difficult to access the labour market (*e.g.*, people on low incomes, women, young people, people with disabilities, migrants, or people from racial or ethnic minority backgrounds). Opportunities are created to develop or expand a customer base, sometimes across borders. Working on platforms gives businesses much greater access to consumers, opportunities to diversify revenues and develop new lines of business. On the other hand, consumers are given improved access to products and services that would otherwise be difficult to obtain, as well as access to a new and more varied range of services.

Platform working is by no means homogenous. Digital work platforms operate in a multitude of economic sectors: from the most visible „in a physical location" service (such as car-ride ordering, deliveries or home working) to micro-skills (such as AI training or data coding) to highly skilled creative or specialised jobs (e.g., architectural design, translations or IT development). Digital work platforms also organise work in different ways, leaving varying degrees of autonomy and independence to people working through them. For some people, working on platforms is the main activity, while for others it is a source of additional income. It is essential that digital work platforms across the EU operate within a clear legal framework.

However, the recent development of the platform economy has also created new challenges for those working through them. These can range from a lack of transparency and predictability of contractual arrangements to health and safety challenges, misclassification of professional status or inadequate access to social protection.

There is a need to create transparency about the professional status of people working through digital work platforms. It is currently estimated that nine out of ten digital work platforms active in the EU classify people working through them as self-employed. Many of these people have real autonomy in their work and value the flexibility and easy access to clients that digital work platforms offer. However, others face subordination to and varying degrees of control by the digital work platforms through which they work (for example, in terms of pay levels, organisation of working time and other aspects of their working conditions). In these cases, it is not always clear whether their professional status is correctly established. Employment status should be based on the facts of the employment relationship, irrespective of the existence of a written contract or its terms and conditions. Professional status has consequences for the obligation's incumbent on digital work platforms and the rights that should be granted to people working through them. Individuals' preferences in terms of desired levels of autonomy, flexibility and protection may vary. It is therefore important that they have legal protection in terms of their status, which would allow them to make conscious and voluntary choices.

Collective bargaining and collective agreements are key to improving working conditions. However, in the context of working on platforms, social dialogue is affected. Frequently, no physical workplace is involved, which means that people working through digital work platforms rarely interact, or at least not in an organised way. In many cases, workers may not know their counterparts on a particular platform or how to contact them.

The Commission is not starting from scratch in its attempt to address these challenges. Various legal acts currently exist or are being proposed at European level, which are very relevant to working on platforms.

These include the whole body of EU labour and equal treatment legislation, as well as internal market instruments such as the General Data Protection Regulation[10], which ensures robust protection of personal data, the Regulation on business platforms[11] and the proposed legislation on artificial intelligence. However, the specific challenges outlined above require further specific actions.

The European Parliament has adopted a report[12] calling for strong measures in the context of working on platforms.

Member States[13] also recognise the need for greater legal certainty regarding the rights and obligations of people working through digital work platforms and point to their unclear professional status as a key issue. The European Economic and Social Committee[14] and the Committee of the Regions[15] have also called for specific action on platform working.

3. EU action on platform working – what does it mean for those who work through digital work platforms retrained as workers?

As we have shown, of the 28 million people expected to work through digital work platforms, the majority are genuinely self-employed. However, there may be up to 5.5 million people who are fictitiously self-employed[16].

This means that although they are described in their contracts with the digital work platforms through which they work as self-employed, in reality they are subject to the control and supervision that is characteristic of the status of

[10] Regulation (EU) 2016/679. Document available online.
[11] Regulation (EU) 2019/1150. Document available online.
[12] European Parliament Report on 'Fair working conditions, rights and social protection for workers on online platforms – new forms of employment linked to digital development' 2019/2186(INI).
[13] Debate on working on online platforms at the Employment and Social Affairs Council on 3 December 2020. The main results are available online.
[14] EESC opinion: Decent work in the platform economy (exploratory opinion at the request of the German presidency).
[15] COR opinion: Working on digital platforms – local and regional regulatory challenges. Document available online.
[16] SWD(2021)396. Impact assessment report accompanying the proposal for a Directive on improving working conditions for people working on platforms, section 2.1 and Annex 5.

'worker'. They may be in a particularly precarious situation. If they wish to challenge the qualification of their professional status, they must go to court and prove that the contractual description of their status is false. This is not easy, as it can take time and money and is particularly challenging for people in a precarious position in the labour market, such as low-paid workers, young people, or those from migrant families. So far, there have been more than 100 court rulings and 15 administrative decisions on the professional status of people working through digital work platforms[17].

In most cases, the judgments confirmed that they were misclassified as self-employed and should in fact be considered workers[18].

Professional status is the route to recognition of legally conferred rights. The misclassification of people in bogus self-employment prevents them from benefiting from the rights to which they would be entitled as workers; these benefits include the right to a minimum wage, collective bargaining, working time, protection of health and safety at work, equal pay for men and women, paid leave, improved access to social protection against accidents at work and occupational diseases, unemployment, etc. Misclassification is not only unfair to the workers affected but can also have negative repercussions for society.

This is why one of the key provisions of the proposed directive is a relative presumption of an employment relationship. The presumption applies to all digital work platforms that exercise control over people working through them. The proposal sets out a number of criteria in relation to this control and, as a related theme, in relation to subordination, providing more legal certainty at EU level.

The proposal includes an obligation for Member States to adopt measures to ensure that the presumption is effective, enforceable, and contestable. It is estimated that between 1.7 and 4.1 million of the 5.5 million people at risk of misclassification could, because of the proposed Directive, be considered as workers and therefore have access to the various protections afforded by labour law and or against social risks. Those who are not reclassified could benefit from contractual conditions modified to be in line with the characteristics of a genuinely self-employed person.

Correct qualification of professional status requires better information on the applicable rules. People working through digital work platforms may not be aware of their rights and obligations under the relevant legislation (*e.g.*, in the field of labour law, social security and taxation). Online digital platforms have

[17] These were pronounced in BE, DE, DK, ES, FI, FR, IE, IT, NL and SE – European Centre of Expertise in the field of Labour Law, Employment and Labour Market Policies (ECE) "Case Law on the Classification of Platform Workers: Cross-European Comparative Analysis and Tentative Conclusions", May 2021.

[18] SWD(2021)396. Impact assessment report accompanying the proposal for a Directive on improving working conditions for people working on platforms, Annex 10.

expressed their dissatisfaction with the regulatory uncertainty and lack of transparency they face regarding the applicable national rules. Member States are best placed to ensure the clarity and transparency of the rules they set.

To complement the measures proposed by the Directive, the Commission invites Member States: Provide advice and guidance to people working through digital work platforms on tax, social security and/or employment law obligations related to their work on the platform; create specific information channels, such as information websites and hotlines, to provide such advice; ensure greater transparency for digital work platforms active on their territory on national rules governing the classification of professional status; facilitate the development of small and medium-sized digital work platforms, for example by providing access models, including relevant and sufficiently comprehensive information on the applicable legal framework.

4. Impact of the Directive on the genuinely self-employed[19]

As an indirect effect of the Directive, some of the digital work platforms, which currently exercise a degree of control over the people working through them, may change their business model to create the conditions for truly independent activities. The Directive will provide incentives for digital work platforms to better clarify their contractual relationships (if necessary). It is expected that the Directive will strengthen the autonomy of self-employed activities and support the ability of self-employed persons to take advantage of their entrepreneurial opportunities, for example by developing their client portfolio. People who are already genuinely self-employed will continue to enjoy the benefits of their professional status.

All self-employed persons through the platforms will gain similar rights to those of workers in terms of algorithmic management, in terms of transparency of the automated systems used and the mechanisms for appeal and review of algorithm-based decisions. Greater clarity on the mechanisms underlying the assignment and proposal of tasks will help them to improve security and predictability of income.

5. E.U. action on working on platforms – reported by enterprises

Conservative estimates suggest that there are over 500 digital work platforms in the EU – Innovative service providers that offer services in line with new consumer preferences in particular, 'on-demand' services that often build

[19] *Communication from the Commission to the European Parliament, the Council, the European Economic and Cocial committee and the Committee of the regions better working conditions for a stronger social europe: harnessing the full benefits of digitalisation for the future of work*, com/2021/761 final, available here in english: https://eur-lex.europa.eu/legal-content/en/txt/?uri=celex:52021dc0761, accessed on 28.06.2022.

their customer base and competitive position through the speed, efficiency, and flexibility with which they deliver services. They bring dynamism to the EU economy, harnessing the benefits of digitisation. However, their potential for innovation risks being limited by the fragmentation of existing regulatory frameworks, which call into question cross-border expansion and prevent digital work platforms from taking full advantage of the economies of scale and breadth of the Single Market[20].

Innovation should take place in a truly competitive and level playing field. For competition to produce positive outcomes in terms of consumer choice, low prices and worker welfare, businesses should compete on the quality of the services they provide and their productivity – rather than on the working conditions of workers. However, some digital work platforms currently build part of their competitive advantage not only on the innovation of the services they offer, but also on the low cost of their labour, by hiring self-employed people who should actually be salaried workers. The natural consequence of this is lower costs than would otherwise be the case; on average, businesses that employ workers face 24.5% higher costs in the form of taxes and contributions[21].

The proposed Directive ensures fair treatment of workers, a level playing field and legal certainty. It provides more clarity on who should be considered as workers and on the obligations of digital work platforms, thus avoiding lengthy court proceedings and giving digital work platforms legal certainty on how they can operate across the EU. The relative presumption and employment criteria proposed by the Directive will ensure that digital work platforms operating through bogus self-employed persons follow the same rules as traditional platforms and companies employing workers and therefore do not benefit from an unfair competitive advantage. The EU legislation will be complemented by guidelines provided by Member States.

For digital work platforms, the possibility to work with genuinely self-employed people will not be significantly affected.

The current inability to transfer the use of rating/reputation systems between digital work platforms hinders competition between them as it discourages people from working through newly established digital work platforms[22]. So-called" lock-in effects" mean that those involved in legal transactions do not switch to other digital work platforms for fear of losing their hard-earned online reputation through client ratings. On the other hand," Superstar effects" mean that newcomers to a platform find it hard to challenge the established position of their competitors, as they cannot bring with them the credentials they may have gained

[20] See Jens-Uwe Franck, Martin Peitz, *Market power of digital platforms*, „Oxford Review of Economic Policy", Volume 39, Issue 1, Spring 2023, p. 34–46, https://doi.org/10.1093/oxrep/grac 045.
[21] Eurostat (2021). Wages and labour costs. Document available online.
[22] See Xiaolan Fu, Elvis Avenyo & Pervez Ghauri, *Digital platforms and development: a survey of the literature*, in „Innovation and Development", 2021, 11:2-3, pp. 303-321, DOI: 10.1080/21579 30 X.2021.1975361.

elsewhere. These favours existing digital work platforms, but also, within a platform, favours those who have worked through it the longest.

6. EU action on working on platforms – reported to national authorities

Clarity on professional status and related tax and social security contributions will support the sustainability of public budgets. Member States are expected to raise up to €4 billion in annual contributions because of reclassification measures[23].

They will also incur lower costs in terms of non-contributory benefits that public authorities may have to provide to unprotected workers to address, for example, social exclusion or medical costs. Correct qualification of occupational status can therefore have a positive impact for all taxpayers.

To facilitate the work of national authorities (such as labour inspectorates, social protection institutions and tax authorities) in enforcing the provisions of the proposed Directive and existing legislation, the proposed Directive includes provisions to ensure transparency and traceability of work on platforms, including in cross-border situations. These provisions should ensure that digital work platforms acting as employers are aware of their obligations in terms of declaring where they carry out their activity. The proposed Directive requires digital work platforms to make available to labour authorities, social protection authorities and other relevant authorities, as well as to representatives of persons working on the platforms, information on the terms and conditions for persons working through them, the number of persons working through them, and the professional status based on which they work. This information will need to be regularly updated and further clarified at the request of the relevant authorities.

As many digital work platforms operate globally, cooperation between jurisdictions is essential.

The EU will work with its global partners to ensure decent working conditions for working on platforms worldwide. The International Labour Organisation is a natural partner in this effort.

[23] SWD(2021)396. Impact assessment report accompanying the proposal for a Directive on improved working conditions for work on platforms, section 6.1 and Annex 5.

7. Conclusions[24]

Digital work platforms play an important role in Europe's economic future, including for the green and digital transition. However, to be sustainable, technological progress must advance in parallel with respect for social principles. This package aims to address the challenges that working on platforms presents to the social model and to ensure conditions for a sustainable development of the platform economy in Europe - where its benefits can be more easily harnessed in a more integrated single market and its disadvantages can be prevented and countered.

As a result of the proposed measures, more people working through digital work platforms will benefit from better income security and predictability, respect for legal working time arrangements and a safer working environment[25]. Workers will be better able to build up an old-age pension, have access to social protection measures they can rely on in difficult times and no longer fear unfair decisions made by automated systems. Those who remain or become genuinely self-employed will be able to make their own choices about their working conditions and use working on platforms to build entrepreneurial careers.

In addition, all people working through digital work platforms – whether employed or self-employed – will better understand and influence how algorithms are used to manage their work. Work carried out through digital work platforms, including across borders, will become easier to track and more transparent. This will allow national authorities and social partners to play a more active role in the platform economy.

The proposed measures will require an adaptation of digital work platforms, workers, and national authorities – helping to harness the many benefits of digital transformation and protecting the social economy over time. Guided by the European Declaration on Digital Rights and Principles for the Digital Decade and the European Pillar of Social Rights, the EU has the means and direction it needs to succeed in this endeavour.

Bibliography

1. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Better working conditions for a stronger social Europe: reaping the full*

[24] Communication from the Commission to the European Parliament, the Council, The European Economic and Social Committee and the Committee of the Regions Better working conditions for a stronger social Europe: harnessing the full benefits of digitalisation for the future of work, COM/2021/761 final, available here: https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:52021DC0761 (accessed 28.06.2022).

[25] For more posibilities see 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.

benefits of digitalisation for tomorrow's work, COM/2021/761 final, available here: https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:52021DC0761 (accessed on 28. 06.2022).

2. Cristina Elena Popa Tache, *Public International Law and FinTech Challenge*, „Perspectives of Law and Public Administration", Volume 11, Issue 2, June 2022.
3. Jens-Uwe Franck, Martin Peitz, *Market power of digital platforms*, „Oxford Review of Economic Policy", Volume 39, Issue 1, Spring 2023, pp. 34–46, https://doi.org/10.1093/oxrep/grac045.
4. Nina Gumzej, *Data protection for the digital age: comprehensive effects of the evolving law of accountability*, „Juridical Tribune - Tribuna Juridica", Volume 2, Issue 2, December 2012.
5. Xiaolan Fu, Elvis Avenyo & Pervez Ghauri, *Digital platforms and development: a survey of the literature*, in „Innovation and Development", 2021, 11:2-3, pp. 303-321, DOI: 10.1080/2157930X.2021.1975361.

Digital Euro Currency, Economic and Legal Implications

PhD. student **Daniela DUȚĂ**[1]
Senior manager **Isabelle OPREA**[2]

Abstract

The digitization of the economy, artificial intelligence and technological innovations are influencing consumers' perception of payment services. As cryptocurrencies and stablecoins became more popular, the central banks of the world realized that they had to offer an alternative, namely, digital currency. To ensure that the population continues to have unlimited access to central bank money in a way that meets their needs in the digital age, the Council of the European Central Bank has decided to advance work on the possible issuance of a digital euro – an electronic form of central bank money, accessible to all citizens and commercial companies. From a legal perspective, the introduction of a digital euro would require careful analysis of cybersecurity, data protection, and consumer protection issues. Legal changes would also be necessary to ensure that the digital euro is recognized as legal mean of payment and subject to the same legal framework as traditional currency, as well as to ensure consumer protection and interoperability with other digital payment systems. The digitalization of the economy and new technologies are likely to influence the users' behavior regarding the digital euro currency?

Keywords*: euro digital, coin, European Central Bank, electronic currency, customer.*

JEL Classification: K22, K24, K33

1. Introduction

In today's economy, the number of electronic transactions is constantly increasing due to the Covid-19 quarantine period, but also due to the rapid evolution of technology. During the quarantine period, the population was encouraged to use electronic payment methods to avoid direct contact with banknotes. In this context, the population's habit of using cash has been changed, in favor of electronic card payments at merchants or in online stores. There has been a similar trend in many European countries, where the use of cash has fallen significantly during the pandemic - the daily value of cash withdrawals from ATMs has

[1] Daniela Duță - Institute of Legal Research „Acad. Andrei Rădulescu" of the Romanian Academy. (School of Advanced Studies of the Romanian Academy); member of the Legal Research Laboratory regarding new technologies ("LCJNT") within the Legal Research Institute "Acad. Andrei Rădulescu", ghituleasad@yahoo.com.
[2] Isabelle Oprea - Vista Bank Romania SA, isabelle.oprea@gmail.com.

fallen by 40% in Ireland and by 90% in Spain.[3]

The digitization of the economy, the use of artificial intelligence systems or technological innovations, influence consumers' perception for payment services. As cryptocurrencies and stablecoins became more popular, the central banks of the world realized that they needed to offer an alternative, namely, digital currency.

Digital or electronic currency is "a digital form of a classical or 'fiat' currency". From a legislative point of view, digital currency[4] is defined in the Law no. 210/2019 on the activity of issuing electronic money as: "monetary value stored electronically, including magnetically, representing a claim on the issuer, issued upon receipt of funds for the purpose of performing operations of payment and which is accepted by a person other than the issuer of electronic money".

Several research methods have been used in documenting the issues under scientific research, analyzed from both an economic and a legal point of view. Among these, the *comparative method* is used to identify the similarities and differences regarding the need for the digital euro, the use of electronic currencies or cash. Through the *legal method*, the national and European legislative framework that could be applicable and the perspective of possible risks resulting from the implementation of the digital euro were subjected to the analysis.

2. Digital currency of Central Bank

A central bank digital currency (hereinafter referred to as "CBDC") is the digital form of a country's fiat currency, which is also a claim on the central bank. Instead of printing money, the central bank issues electronic currencies or government-backed accounts. This currency is accessible to everyone.

CBDCs are classified as follows considering the intended users:

- CBDC for individuals is based on ledger technology, is traceable, anonymous and available all the time. It also offers the possibility of applying the interest rate. Due to these advantages, a central bank digital currency for individuals is particularly focused on supporting the general public. In addition, it helps lower the cost of printing cash and promotes financial inclusion.

- CBDC for institutions increases payment efficiency and security efficiency, while solving liquidity and counterparty risk issues. It is suitable for financial institutions that have reserves deposited with a central bank[5].

There are many reasons to explore digital currencies, and the motivation

[3] Financial Times, 27.05.2020 - *Coronavirus accelerates shift away from cash*. The document is available online at: https://www.ft.com/content/430b8798-92e8-4b6a-946e-0cb49c24014a and was accessed on 25 March 2023.

[4] Art. 4, letter f) of the Law no. 210/2019 on the activity issuing electronic money, Document date: 8th of November 2019, issued by Romanian Parliament, entered in force on 13th of December 2019 and published in Official Monitor no. 914 on 13th of Nov 2019.

[5] What is a central bank digital currency (CBDC)? - the document is available online at: https://hedera.com, accessed on 25 March 2023.

of different countries for issuing CBDCs depends on their economic situation. Some common motivations are: promoting financial inclusion by providing easy and safer access to money for unbanked and underbanked populations; introducing competition and resistance to the internal payments market, which may need incentives to provide cheaper and better access to money; increasing the efficiency of payments and reducing transaction costs; creating programmable money and improving the transparency of money flows; and ensuring the uniform and smooth flow of monetary and fiscal policy.

There are several challenges and each needs careful consideration before a country launches a CBDC. Citizens could withdraw too much money from banks at once by purchasing CBDC, triggering a bank default – affecting their ability to make loans and sending a shock to interest rates. This is especially a problem for countries with unstable financial systems. CBDCs also present operational risks as they are vulnerable to cyber-attacks and must be made resilient against them. Finally, CBDCs require a complex regulatory framework, including robust confidentiality, data protection, consumer protection and anti-money laundering standards, before adopting this technology.

Thus, 114 countries around the world are currently exploring issuing a Central Bank digital currency; 11 countries have launched digital currency; China's digital currency (pilot project) is accessible to 260 million people, and in the course of 2023, it will be extended to the entire population of the country; the most recent digital currency issued is that of Jamaica – JAM-DEX.[6]

During 2023, more than twenty countries will take major steps to issue a digital currency through pilot projects. Australia, Thailand, Brazil, India, South Korea and Russia will continue or start pilot tests in this regard.[7]

3. Digital Euro

An important part of the Eurosystem's[8] mission is to provide to the citizens risk-free money for their payments. The Eurosystem has provided euro banknotes for more than two decades.

While cash is still the dominant means of payment in the euro area, new technologies and increasing consumer demand for speed are changing the way European citizens make payments.

To ensure that the population continues to have unlimited access to central bank money in a way that meets their needs in the digital age, the European

[6] Jamaica's Central Bank Digital Currency (CBDC) – JAM-DEX: https://boj.org.jm/core-functions/currency/cbdc/; information about the online document accessed on 25th of March 2023.
[7] The document is available online at: https://www.atlanticcouncil.org - Central Bank Digital Currency Tracker, accessed on 25 March 2023.
[8] The Eurosystem, made up of the European Central Bank and the national central banks of the member states that have adopted the euro, is the monetary authority of the euro area. Ecb.europe.eu European Central Bank - Eurosystem.

Central Bank Council has decided to advance the work on the possible issuance of a digital euro – an electronic form of central bank money, accessible to all citizens and companies. A digital euro would be introduced alongside cash, not replace it.[9]

The digital euro is the digitalcurrency of central bank (CBDC) for population that the Eurosystem may issue in the future.[10]

According to the European Central Bank, the digital euro should work like a virtual currency, but with some unique features. In essence, the digital euro is a virtual currency that:

- it will have legal value guaranteed by the European Central Bank.
- can be used alongside banknotes to make payments in the 20 countries of the euro zone.
- will provide a fast, secure and innovative payment method.
- can be used by both companies and citizens.

The digital euro will be managed and regulated using blockchain technology. To use it, a digital wallet will need to be created and a bank account will not need to be opened. In fact, the money can be deposited directly at the European Central Bank. In this way, transactions can be carried out without the need for a commercial bank to act as an intermediary.

4. The motivation for the introduction of the digital euro currency

The digitization and independence of the European economy can benefit from a digital form of central bank money available to citizens. Issuing a digital euro can be a way to stimulate the digitization of the economy, supporting the development of innovative solutions in all types of industries. To the extent that it would fill the gaps in the providal of digital payment solutions and functionalities, the digital euro available to the general public would support the digitalisation of the financial sector and therefore the economy in general. It could reduce costs for payment services by streamlining processes and streamlining new business models.[11]

For example, the digital euro could be issued to facilitate the development by intermediaries of a full range of pan-European consumer solutions for end-users. End-user solutions could be used for both commercial and central bank

[9] Report on a digital euro – European Central Bank, October 2020. The document is available online at: https://www.ecb.europa.eu/pub/pdf/other/Report_on_a_digital_euro~4d7268b458.en. pdf, accessed on 25 March 2023.

[10] Digital euro glossary, European Central Bank – 30.09.2022, The document is available online at: https://www.ecb.europa.eu/paym/digital_euro/investigation/profuse/shared/files/dedocs/ecb.dedocs220420.en.pdf?b268d673898445396fb1a59efbcf01f3, accessed on 25 March 2023.

[11] "This could include, for example, the digitization of information exchanges such as e-invoices and e-receipts, as well as the acceptance of national e-identity and e-signature solutions that comply with the European Regulation on electronic identification, authentication and trust services." European Central Bank - Report on a digital euro.

money distribution. In such a scenario, issuing a digital euro would help preserve European autonomy in a strategic sector such as retail payments. The system's architecture underlying the digital euro should be flexible and easily extensible, with open standardized interfaces between system components, so as to support eventual payment needs and the easy integration of new types of devices over time.[12]

A decline in the use of cash in the economy would imply an increased reliance on private forms of money and payment solutions in the euro area. Such a trend could jeopardize the sustainability of the cash infrastructure and prevent the delivery of adequate services.[13]

In response to a decline in the use of cash, the Eurosystem could introduce a digital euro as an additional form of public money and means of payment. To meet the needs of users, the digital euro should be cheap (result in very low costs for users), secure (provide the highest levels of fraud prevention and consumer protection), risk-free (its holders should not be subject to market risk or issuer default risk), be easy to use (even for ordinary consumers and merchants) and be efficient (allow fast payments).

Cash has distinct inherent characteristics – its physical nature, the ability to ensure confidentiality in payment transactions and the ability to be used without any technical infrastructure. Ideally, a digital euro should allow citizens to continue to make payments in the same way as they currently do, cash payments.[14] In addition, the issuance of a digital euro should be ensured by strong support from citizens and be seen as a symbol of European unity, taking into account the risk that the symbolic value of physical euro banknotes and coins could diminish once with the decrease in the use of cash.

Digital currencies are becoming a credible alternative as a mean of exchange in the Euro zone. Many foreign central banks are evaluating the possibility of issuing their own electronic currencies, which could be made available to European citizens. This could cause currency substitution and an increase in currency risk in the euro area economy. On the other hand, private actors – possibly those outside the supervision of European financial authorities – including large technology firms, are developing non-euro payment solutions (such as "stable coins") that would be used globally and obviously also in the Euro zone.

---

[12] Ibidem, p.10.

[13] "Although this trend is not currently seen in the euro area as a whole, it is taking shape in some EU member states and could spread or be accelerated by extreme events, such as the COVID-19 outbreak, which caused a change of payment habits. If other countries follow, the costs of maintaining cash infrastructure relative to the number of cash transactions could increase beyond acceptable limits and accelerate the decline in cash availability and acceptance" - European Central Bank – Report on a digital euro, p. 10.

[14] "The digital euro should not aim to replace cash, but should only be a complementary form of payment. It would be up to European citizens to decide whether to use digital euro instead of cash. The Eurosystem's position is that the availability of cash should be ensured and measures should be taken in this regard. European Central Bank" – Report on a digital euro, p. 11.

Such developments would stimulate innovation, but could also threaten European financial, economic and ultimately political sovereignty.[15]

Widespread acceptance of a non-euro means of payment could weaken or even impair the transmission of monetary policy in the euro area. It would also have unclear implications for financial intermediation and cross-border capital, which could ultimately affect financial stability. In such circumstances, issuing a digital euro could support European sovereignty and stability, especially in the monetary and financial dimensions. The supply of electronic payments by foreign central banks or by private service providers located outside the euro area would likely pose additional challenges for the Eurosystem regarding the safety and efficiency of European payments. The Eurosystem could therefore consider issuing a digital euro to ensure that payments in the euro area meet the highest standards and are carried out under its direct control. In addition, the Eurosystem could ensure by providing digital payments that European citizens have access to payments at the technological frontier.[16]

It is necessary to reduce the probability that a cyber incident, natural disaster, pandemic or other extreme events will prevent the supply of payment services. The financial institutions and infrastructures are threatened by a wide range of risks. Cyber security risks are always present, the probability of cyber attacks increasing in parallel with the increase in the share of payment services that are digitized.[17] Payments infrastructure could similarly be affected by other risks such as natural disasters. As a result, disruptions to private card payments, online banking and automated teller machine (ATM) cash withdrawals could significantly affect retail payments and erode confidence in the financial system in general. In these scenarios, the digital euro, together with cash, could constitute a possible contingency mechanism for electronic retail payments that could remain in use even when private solutions are not available.[18]

A pandemic can be considered to fall into this scenario, for example, because social distancing could change consumers' payment habits. Consumers may perceive cash as a vector of infection, despite the lack of specific evidence of infection risks associated with banknote use.[19] It could be, therefore, that the pop-

[15] Report on the impact of global stablecoins, G7 Working Group on Stablecoins, October 2019, p. 5. The document is available online at: https://www.tresor.economie.gouv.fr/Articles/5f8c26f2-a2cd-4685-ba82-fa9e4d4e5d67/files/d10fb97f-a9a6-472b-842a-8b279e8863c4, accessed on 25 March 2023.

[16] European Central Bank – Report on a digital euro, p. 12

[17] Protecting the European financial sector: the Cyber Information and Intelligence Sharing Initiative, Introductory remarks by Fabio Panetta, Member of the Executive Board of the ECB, at the fourth meeting of the Euro Cyber Resilience Board for pan-European Financial Infrastructures, Frankfurt am Main, 27 February 2020; The document is available online at: https://www.ecb.europa.eu/press/key/date/2020/html/ecb.sp200227~7aae128657.en.html, accessed on 25 March 2023.

[18] European Central Bank – Report on a digital euro, p. 13.

[19] "Possible concerns regarding the use of cash include: i) social distancing measures, which could become the new norm supported by, for example, the implementation of social protection measures

ulation is less willing to use cash and more inclined towards online and contactless payments.

A strong international role of the euro is an important factor in strengthening European economic autonomy. The issuance of electronic currencies by major foreign central banks could improve the status of another international currency to the detriment of the euro. In such a situation, the Eurosystem could consider issuing a digital euro, in part, to support the international role of the euro by stimulating demand for the euro among foreign investors.[20]

The cooperative approach of interoperable electronic currency projects could help strengthen the international role of the euro and improve cross-payments, without the need to give non-euro area residents access to the digital euro.[21] In addition, a digital euro could help fill gaps or correct inefficiencies in existing cross-payment infrastructures through improved interoperability between payment systems dealing in different currencies.

The Eurosystem decides to proactively support the lowering of the overall costs and ecological footprint of the monetary and payments system. The production of payment instruments and related infrastructure may not always be energy efficient.[22]

A well-designed digital euro can thus contribute to overall cost reduction.[23] In this context, the Eurosystem would play a catalytic role and lead by example[24], creating incentives and putting pressure on payment service providers to reduce their costs. This would be achieved by highlighting the costs and energy

---

by governments through government-to-person (G2P) payments; ii) difficulties in banking relationships and limited access to other financial services; iii) increased preference for online shopping and contactless payments determined by the fear of infection." European Central Bank - Report on a digital euro, p. 13.

[20] "It is estimated that around 30% of euro cash (€341 billion out of a total of around €1.1 trillion in circulation) was held outside the euro area at the end of 2016, mainly in countries neighboring the euro area - The international role of Euro, ECB, 2017" - European Central Bank – Report on a digital euro, p. 14

[21] "As an example, currently most cross-border payments are ultimately cleared in US dollars by correspondent banks located in the US. A multilateral electronic currency system, where an electronic currency is held only by residents of the respective currency area, but is used for cross-border payments between participating central banks, could boost the international role of the euro. European Central Bank" – Report on a digital euro, p. 14.

[22] Environment, health and safety for an ECB assessment of the environmental impact of banknotes; and Hanegraaf, R., Larçin, A., Jonker, N., Mandley, S. and Miedema, J., *Life cycle assessment of cash payments in the Netherlands*, „International Journal of Life Cycle Assessment", Vol. 25, pp. 120-40, 2019.

[23] "Attacking the cost of cash", McKinsey & Company, 2018. The document is available online at: https://www.mckinsey.com/industries/financial-services/our-insights/attacking-the-cost-of-cash, accessed on 25 March 2023.

[24] Climate change and the financial sector", speech by Christine Lagarde, President of the ECB, 27 February 2020. The document is available online at: https://www.ecb.europa.eu/press/ key/date/2020/html/ecb.sp200227_1~5eac0ce39a.en.html, accessed on 25 March 2023.

efficiency of the digital euro compared to other payment solutions when promoting its use.

5. Digital Euro - potential effects of the introduction into the Euro Zone

5.1. Effects in the banking sector, monetary policy and financial stability

The introduction of a digital euro could affect the transmission of monetary policy and have a negative impact on financial stability, namely interest rates. Depending on the form of investment, it could cause depositors to convert their commercial bank deposits into central bank liabilities. This could increase banks' funding costs and, consequently, interest rates on bank loans.[25]

The substantial demand for digital euros may also have a negative impact on financial stability, given the key role of the banking sector in financial intermediation. When asked to raise their funding costs, banks may have to reduce leverage and decrease credit supply, thus preventing an optimal level of aggregate investment and consumption. If this process ultimately entails higher costs for borrowers, economic activity could be hampered. Moreover, if their traditional business model is compromised, banks may decide to take on greater risk in an attempt to earn more to compensate for reduced profitability.[26]

The digital euro should be an attractive means of payment, but it should be designed in such a way as to avoid its use as a form of investment and the associated risk of large changes from private money (e.g., bank deposits) to the digital euro.[27]

5.2. The impact of the digital euro on profitability and risk-taking by the Central Bank

Issuing a digital euro would change the structure and most likely the size of the Eurosystem's balance sheet and therefore affect its profitability and exposure risk. Issuing money is normally profitable and generates emission rights income due to the difference between the remuneration of the central bank's assets and the interest rate applied to the central bank's liabilities (the rate is zero for banknotes). In the case of a digital euro, several factors must be considered:

(i) a digital euro can to some extent, replace banknotes, therefore it would not necessarily increase the risks to the Eurosystem's balance sheet; at the same

[25] European Central Bank – Report on a digital euro, p.16.

[26] "From the perspective of the Central Bank, the problem related to the higher financing costs of the banking sector is not one related to lower profits for individual banks, but to a possible instability of the financial system as a whole". - European Central Bank – Report on a digital euro, p. 17.

[27] European Central Bank – Report on a digital euro, p. 18.

time, considerable growth could occur if non-euro area residents moved a large part of their portfolios to the digital euro. In such a situation, the Eurosystem's balance sheet risks could increase significantly;

(ii) to the extent that the size of the balance sheet increases, the Eurosystem should purchase assets (loans or securities);

(iii) unlike cash, the digital euro could be remunerated, which would affect issuance revenues.

In addition to risks related to the size and structure of its balance sheet, the Eurosystem could also be exposed to financial liabilities as a payment system operator. For example, the malfunctioning of the IT infrastructure underlying the digital euro could cause loss and damage to individual users, raising questions about central bank responsability.[28]

5.3. The effects of the introduction of the digital euro on the safety and efficiency of retail payments

The digital euro used for retail payments would inevitably have implications for the operation of the payment system. It should therefore be designed in such a way that it does not hinder, but rather enhances, the smooth functioning of the payments system and its role in maintaining confidence in the euro and promoting an efficient market economy. Issuing a digital euro would particularly affect the activity and role of commercial bank money issuers and related payment service providers. The role of the Eurosystem should not go beyond what is necessary to ensure the effectiveness of a digital euro (e.g., controlling the monetary base; ensuring the security of the infrastructure; ensuring that related service providers are adequately supervised), as well as the efficiency and usability (e.g., in relation to IT services, customer support, personalization and technological innovation).

The provision of additional services should be left to supervised intermediaries. The Eurosystem would still be responsible for ensuring that the services provided to users are consistent with public interests. Therefore, it should be ensured that the payment facilities offered to citizens serve the needs of all segments of the population in a non-discriminatory manner. For the needs of the citizens, information campaigns will have to be made that would greatly support the Eurosystem in the field of electronic retail payments; both euro and digital euro banknotes should remain in circulation to avoid financial exclusion.[29]

[28] European Central Bank – Report on a digital euro, p. 18.
[29] European Central Bank – Report on a digital euro, p. 20.

5.4. Reputational and other risks

Issuing a digital euro and its functionality would affect the image of the central bank. A loss of reputation could occur if the implementation of the digital euro is delayed from the originally announced implementation date, if the IT infrastructure underlying the digital euro turns out to be unstable (including in the case of cyber-attacks), or if the services digital data are provided outside the regulatory framework applied to private payments and possibly used for illegal activities (e.g. money laundering or terrorist financing).[30] In the context of the Eurosystem, reputational issues could arise if accessibility for the digital euro was not the same across the territories of the euro area countries.

Legal risks could also arise if there was uncertainty about the legal basis for issuing the digital euro.

6. The legal basis for the Eurosystem's issuance of a digital euro

The Digital Euro Report mentioned above states that the selection of primary law of the European Union to be used as the legal basis for issuance will depend on the design of the digital euro and the purpose for which it is issued.

Thereby:

- if the digital euro were issued as a **monetary policy instrument**, similar to central bank reserves and only accessible to central bank counterparties, then the Eurosystem could invoke as a legal basis article 127 paragraph (2) of the Treaty on the Functioning of the European Union (TFEU) in conjunction with the first part of article 20 of the Statute of the European System of Central Banks (ESCB).

- if the digital euro were made available to households and other private entities through accounts held at the Eurosystem, the Eurosystem could invoke, as a legal basis, Article 127(2) of the TFEU, in conjunction with Article 17 of the Statute of the ESCB (which, however, cannot serve as the sole legal basis).

- if the digital euro was issued as a specific means of establishing payments, processed by a dedicated payment infrastructure, accessible only to eligible participants, then the legal basis for its issuance would be Article 127(2) of the TFEU in conjunction with Article 22 of the Statute ESCB.

- if the digital euro were issued as an instrument equivalent to a banknote, then the legal basis for its issuance would be Article 128 of the TFEU in conjunction with the first part of Article 16 of the Statute of the ESCB. In general, invoking Article 128(1) TFEU in conjunction with Article 16 of the Statute of the ESCB would give the Eurosystem the widest level of discretion to issue a digital

[30] "The application of the AML/CFT (Anti-Money Laundering and Countering the Financing of Terrorism) framework to the digital euro should send a clear message that illicit money will be verified in the digital euro network and it is extremely important to ensure the integrity, stability and digital euro reputation". - European Central Bank – Report on a digital euro, p. 19.

euro with legal tender status.

Relying on Article 127(2) TFEU in conjunction with Articles 17, 20 or 22 of the ESCB Statute would be more consistent with the issuance of digital euro variants for limited uses, lacking the general status of legal tender.

A secondary law, adopted on the basis of Article 133 of the TFEU, could be developed to regulate the conditions for issuing a digital euro with legal tender status by the Eurosystem.

7. The legal implications of the different digital euro access options

In the situation where consumers have direct access to the digital euro, the Eurosystem would become the sole payment service provider for the digital euro, while in the situation where end-users have intermediate access, the Eurosystem would depend on third parties for the distribution of the digital euro.

Access to digital euro for end-users involves considerable legal novelty, while non-retail access would be simpler as it would be more similar to current practices.

A retail account-based digital euro could be implemented by opening accounts directly with the Eurosystem or through supervised intermediaries, while the distribution of a bearer-based digital euro (also referred to as a "token-based" or "value-based" digital euro) would likely require the involvement of supervised intermediaries.[31]

In principle, practical aspects that do not affect the central bank's balance sheet (e.g., storage of units, handling of payments on behalf of the public, etc.) could be outsourced, under the strict supervision of the Eurosystem. However, the design and issuance elements of a digital euro (such as remuneration, anonymity, infrastructure, issuance model, etc.) cannot be outsourced.[32]

The introduction of a digital euro would have important legal implications. Specifically, the following aspects should be considered:

- legal recognition, it is necessary to amend the legislation in order to recognize the digital euro. This recognition should apply in all member states of the European Union.

- data protection, in the context of using the digital euro, special attention should be paid to the protection of the personal data of the data subjects. For example, an appropriate framework should be established for the collection, storage and use of this data, privacy by design/default.

- cyber security, since the digital euro would be used for financial transactions, adequate cyber security is required to prevent unauthorized access to financial information and to protect against cyber attacks.

---

[31] European Central Bank – Report on a digital euro - The document is available online at: https://www.ecb.europa.eu/pub/pdf/other/Report_on_a_digital_euro~4d7268b458.en.pdf, accessed on 25 March 2023.

[32] Ibid.

- from the point of view of the consumer protection legislation.

- responsibility against fraud or trading errors, the responsibility for such situations should be clearly defined and also an appropriate mechanism for resolving potential disputes.

- transparency and consumer information - to ensure a correct and safe use of the digital euro, clear and complete information on the characteristics, risks and costs associated with its use would be necessary.

- accessibility and interoperability - to ensure equal access to the digital euro for all consumers, interoperability with other digital payment systems should be guaranteed and flexible payment options adapted to the needs of different consumer groups should be available.

Thus, from a legal point of view, the introduction of the digital euro currency would require the adoption of a specific legal framework to regulate aspects related to its use and operation, so that it can be used for all commercial and financial transactions.

At the same time, clear regulations and procedures should be established for its issuance, administration and circulation, as well as for data protection and transaction security. The fiscal and customs implications of using the digital euro should also be considered, as well as its possible effects on financial stability and monetary policies.

8. Digital currency

8.1. The legislative framework of the European Union regarding digital currency

The European Union (EU) has adopted a number of regulations and directives governing the use of electronic money within the European Union. The regulations are intended to protect consumers, ensure the safety and security of transactions and prevent money laundering.

It is worth mentioning the **Payment Services Directive**[33] (PSD2) which entered into force in September 2019, and which sets standards for payment services and obliges financial institutions to implement stronger security measures to prevent fraud.

Also, the European Union adopted the **Directive on electronic currencies**[34] which establishes specific requirements for electronic currency issuers to

[33] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No. 1093/2010, and repealing Directive 2007/64/EC, OJ L 337, 23.12.2015, p. 35–127.

[34] Directive 2009/110/EC of the European Parliament and of the Council of 16t[h] of September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC OJ L 267, 10.10.2009, p. 7–17.

keep funds in separate accounts and to provide clear and complete information to customers and was partially transposed by BNR Regulation no. 5/2019 regarding electronic money issuing institutions.[35]

The General Data Protection Regulation (GDPR)[36] focuses on the protection of data subjects' personal data, regardless of how it is collected, processed or stored. With regard to electronic currency, it can be assumed that personal data may be collected and processed by payment service providers to enable consumer transactions.

The GDPR regulates the collection, processing and storage of personal data associated with the use of electronic money. Payment service providers must take appropriate technical and organizational measures to protect the personal data of electronic money users, including by ensuring the security of information and respecting the right to personal data protection.

Payment service providers must also take appropriate measures to protect the confidentiality of their customers' data and ensure that this data is stored and processed in a secure manner and in accordance with the provisions of the General Data Protection Regulation and other relevant laws on the protection of personal data, applicable.[37]

And in the case of electronic currency used as a mean of payment, payment service providers must take appropriate measures to verify the identity of users and to fulfill their obligations to know the clientele at the beginning of the contractual relationship and during its development, but also in case transactions with large amounts or in the case of transactions that are suspicious from the point of view of preventing money laundering or terrorism financing.[38]

In January 2023, the **Financial Sector Digital Operational Resilience Regulation**[39] entered into force, impacting the field of cyber security for financial

[35] Regulation 5/2019 regarding institutions issuing electronic money, Act date: 13 Dec. 2019, Issuer: Banca Nationala a Romaniai, entered into force on 19 December 2019, and was published in M. Of. 1021 of 2019.12.19.

[36] Regulation no. 679 of April 27, 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and on the repeal of Directive 95/46/EC (General Data Protection Regulation).

[37] Law no. 190 of July 18, 2018 on measures to implement Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of natural persons in terms of the processing of personal data and regarding the free movement of such data and the repeal of Directive 95/46/EC (General Data Protection Regulation).

[38] According to the provisions of Law no. 129 of July 11, 2019 for the prevention and combating of money laundering and the financing of terrorism, as well as for the modification and completion of some normative acts, Published in the Official Gazette no. 589 of July 18, 2019 and Directive (EU) 2015/849 of the European Parliament and of the Council of May 20, 2015 on preventing the use of the financial system for the purpose of money laundering or terrorist financing, amending Regulation (EU) no. 648/2012 of the European Parliament and of the Council and repealing Directive 2005/60/EC of the European Parliament and of the Council and Directive 2006/70/EC of the Commission published in OJ L 141, 5.6.2015, pp. 73–117.

[39] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14th of December 2022 on the digital operational resilience of the financial sector and amending Regulations (EC)

sector organizations and creating the first legislative framework to harmonize cyber security and risk measures for all financial sector entities, at European level.

The **Digital Services Regulation**[40] is the European Union's new set of reference rules for ensuring a safe and responsible online environment. It applies to all digital services that connect consumers with providers of goods, services or online content. The Regulation creates new obligations for online platforms aimed at reducing potential harm and countering risks in the online environment and provides strong safeguards to protect the rights of online users and a new and unique framework of transparency and accountability for digital platforms.[41]

8.2. The national legislative framework regarding digital currency

The national legislative framework regarding digital currency includes:[42]

- Law no. 210/2019 regarding the activity of issuing digital currency;[43]
- NBR Regulation no. 5/2019 regarding institutions issuing digital currency;[44]
- NBR Regulation no. 5/2012 regarding credit classification and the establishment, regularization and use of specific credit risk provisions applicable to entities supervised by the National Bank of Romania, other than credit institutions;[45]
- NBR order no. 4/2012 regarding the reporting of the situation of the classification of exposures from loans/credits related to payment services and the need for specific provisions for credit risk related to them, applicable to entities

no. 1060/2009, (EU) no. 648/2012, (EU) no. 600/2014, (EU) no. 909/2014 and (EU) 2016/1011, published in OJ L 333, 27.12.2022, p. 1-79.

[40] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19th of October 2022 on a single market for digital services and amending Directive 2000/31/EC (Digital Services Regulation), OJ L 277, 27.10.2022, p. 1–102.

[41] The press release issued by the European Commission on 16.11.2022 - Regulation on digital services: the reference rules of the EU regarding online platforms have entered into force, which can be consulted here: Regulation on digital services: the reference rules of EU on online platforms (europa.eu).

[42] https://www.bnr.ro/Legislatie-financiar-bancara-735.aspx, accessed on 25 March 2023.

[43] Law no. 210/2019 regarding the activity of issuing electronic money, Date of act: 8th of Nov. 2019, Issuer: Parliament, entered into force on 13th of December 2019 and was published in M. Of. 914 of 2019.11.13.

[44] Regulation 5/2019 regarding institutions issuing digital currency, Act date: 13th of Dec. 2019, Issuer: National Bank of Romania, entered into force on 19 December 2019, and was published in Official Gazette no. 1021 of 2019.12.19.

[45] Regulation no. 5 of 8th of March 2012 regarding the classification of loans and the establishment, regularization and use of specific provisions for credit risk applicable to entities supervised by the National Bank of Romania, other than credit institutions, Official Gazette, Part I, No. 179, 20 March 2012, entry in force on March 20th, 2012.

supervised by the National Bank of Romania, other than credit institutions.[46]

9. Conclusions

The digital euro project is an European initiative, it is not just a technical project: it has a clear political dimension, given its large societal implications.

A digital euro would respond to the increasing preferences of the population for electronic payments by making public money available in digital form as well. Along with cash, a digital euro would give Europeans access to means of payment that would allow them to pay anywhere in the euro area, free of charge. The digital euro would be a public good. Therefore, its core services should be free – for example, when the digital euro is used to make a payment to another person, as is the case with cash.[47]

To ensure consumer protection, specific regulations should be adopted to ensure transparency, information and protection against fraud, as well as an appropriate dispute resolution mechanism. The interoperability of the digital euro with other digital payment systems should also be guaranteed so that it can be used efficiently and affordably by all users. In conclusion, the introduction of the digital euro currency would require the adoption of a well-established legal framework.

Bibliography

1. *Coronavirus accelerates shift away from cash*, Financial Times, 27.05.2020.
2. *Report on a digital euro*, European Central Bank, October 2020.
3. *Report on the impact of global stablecoins*, G7 Working Group on Stablecoins, October 2019.
4. *Protecting the European financial sector: the Cyber Information and Intelligence Sharing Initiative*, European Central Bank, 27 February 2020.
5. Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No. 1093/2010, and repealing Directive 2007/64/EC OJ L 337, 23.12.2015.
6. Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC OJ L 267, 10.10.2009.

[46] Order no. 4 of March 8th, 2012, regarding the reporting of the situation of the classification of exposures from loans/credits related to payment services and the need for specific provisions for credit risk related to them, applicable to entities supervised by the National Bank of Romania, other than credit institutions, Official Gazette, Part I 179 20.mar.2012, Entry into force on 20 March 2012.

[47] ECB - Report on a Digital Euro - The scope of basic digital services in the euro has not yet been defined, but should be of a similar nature to the basic services that credit institutions have to provide under the Directive on payment accounts (DPA). Therefore, they could include features such as free opening of digital wallets/accounts in Euro, making payments between people.

7. Law no. 210/2019 regarding the activity of issuing digital currency.
8. Regulation 5/2019 regarding institutions issuing electronic money, Act date: 13-Dec-2019, Issuer: National Bank of Romania, entered into force on 19 December 2019, and was published in M. Of. 1021 of 2019.12.19.
9. Regulation no. 679 of April 27, 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and on the repeal of Directive 95/46/EC (General Data Protection Regulation).
10. Law no. 190 of July 18, 2018, on measures to implement Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of natural persons in terms of the processing of personal data and regarding the free movement of such data and the repeal of Directive 95/46/EC (General Data Protection Regulation).
11. Law no. 129 of July 11th, 2019, for the prevention and combating of money laundering and the financing of terrorism, as well as for the modification and completion of some normative acts, published in the Official Gazette no. 589 of July 18, 2019.
12. Directive (EU) 2015/849 of the European Parliament and of the Council of May 20th, 2015, on preventing the use of the financial system for the purpose of money laundering or terrorist financing, amending Regulation (EU) no. 648/2012 of the European Parliament and of the Council and repealing Directive 2005/60/EC of the European Parliament and of the Council and Directive 2006/70/EC of the Commission published in OJ L 141, 5.6.2015.
13. Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on the digital operational resilience of the financial sector and amending Regulations (EC) no. 1060/2009, (EU) no. 648/2012, (EU) no. 600/2014, (EU) no. 909/2014 and (EU) 2016/1011, published in OJ L 333, 27.12.2022.
14. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19th October 2022 on a single market for digital services and amending Directive 2000/31/EC (Digital Services Regulation), OJ L 277, 27.10.2022.
15. Law no. 210/2019 regarding the activity of issuing electronic money, Date of act: 8th of Nov. 2019, Issuer: Parliament, entered into force on 13th of December 2019 and was published in M. Of. 914 of 2019.11.13.
16. Regulation 5/2019 regarding institutions issuing digital currency, Act date: 13th of Dec 2019, Issuer: National Bank of Romania, entered into force on 19th of December 2019, and was published in M. Of. 1021 of 2019.12.19.
17. Regulation no. 5 of 8th of March 2012 regarding the classification of loans and the establishment, regularization and use of specific provisions for credit risk applicable to entities supervised by the National Bank of Romania, other than credit institutions, Official Gazette, Part I 179 20 March 2012, entry in force on March 20th, 2012.
18. Order no. 4 of March 8th, 2012, regarding the reporting of the situation of the classification of exposures from loans/credits related to payment services and the need for specific provisions for credit risk related to them, applicable to entities supervised by the National Bank of Romania, other than credit institutions, Official Gazette, Part I 179 20.mar.2012, Entry into force on March 20th, 2012.

The Complexity of the Legislative Framework and the Difficulties of Correlation with Economic and Social Impact in Public Administration. The Digitalization of Public Services

Professor **Vasilica NEGRUȚ**[1]
Lecturer **Mircea Valentin CARLAN**[2]

Abstract

Public administration intends, as in all modern countries, to solve public affairs, it is linked to the state system, and it must act for the common good. Continuous adaptation to society's needs is a constant concern of public authorities. One such concern is the digitalization of public services, which consists of a set of activities necessary to adapt all legally regulated processes to transfer the stages of their fulfillment to automated information technology infrastructures organized by artificial intelligence. In this article, starting from the purpose of the public administration, using the logical interpretation, as well as the comparative analysis, we aimed at highlighting the need for the digitalization of public services and the benefits of this process, in the context of a complex legislative framework, emphasizing, at the same time, the difficulties of correlation with economic and social impact in public administration. The digitalization of public services is a mandatory requirement, which will represent a solution for the uniqueness of the stages within the technical-material operations, aspects that will eliminate any possible violations of fundamental rights and freedoms. Digitalization aims not only at facilitating citizens' access to the benefits of public services, but also at changing the perception of citizens towards the public administration, the goal being the achievement of a transparent public administration, as close as possible to the citizen.

Keywords: *public administration; public service; digitalization; information technologies; cyber security.*

JEL Classification: K23, K24

1. Introduction

As a complex phenomenon, public administration represents an activity[3] through which the modernity of a country can be defined. A modern public administration is a major objective of any government in a democratic and social state of law. Public administration is intended, in all modern countries, for the resolution of public affairs, it is linked to the state system and must act for the

[1] Vasilica Negruț - "Dunarea de Jos" University of Galati, Romania, vasilica.negrut@ugal.ro.
[2] Mircea Valentin Carlan - „Danubius University" of Galati, Romania, carlan.mircea@gmail.com.
[3] According to art. 5, letter b) from the Administrative Code, public administration represents "*all the activities carried out, under the regime of public power, of organizing the execution and concrete execution of the law and of providing public services, in order to satisfy the public interest".*

common good. The main purpose[4] of public administration is to satisfy the public interest.

After 1990, the public administration in Romania went through countless transformations, local public administration laws were adopted[5] administrative contentious[6], decentralization[7], culminating with the entry into force of the Administrative Code in 2019[8].

The public administration currently operates based on general principles, which ensure coherence, transparency, and continuity. These principles are mentioned and defined by the Administrative Code in art. 6-13[9].

---

[4] What characterizes public administration is the goal it pursues. M. Văraru, *Manual de drept administrativ/Handbook of administrative law*, Imprimeria statului, Chișinău, 1925, p. 62.

[5] Local public administration law no. 69/1991 repealed by Law no. 215/2001; Local public administration law no. 215/2001, repealed by the Administrative Code.

[6] Law on Administrative contentious no. 29/1990, repealed by Law no. 554/2004; Administrative litigation Law no. 554/2004, published in Official Monitor no. 1154 of 07.12.2004, with subsequent amendments and additions.

[7] Decentralization Law no. 340/2004, repealed by Law no. 195/2006; Decentralization Law no. 195/2006, published in Official Monitor no. 453 of May 25, 2006, repealed by the Administrative Code.

[8] Approved by the Emergency Ordinance of the Government no. 57/2029, published in the Official Monitor no. 555 of July 5, 2019.

[9] According to *the principle of legality*, "Public administration authorities and institutions, as well as their staff, have the obligation to act in compliance with the legal provisions in force and the international treaties and conventions to which Romania is a party" (art. 6). *The principle of equality* assumes that "Beneficiaries of the activity of public administration authorities and institutions have the right to be treated equally, in a non-discriminatory manner, correlative with the obligation of public administration authorities and institutions to treat all beneficiaries equally, without discrimination on the criteria provided by law" (art. 7). According to *the principle of transparency*, "in the process of drafting normative acts, public authorities and institutions have the obligation to inform and submit draft normative acts to public consultation and debate and to allow citizens access to the administrative decision-making process, as well as to data and information of public interest, within the limits of the law. Beneficiaries of public administration activities have the right to obtain information from public administration authorities and institutions, and they have their correlative obligation to provide beneficiaries with information ex officio or upon request, within the limits of the law". *The principle of proportionality* is defined by art. 9 of the Administrative Code. Thus, "The forms of activity of the public administration authorities must be appropriate to the satisfaction of a public interest, as well as balanced from the point of view of the effects on individuals. The regulations or measures of the public administration authorities and institutions are initiated, adopted, issued only following the assessment of public interest needs or problems, the risks and the impact of the proposed solutions". As we have already mentioned, the purpose of administration is to satisfy the public interest. According to Art. 10 entitled "Principle of satisfaction of the public interest", "authorities and public administration institutions, as well as their staff, have the obligation to pursue the satisfaction of the public interest before the individual or group interest. The national public interest has priority over the local public interest". Another principle with a general feature is that of *impartiality*, "public administration staff having the obligation to exercise their legal duties, without subjectivity, regardless of their own beliefs or interests" (art. 11). The activity of the public administration is continuous, exercising without interruption, in compliance with the legal provisions (art. 12). At the same time, the public administration constantly adapts to the needs of society (art. 13).

Continuous adaptation to society's needs is a constant concern of public authorities. In this sense strategic documents were adopted by the Government such as: Decision no. 909/2014 regarding the approval of the Strategy for the consolidation of the public administration 2014-2020 and the establishment of the National Committee for coordinating the implementation of Strategy for the consolidation of the public administration 2014-2020[10]; The 2014 Strategy regarding better regulation 2014-2020, approved by Decision 1076/2014[11]; Strategy from 2016 regarding professional training for public administration 2016-2020, approved by Government Decision no. 650/2016[12] etc.

Public administration is considered having a set of extremely diverse activities, which can be identified by simply reading the titles from the state budget or local budgets: national defense, science and culture, education, activities in the social field (social protection, public health) etc.[13]. Hence the great diversity of normative acts, which sometimes makes quite difficult the correlation process with the needs of society and implicitly citizens' access to public services.

2. Brief considerations regarding public services

The notion of *public service* has a historical content, representing "*the quintessence of public administration"*[14].

The public service is defined by the Administrative Litigation Law no. 554/2004 by reference to two fundamental notions, namely the notion of *public authority* and the notion of *legitimate public interest*. According to art. 2, para. (1) letter m), the public service represents "*the activity organized or, as the case may be, authorized by a public authority, in order to satisfy a legitimate public interest".* By legitimate public interest is understood, according to art. 2 para. (1) letter r) from Law no. 554/2004, "*the interest aimed at the legal order and constitutional democracy, guaranteeing the rights, freedoms and fundamental duties of citizens, meeting community needs, achieving the competence of public authorities".*

According to art. 5, letter kk) of the Administrative Code[15], public service means "*the activity or set of activities organized by a public administration authority or by a public institution or authorized or delegated by it, in order to*

[10] Published in Official Monitor no. 834 bis of 17.11.2014.
[11] Published in Official Monitor no. 917 of 17.12.2014.
[12] Published in Official Monitor no. 777 bis of 04.10.2016.
[13] Ioan Alexandru, Mihaela Cărăușan, Sorin Bucur, *Drept administrativ/Administrative Law,* 3rd revised and added edition, Universul Juridic, Bucharest, 2007, p. 36.
[14] *Idem*, p. 144 et seq. See in this regard: Cătălin-Silviu Săraru, *Drept administrativ. Probleme fundamentale ale dreptului public*, C.H. Beck, Bucharest, 2016, p. 243-274; Cătălin-Silviu Săraru, *Considerations on the public services in the XXI century*, „Juridical Tribune - Tribuna Juridica", Volume 6, Special Issue, October 2016, p. 160-166.
[15] The Administrative Code was adopted by Emergency Ordinance no. 57/2019, published in the Official Monitor no. 555 of July 5, 2019.

satisfy a general need or an interest publicly, regularly and continuously".

The notion of public service has acquired constitutional values through its inclusion in the texts of the Constitution[16], which makes express or implicit references to the idea of public service, either as an activity or as a set of means[17] of carrying out the activity in: art. 6 (for the state's guarantee of the right to identity); art. 7 (for the state's support of strengthening the ties of Romanians abroad in Romania); art. 21 (for ensuring free access to justice); art. 22 and 23 (to guarantee life, physical and mental integrity, as well as individual freedom); art. 26, 27, 28 (to protect private life, to guarantee the inviolability of the domicile and correspondence); Art. 31 (right to information); art. 39 (to guarantee freedom of meetings); art. 50 (for protecting persons with disabilities), art. 52 (for the exercise of administrative contentious); art. 79 (for the systematization, unification and coordination of legislation); art. 118 (for ensuring national defense, public order and national security); art. 120 (to achieve the principles of local public administration); art. 124 (for the making justice) etc.

The administrative code, in art. 580, regulates *the principles that are the base of the establishment, organization and provision of public services*: the principle of transparency; the principle of equal treatment; the principle of continuity; the principle of public service adaptability; the principle of accessibility; the principle of the responsibility of ensuring the public service; the principle of providing public services at a high level of quality.

Regarding *the principle of transparency*, public administration authorities have the obligation to inform about "*how to establish the component activities and objectives, how to regulate, organize, operate, finance, provide and evaluate public services, as well as user protection measures and mechanisms for solving complaints and disputes"*[18]. The requirement of transparency and protection of users also results from the obligations that public administration authorities have towards them[19].

Resulting from the broader principle of equality before the law, *the principle of equal treatment* is defined by Article 7 of the Administrative Code, according to which "*beneficiaries of the activity of public administration authorities and institutions have the right to be treated equally, in a non-discriminatory manner, correlative with the obligation of public administration authorities and*

[16] O. Puie, *Serviciile de utilitate publică/Public utility services*, Ed. Universul Juridic, Bucharest, 2012, p. 16.

[17] A. Iorgovan, *Tratat de drept administrativ /Treaty on Administrative Law*, vol. I, 4th edition, All Beck, Bucharest, 2005, p. 185.

[18] Art. 580 para. (2) of Administrative Code.

[19] Local public administration authorities have the following obligations towards users of public utility services: to *consult* user associations to establish local policies and strategies and the methods of organization and operation of services; to periodically inform users about the state of public utility services and their development policies; to mediate and resolve conflicts between users and operators, at the request of one of the parties [art. 9 para. (1) the second sentence, letters e), f), g) from Law no. 51/2006].

institutions to treat all beneficiaries equally, without discrimination based on the criteria provided by the law". *The principle of equal treatment* in the provision of public services implies "*the elimination of any discrimination against the beneficiaries of public services based, as the case may be, on criteria of ethnic or racial origin, religion, age, gender, sexual orientation, disability, as well as ensuring the application of certain rules, requirements and identical criteria for all authorities and bodies providing public services, including in the public service delegation process"*[20].

The principle of continuity is provided by article 580 para. (4) of Administrative Code and has in mind the development of the public administration activity *without interruptions, in compliance with the legal provisions*[21]. But the continuity in the provision of public services must be considered starting from the existence of completion periods, programs, etc., according to the specialized literature[22], in the sense of not absolutizing the expression "*without interruptions",* in terms of the actual provision of the activity. The public service will be abolished in the situation where the public interest is no longer justified.

The principle of adaptability implies the obligation of the public administration to respond to the needs of society by organizing public services[23]. Adaptability is a real obligation for public administration[24]. Considering the changes that are constantly occurring in society, public authorities have the obligation to adapt their activity to the needs of the community.

To comply with *the principle of accessibility*, which requires ensuring access to public services for all beneficiaries, especially those services that respond to their basic needs, public authorities must consider, from the foundation phase of the establishment of the public service, the aspects related to at cost, availability, adaptation, proximity[25].

The principle of responsibility for the provision of the public service im-

[20] Art. 580 para. (3) of Administrative Code.

[21] The Administrative Code does not specify what these provisions are, but we have in mind the provisions of the Social Dialogue Law no. 367/2022, regarding the obligation to provide certain public services in the event of a strike. We exemplify in this sense the provisions of art. 173 para. (1), according to which "*In the sanitary and social assistance units, telecommunications, radio and public television, in the units of the national energy system, the operative units from the nuclear sectors, in the railway transport units, in the units that ensure the transport in common and the sanitation of the localities, as well as the supply of the population with gas, electricity, water and heat, the strike is allowed on the condition of ensuring at least one third of the normal activity, spread over the entire duration of the day, which does not endanger life and the health of the population and/or the operation of facilities in complete safety*". Law no. 367/2022 was published in the Official Monitor of Romania, Part I, no. 1238 of 22.12.2022.

[22] V. Vedinaș, *Tratat teoretic și practic de drept administrativ/Theoretical and practical treatise on administrative law*, Volume II, Universul Juridic, Bucharest, 2018, p. 407.

[23] Art. 580 para. (5) of Administrative Code.

[24] V. Vedinaș, *op. cit*., vol. II, 2018, p. 408.

[25] Art. 580 para. (6) of Administrative Code.

plies the existence of a competent public administration authority with the provision of the public service, independent of the way of management and provision of it by the beneficiary[26]. Also, public authorities must respect both the quality standards[27] and the cost standards[28] used to provide public services. These are the requirements of providing public services at a high level of quality. In this sense, throughout the duration of the provision of public services, the public authorities establish and monitor the quality indicators for each public service[29].

3. The digitalization of public services

Naturally, starting from the purpose of public services, they must clearly have an accessible feature, and the fulfillment of their purpose must be as limited as possible in time so that the effectiveness of the principles stated in the previous section is fully achieved.

Thus, the digitalization of public services represents a set of activities necessary for the adaptation of all legally regulated processes to transfer the stages of their fulfillment to automated information technology infrastructures organized by artificial intelligence.

The 2021-2024 Government Program, as it was adopted, in Annex no. 2 of Parliament Decision no. 42/2021 for the granting of confidence to the Government[30], provides as objectives, among others, "digitalization of transport", "digital transformation of public services offered to citizens by the structures of the Ministry of Internal Affairs", "digital transformation of the economy and administration", "reindustrialization of Romania through the creation of industrial ecosystems and a network of industrial hubs and the promotion of digital technologies, modern production techniques, new materials and the development of the circular economy", "digitalization of the energy sector by promoting the production of electricity from renewable sources, energy efficiency and technologies, accelerating digitalization processes to improve public services", "system preparation of education: generalized connectivity, (...), digital content for all subjects and all levels, training of all teaching staff for digital pedagogy, dedicated and secure assessment platforms"[31].

---

[26] Art. 580 para. (7) of Administrative Code.

[27] "*The set of quality norms in the provision of a public service and/or of public utility, established by normative acts"* [art. 5, point 42, letter nn) from Administrative Code].

[28] "*The normative costs used to determine the number of resources allocated to the local budgets of the administrative-territorial units in order to provide a public service and/or public utility at the quality standard established by normative acts"* [*art.* 5, point 43 letter oo) from Administrative Code].

[29] Art. 580 para. (8) of Administrative Code.

[30] Published in the Official Monitor of Romania, Part I, no. 1122 of November 25, 2021.

[31] For an even more precise specificity, we expose in the field of social policy, the digitalization of public services, as concrete measures: the digitalization of the services offered by ANOFM (National Agency for Employment) (such as the online submission of documents for the registration

The implementation of these digitalization measures of public services requires the adoption of a specific legal framework as well as the identification of funding sources to ensure the fulfillment of investment objectives[32]. In this sense, the National Recovery and Resilience Plan was established based on Regulation (EU) 2021/241 of the European Parliament and of the Council of February 12, 2021, establishing the Recovery and Resilience Mechanism, within which component 7 dedicated[33] to digital transformation, including both reform elements and digital infrastructure investment elements.

At the level of the European Union, more than half of the Member States have either developed new strategies in this area, or updated or revised their existing strategies (for example, Cyprus, Germany or Finland).

As far as the reform elements are concerned, they are mainly embodied in the regulation of strict areas, such as the field of interoperability or cyber security, regulated matters with an obvious novelty both domestically and internationally. Later, as a stage in the digitalization process, the infrastructure of the government cloud is created, as a technical-operational ensemble that will host information for several institutions and public authorities from several policy areas of the state, considering that it will serve both services, public as well as private, respectively it will have a hybrid feature.

As for the previously mentioned areas, we will further explain the two regulations in detail.

---

of beneficiaries and the granting of benefits, the possibility to register and participate in online training courses and the assessment of professional skills, online counseling sessions) and the modernization of the infrastructure; digitization of the Territorial Labor Inspectorates (ITM), aimed at the control activity in the field of labor relations and occupational safety and health (computer system, electronic signatures, simplification of the notification procedure). In addition, the REGES-ONLINE project is expected to digitalize the relationship between territorial labor inspectorates and employers, facilitating the transmission of data on employees and their individual employment contracts; digitalization of social assistance benefits managed by the National Agency for Payments and Social Inspection - ANPIS (including the operationalization of the digital platform for the implementation of the minimum income of inclusion). In this sense, the development of tools for real-time communication with citizens and electronic management of files related to social benefits and benefits is being considered; the digitalization of databases, as well as the way of correspondence with the beneficiaries of the services offered by the territorial public pension houses; storing information/archives in digital databases; training courses in the field of digital skills for ANOFM, ANPIS and IM employees (see the 2021-2024 Governance Program, as it was adopted, at Annex No. 2 of Parliament Decision No. 42/2021 for granting the Government's confidence, published in the Official Monitor of Romania, Part I, No. 1122 of November 25, 2021.

[32] See general standards in investments in Cristina Elena Popa Tache**,** *Ranking of Treatment Standards in International Investments,* „International Investment Law Journal", Volume 1, Issue 1, February 2021, pp. 79-87.

[33] Published in the Official Journal of the European Union, L 57 of 18.2.2021.

3.1. Law no. 242/2022[34] on the exchange of data between IT systems and the creation of the National Interoperability Platform

The regulatory framework of the Law aims at adopting measures related to technologies, equipment, software programs and the data used by them, to contribute to increasing the degree of interconnection between the IT systems of the authorities and public institutions and to facilitating the exchange of data between them, starting from the principles and objectives of the European Interoperability Framework[35].

The creation, operationalization and administration of the tool/means necessary for the delivery in an integrated format of several electronic services through the implementation of the interoperability platform is thus regulated, as well as the establishment of the attributions of public authorities and institutions regarding the use and integration into the National Interoperability Platform, as well as the data exchange, respectively the attributions of the public authority responsible for its creation, development and administration.

By regulating the field of interoperability, the aim was to increase the quality of public services by facilitating the exchange of data between IT systems, reducing the bureaucratic and administrative tasks of natural and legal persons and increasing the transparency of the use of data by public authorities and institutions.

The operating principle of the interoperability process is based on voluntary participation, which requires the existence of a data exchange contract, where legal entities under private law, respectively individuals who exercise regulated liberal professions, who own computer systems and have data of interest to the authorities and public institutions, will ensure access to the latter. Exceptions to interoperability are the basic registers managed by the institutions of the national defense system, public order, and national security, except for those necessary to provide public services, respectively the basic registers for which the authorities and public institutions expressly request interconnection with the National Platform of interoperability.

Achieving interoperability is exercised through reference rules (hereinafter referred to as NRRI), which contain measures and obligations for central and local public authorities and institutions, in order to ensure interoperability between public authorities and institutions or private entities for the provision of public services. NRRIs contain a set of common elements such as vocabulary, concepts, principles, recommendations, standards, specifications and practices.

---

[34] Published in the Official Monitor of Romania, Part I, no. 752 of July 27, 2022.

[35] See in this regard COM(2017) 134 final *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions* - European Interoperability Framework - Implementation Strategy, document accessible at the following internet address: https://eur-lex.europa.eu/legal-content/RO/TXT/HTML/?uri=CELEX:52017DC0134&from=en.

The use of NRRI by public authorities and institutions must respect at least the following principles[36]:

a) the principle of re-use, respectively the authorities and public institutions cooperate for the development of common IT solutions, in order to provide public services, share and reuse components of IT solutions, in order to provide public services.

b) the principle of effectiveness and efficiency, respectively the IT systems that are the basis of electronic public services will be designed or adapted to easily allow the transfer of data between them, in compliance with the legislation on the protection of personal data.

c) the principle of administrative simplification, that is, public authorities and institutions design or adapt their public services for an electronic working environment, streamlining and simplifying the administrative processes underlying the provision of those public services.

d) the principle of security and confidentiality, according to which public authorities and institutions guarantee respect for privacy, confidentiality, authenticity, integrity, non-repudiation of data and the prohibition of the unauthorized transfer of information provided by users.

e) the principle of subsidiarity and proportionality, according to which the national approach in the field of interoperability of IT systems for the provision of public services is aligned with the European one, which it extends and adapts to national needs.

f) the principle of transparency establishes that the published documentation is detailed and updated at least in terms of semantic level of the external interfaces of the IT systems through which public services are provided.

g) the principle of administrative openness according to which the data held by public authorities and institutions, except for those for which legal restrictions are applied and which are subject to personal data protection regulations, are published as open data.

h) the principle of information conservation, respectively the information held by public authorities and institutions is modified only in accordance with the applicable regulations in the respective field and can be accessed in accordance with the legislation on IT security, personal data protection and archiving.

i) the principle of non-discrimination, respectively the authorities and public institutions will take measures to make electronic services available to people who rarely or never use the online environment, providing them with additional ways to access public services without additional costs.

j) the principle of neutrality and adaptability, respectively when defining an electronic public service, public authorities and institutions will take into account the functional requirements and avoid imposing a technology or a product

[36] See the provisions of art. 4 of Law no. 242/2022 on the exchange of data between IT systems and the creation of the National Interoperability Platform.

on partners, in order to be able to adapt to the technological environment which continuously evolves.

k) the principle of focusing on the user, respectively the requirements of the citizen must determine which services are needed and how they are provided.

l) the principle of inclusion and accessibility, respectively authorities and public institutions will use information technology to create equal opportunities for citizens and the business environment through electronic public services publicly presented and accessible without discrimination.

m) the principle of multilingualism, respectively multilingualism must be carefully considered when designing public electronic services.

The authorities and public institutions responsible for the creation and implementation of the National Interoperability Platform are the Ministry of Research, Innovation and Digitalization, exercising the regulatory and monitoring function, as well as the Authority for the Digitalization of Romania, which exercises the function of monitoring, control, and evaluation of the implementation of policies in the field of interoperability[37]. The separation of functions is a principle for ensuring compliance with the principles stated above.

3.2. Law no. 58/2023[38] on security and cyber defense of Romania, as well as the modification and completion of some normative acts

It is the normative act that establishes the legal and institutional framework regarding the organization and conduct of activities in the fields of cyber security and defense, the cooperation mechanisms, and the responsibilities of the institutions with attributions[39] in the mentioned fields.

Cyber security and defense are achieved by adopting and implementing policies and measures to identify, prevent and counter vulnerabilities, risks and threats in cyberspace[40].

The process of ensuring cyber security and defense is carried out according to the following principles:

a) the principle of personality, assuming the responsibility for ensuring the cyber security and/or cyber defense of a system, a network and/or an IT service rests with the natural or legal person who owns, organizes, administers and/or uses them, depending on the case.

b) the principle of full protection, according to which the natural or legal person responsible for the security and/or cyber defense of a system, a network

[37] See art. 14 of Law no. 242/2022 on the exchange of data between IT systems and the creation of the National Interoperability Platform.

[38] Published in the Official Monitor of Romania, Part I, no. 214 of March 15, 2023.

[39] See art. 10 of Law no. 58/2023 on the security and cyber defense of Romania, as well as for the modification and completion of some normative acts.

[40] For international level see Dennis Broeders, *Private active cyber defense and (international) cyber security—pushing the line?*, in „Journal of Cybersecurity", Volume 7, Issue 1, 2021, p. 2-12, https://doi.org/10.1093/cybsec/tyab010.

and/or an IT service is responsible for managing the risks associated with them and their connections with other systems, networks and/or or third-party IT services, as well as the implementation of technical and organizational measures necessary for cyber protection.

c) the principle of minimization of effects, according to which in the event of a cyber security incident, the natural or legal person responsible for the security and/or cyber defense of the system, network and/or IT service in question takes measures to avoid amplifying the effects and expanding of them to other systems, networks and/or IT services on their own responsibility or on the responsibility of other natural or legal persons.

d) the principle of collaboration, cooperation and coordination consists in carrying out, jointly by the natural or legal persons responsible, all the activities that ensure the security and/or defense of the IT systems, networks and services that are the subject of this law, as well as the management cyber security incidents, mitigating the effects and eliminating the situations that generated the cyber alert states established at the national level.

3.3. Emergency Government Ordinance no. 89/2022[41] on the establishment, administration and development of infrastructures and cloud IT services used by public authorities and institutions

Thus, it is regulated the general legal regime on the establishment, administration, and development, at national level, of a hybrid cloud infrastructure, the Government Cloud Platform, consisting of a private cloud component, hereinafter referred to as the Government Private Cloud, and resources and certified public services from other public or private clouds. The governmental private cloud is operationally managed by ADR and consists of a set of IT, communications and cyber security resources owned by the Romanian state, interconnected at the service level with public and/or private clouds.

The authorities responsible for the achievement of the private governmental Cloud are the Ministry of Research, Innovation and Digitalization and the Authority for Digitalization of Romania, in collaboration with the Special Telecommunications Service and the Romanian Information Service.

The IT systems used by central public authorities and institutions are developed to be suitable for migration to or interconnected with the Government Private Cloud and required to migrate electronic public services to the Government Private Cloud.

This regulation does not apply to the IT systems of public authorities in the field of defence, public order and national security, nor to those of the public authorities provided for in the Constitution in title III, chapters I, II and VI, with the exception of those systems that provide electronic public services, which they

[41] Published in the Official Monitor of Romania, Part I, no. 638 of June 28, 2022.

will interconnect with the governmental private Cloud, respectively of the IT systems for which the respective authorities expressly wish to use its resources and services.

4. Conclusions

In the current context, with the related challenges, the digitalization of public services is a mandatory requirement, which will represent a solution for the uniqueness of the stages within the technical-material operations, aspects that will eliminate any possible violations of fundamental rights and freedoms. Digitalization aims not only at facilitating citizens' access to the benefits of public services, but also at changing the perception of citizens towards the public administration, the goal being the achievement of a transparent public administration, as close as possible to the citizen. But to achieve these objectives, it is necessary to adopt a strategy that establishes the methods and stages of effective implementation of the digitalization of public services in our country[42].

Bibliography

1. Administrative Code, approved by the Emergency Ordinance of the Government no. 57/2029, published in the Official Monitor no. 555 of July 5, 2019, with subsequent changes.
2. Antonie Iorgovan, *Tratat de drept administrativ/ Treaty on Administrative law*, vol. I, 4th edition, All Beck, Bucharest, 2005.
3. Cătălin-Silviu Săraru, *Considerations on the public services in the XXI century*, „Juridical Tribune - Tribuna Juridica", Volume 6, Special Issue, October 2016.
4. Cătălin-Silviu Săraru, *Drept administrativ. Probleme fundamentale ale dreptului public/Administrative law. Fundamental problems of public law*, C.H. Beck, Bucharest, 2016.
5. Cristina Elena Popa Tache**,** *Ranking of Treatment Standards in International Investments,* „International Investment Law Journal", Volume 1, Issue 1, February 2021.
6. Dennis Broeders, *Private active cyber defense and (international) cyber security—pushing the line?*, in „Journal of Cybersecurity," Volume 7, Issue 1, 2021, https://doi.org/10.1093/cybsec/tyab010.
7. Emergency Government Ordinance no. 89/2022 on the establishment, administration and development of infrastructures and cloud IT services used by public authorities and institutions, published in the Official Monitor of Romania, Part I, no. 638 of June 28, 2022.

[42] As it appears from the Digitization Report - Q2 2022 (April - June 2022) of ADR, the Authority for Digitization of Romania and the Technical University of Cluj Napoca are implementing a project aimed at developing the first national artificial intelligence strategy - https://www.adr ... for the efficiency of the activity", code SIPOCA 704 Activity A6.1. The national strategic framework in the field of artificial intelligence).

8. Ioan Alexandru, Mihaela Cărăuşan, Sorin Bucur, *Drept administrativ/ Administrative law*, 3rd revised and added edition, Universul Juridic, Bucharest, 2007.
9. Law no. 58/2023 on security and cyber defense of Romania, as well as the modification and completion of some normative acts, published in the Official Monitor of Romania, Part I, no. 214 of March 15, 2023.
10. Marin Văraru, *Manual de drept administrativ/Handbook of administrative law*, Imprimeria statului, Chișinău, 1925.
11. Oliviu Puie, *Serviciile de utilitate publică/Public utility services*, Universul Juridic, Bucharest, 2012.
12. Verginia Vedinaș, *Tratat teoretic și practic de drept administrativ/ Treaty on Theoretical and practical administrative law*, Volume II, Universul Juridic, Bucharest, 2018.

Blockchain Technology and Smart Contracts - Public Policy Needed in the Technology Race

Associate professor **Camelia Daciana STOIAN**[1]
Professor **Dominic BUCERZAN**[2]
Associate professor **Crina Anina BEJAN**[3]

Abstract

To write about a branch of law entitled "new technologies" places us in a challenging but topical realm because we can only identify in a fragmentary way the meaning of a set of legal rules that have been promulgated by the legislature, and even less the positive law that is actually applicable at national level or even in most EU countries. However, it is not only with this thought that we proceed in the conception of the present material, but also with the idea that has become dominant as a business concern, an idea that highlights the prerogative of any person to "try his luck" by concluding a coded agreement , using a laptop and at the same time at least one other subject of law willing in consensus to use blockchain technology. We can also visualize the public official automatically enrolled in the digitization process, acting as a "business partner" of the public administration and performing in the context of the current legal area mismatch service duties using blockchain technology in energy market procurement. To conclude a so-called "smart contract" by means of blockchain technology certainly implies an agreement of wills and the typed intention of the parties concerned in a legal framework not regulated by general legal rules or specific and applicable particular provisions. We thus aim to quantify and even outline a legitimate content with finality, which aims at what as early as 2018 at the level of the Committee on International Trade was highlighted and expressed in the Report[4] indicating blockchain technology as a policy and business practice of the future that seems to have already caught up with us. This paper proposes a statistical study that reflects the integration of the concepts of blockchain technology and smart contracts into the knowledge of legal-administrative practice in Romania.

Keywords: *cryptoeconomy, encrypted contract, blockchain, smart contracts, technological change and growth.*

JEL Classification: K12, K24

[1] Camelia Daciana Stoian - "Aurel Vlaicu" University of Arad, Romania, av.stoiancameliadaciana @yahoo.com.
[2] Dominic Bucerzan - "Aurel Vlaicu" University of Arad, Romania, dominic@bbcomputer.ro.
[3] Crina Anina Bejan - "Aurel Vlaicu" University of Arad, Romania, ratiu_anina@yahoo.com.
[4] See European Parliament motion for a resolution on the potential usefulness of blockchain technology, accessible at: https://www.europarl.europa.eu/doceo/document/A-8-2018-0407_RO.html.

1. Introduction

The emergence of blockchain technology and cryptocurrencies has influenced the financial industry, generating positive effects that have led to the development of a new economic branch, namely *the cryptoeconomy*[5].

Blockchain technology emerged in 2008 at the same time as Bitcoin, the first cryptocurrency developed by an individual or group of individuals acting under the pseudonym Satoshi Nakamoto. Bitcoin was the first widely accepted system of decentralised electronic cash. These technologies succeeded for the first time in ensuring the anonymity of users and the security of transactions between unknown third parties[6].

From their development to today, cryptocurrencies are a controversial topic. In this respect, we identify the following factors that have led to a blurred environment regarding cryptocurrencies despite the main technical aspects that this technology has solved decentrally (double spending problem, anonymity and trust between unknown third parties):

- uneven adoption as legal tender by countries around the world;
- restricting the development of this technology as legal tender and attempting to restrict it to the status of a financial asset by legislative means;
- the evolution of the exchange price of cryptocurrencies into legal tender and the fluctuations of this price;
- the direct influence of various events outside the system on the exchange price (media announcements, government decisions, energy prices)[7].

The global spread of cryptocurrencies has strengthened and stabilised the underlying blockchain platform. This technology has continued to develop technically and expand its scope beyond the perimeter of cryptocurrencies, which has led to a new stage in the development of the crypto-economic environment with the emergence of smart contracts, and so attempts are being made to add a legal side to the already complex system.

The second phase of evolution of the cryptoeconomy started with the im-

[5] Khan, S.N., Loukil, F., Ghedira-Guegan, C. et al., *Blockchain smart contracts: Applications, challenges, and future trends*. Peer-to-Peer Netw. Appl. 14, 2901-2925 (2021). https://doi.org/10.1007/s12083-021-01127-0.

[6] Bucerzan, D., Bejan, C.A. (2021). *Blockchain. Today Applicability and Implications*. in: Balas, V., Jain, L., Balas, M., Shahbazova, S. (eds.) *Soft Computing Applications. SOFA 2018. Advances in Intelligent Systems and Computing*, vol. 1221. Springer, Cham, p. 152-164, https://doi.org/10.1007/978-3-030-5 1992-6_13.

[7] Bejan, Crina Anina, Dominic Bucerzan, and Mihaela Daciana Crăciun. *Bitcoin price evolution versus energy consumption; trend analysis.* „Applied Economics" (2022): 1-15. Bucerzan, D., Bejan, C.A. *op. cit.*, (2021), p. 155; Bejan, C.A., Bucerzan, D., Crăciun, M.D. (2023). *Perspectives of Cryptocurrency Price Prediction*. In: Ciurea, C., Pocatilu, P., Filip, F.G. (eds.) *Education, Research and Business Technologies. Smart Innovation, Systems and Technologies*, vol 321. Springer, Singapore. https:// doi.org/10.1007/978-981-19-6755-927.

plementation of *smart contracts*. These consist of the use of computerised cryptographic protocols to automatically verify, negotiate and agree between unknown parties in a decentralised manner in *a circumspect environment* such as the internet[8]. The idea of smart contracts was first coined around 1994 by American computer scientist Nick Szabo. He proposed the use of computer protocols to enforce the terms of a contract. However, the economic and communications infrastructure at the time could not support the implementation of the necessary protocols[9].

Ten years after the launch of the smart contract idea, around 1994, the first platform to facilitate the development of smart contracts appeared. It was initiated by programmer Vitalik Buterin and is called Ethereum[10]. The platform is based on the blockchain technology advanced by bitcoin and supports a wide variety of programming languages (Solidity, Serpent, Yul, etc.) for implementing smart contract code.

Since the launch of Ethereum, other blockchain technology-based platforms have emerged and taken over the implementation of the smart contract function. In 2016, the Cordana platform for financial services was launched, bringing improvements in transaction rates. The Quorum platform introduces technical enhancements on the execution of smart contracts on the blockchain in privacy[11]. The Hyperledger Fabric platform, developed by IBM, enables modular and versatile smart contract programming making it suitable for implementation in various economic and industrial branches such as logistics, education, various businesses[12].

The adoption of smart contracts by business has led to the emergence of decentralised applications, through which unknown users can interact for commercial, financial and legal purposes without the presence of a central authority guaranteeing the identity of users and transactions between them[13].

The positive security effects generated by blockchain technology applied to cryptocurrencies have also spilled over to the smart contracts branch, but from a system security point of view it has not had the cryptocurrency path due to the shortcomings generated by the contradiction of the technical (coding) component and the legislative/legal aspects in the traditional economic environment of[14].

---

[8] Khan, S.N., Loukil, F., Ghedira-Guegan, C. et al., *op. cit*., 2021, p. 17.

[9] Mark Giancaspro, *Is a 'smart contract' really a smart idea? Insights from a legal perspective*, „Computer Law & Security Review", Volume 33, Issue 6, 2017, p. 825-835, ISSN 0267-3649, https://doi.org/10.1016/j.clsr.2017.05.007.

[10] Bin Hu, Zongyang Zhang, Jianwei Liu, Yizhong Liu, Jiayuan Yin, Rongxing Lu, Xiaodong Lin, *A comprehensive survey on smart contract construction and execution: paradigms, tools, and systems*, „Patterns", Volume 2, Issue 2, 2021, p. 1-51, ISSN 2666-3899, https://doi.org/10.1016/j.patter.2020.100179.

[11] Ibid, footnote 9.

[12] Ibid, footnote 4.

[13] Ibid, footnote 1.

[14] Ibid, footnote 1.

In this article we propose the following goals: to identify the possible vulnerabilities generated by the implementation of smart contracts and the contradictions resulting from the Romanian legislation; to propose technical and legal solutions to the identified vulnerabilities; as well as a statistical study reflecting the degree of accommodation and acceptance of this technology in the legal, commercial and administrative environment in Romania.

2. Blockchain technology - analysis in the context of the topic

The history of the industrial revolution so far marks four main stages of development: mechanisation, electrification, automation and digitalisation[15].

Thanks to technological progress, marked by the development of areas such as the Internet of Things (IoT)[16], information technology, artificial intelligence, business intelligence[17], blockchain, etc., today we are witnessing the beginning of a new industrial era (see Figure 1).

While until now computers and the internet have been used to manage physical resources and values, blockchain technology offers the possibility to create digital resources[18], the first implementation of its kind being cryptocurrencies. Blockchain technology is a complex system and is the result of the convergence of computer science, mathematics, economics and cryptography.

At the same time, it is the starting point for the second stage of the digital economy's evolution. The steps of development and evolution of Blockchain technology can be structured in four stages as follows[19]:

- *Origins*: 1990 - advent of distributed computing systems and Distributed Ledger Technology, inspired by accounting procedures; 2008 - advent of Bitcoin and cryptocurrencies;
- *Transactions*: 2011 - development of systems that allow cash to be linked to cryptocurrencies; 2012 - development of currency transfer and digital payment systems between cryptocurrencies and traditional currencies;
- *Contracts*: 2013 - extension of blockchain technology to financial mar-

[15] Bejan, Crina Anina, Dominic Bucerzan, and Mihaela Daciana Crăciun, *op. cit*., (2022): 1-15.
[16] Szentesi, S. G., L. D. Cuc, R. Lile, and P. N. Cuc. 2021. *Internet of Things (IoT), Challenges and Perspectives in Romania: A Qualitative Research*. „Amfiteatru Economic" 23 (57): 448-464.
[17] Rad, D.; Cuc, L. D.; Lile, R.; Balas, V.E.; Barna, C.; Pantea, M.F.; Bâtcă-Dumitru, G.C.; Szentesi, S.G.; Rad, G., *A Cognitive Systems Engineering Approach Using Unsupervised Fuzzy C-Means Technique, Exploratory Factor Analysis and Network Analysis-A Preliminary Statistical Investigation of the Bean Counter Profiling Scale Robustness.* „International Journal of Environmental Research and Public Health" 2022, 19, p. 3-5, https://doi.org/10.3390/ijerph191912821.
[18] Bejan, Crina Anina, Dominic Bucerzan, and Mihaela Daciana Crăciun, *op. cit*., (2022): 1-15.
[19] Dominic Bucerzan, Crina Anina Bejan, *Wallet Key Management in Blockchain Technology*, Proceedings of the IE 2020 International Conference, ISSN 2284-7472, https://www.conference ie.ase.ro/wp-content/uploads/2020/06/ProceedingsIE2020/wallet_key_management_in_blockchain_technology.pdf.

kets and non-cryptocurrency applications; 2014 - start of ***smart contract*** development;

● *Applications*: 2015 - development of private blockchain networks by introducing a new level of security using user authentication, compared to public cryptocurrency blockchain systems; from 2016 to the present there is an evolution of blockchain-based financial markets, an expansion of this technology in various industries.

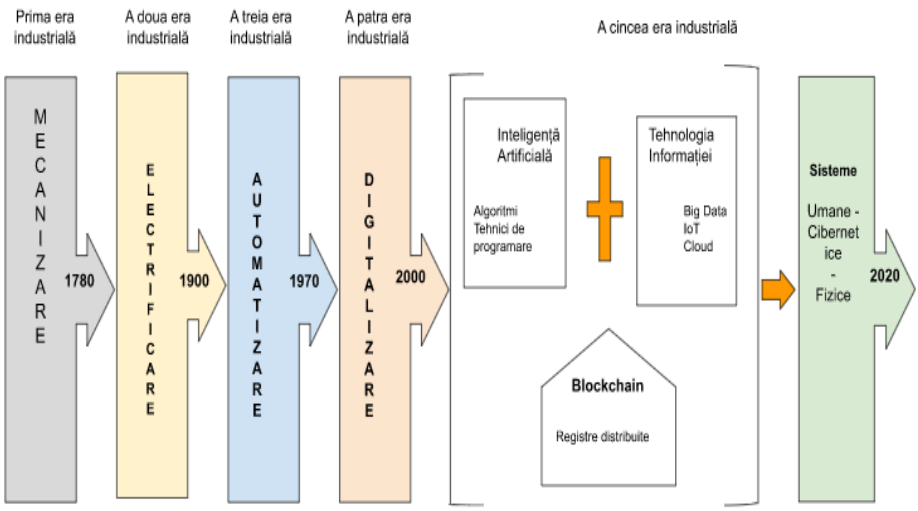

Figure 1 - Stages of technological development that have required changes in the economic, legal and administrative framework.

Blockchain technology can be seen as a security infrastructure for decentralised communication of digital information. This system has the following components: network nodes or miners, blocks, links between blocks (chaining), consensus algorithm, transactions and users[20].

Network ***nodes***, or miners, are specific hardware devices that are designed to keep transactions running smoothly by calculating the hash function, validating transactions and writing data to the block.

Data blocks are digital registers that store data transactions that take place on the network. Each block in the network can be divided into the following sequences: *a header* storing the hash value of the previous block and block identifiers, except for the root block (the first block in the network) which has no predecessor block; *a body* containing transaction data and other transaction identifiers; and *a footer* containing the hash code of the current block. The footer and header are used to chain the blocks (see Figure 2). These transaction ledgers have

[20] Bucerzan, D., Bejan, C.A. *op. cit.* (2021). p. 157.

the peculiarity that once the data is written, it cannot be subject to subsequent modifications, i.e. it is immutable. Transactions are therefore irreversible, and the transaction registers/blocks are public and can be consulted by all users.

Cryptographic *hash* functions are algorithms used in cryptography in information security processes, generally for verifying data integrity in authentication procedures, for indexing data and for digital marking. Blockchain technology introduces the use of hash functions to achieve the security chain linking blocks of data together (see Figure 2).

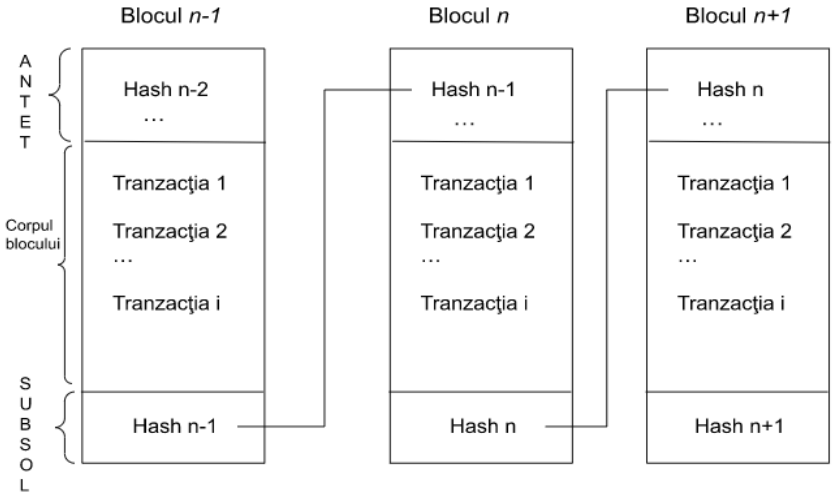

Figure 2 - The hash function and its role in linking blocks.

Each transaction block contains two hash codes: in the header the hash of the previous block and in the footer its own hash code in the calculation of which the hash of the previous block is included. This chaining method gives blockchain technology the property of immutability, in that if data changes in the transactions written to the block, the hash code in the footer of the block will change and will no longer match the hash code in the header of the next block. For such an attack on the blockchain network to be successful, the other hash codes in the entire network would have to be modified. This procedure requires very high computing power and electricity consumption, making the possible attack unprofitable. Hash functions guarantee the blockchain network's resistance to modification and the originality of the transactions entered in the blockchain.

The consensus algorithm is taken from distributed systems theory and consists of a set of procedures and rules that are designed to determine using minimal resources, under conditions of integrity and transparency, which miner will write a new block of transactions to the network. The consensus algorithm ensures that the whole system is fault tolerant. Currently within blockchain technology there are a wide variety of proposed consensus algorithms for both public

and private blockchain networks. Consensus algorithms intended for the blockchain network can be classified into two categories: algorithms based on the concept of PoW (Proof of Work) and algorithms based on voting[21]. PoW-based algorithms are encountered in public blockchain networks and are based on a reward system (in cryptocurrencies issuing new monetary units that accrue to the miners involved to reward the work done). Voting-based algorithms are used in private, corporate or commercial blockchain networks. Compared to PoW vote-based algorithms significantly reduce the problem of computational waste, but at the same time they have low flexibility and scalability[22] .

Blockchain technology through these protocols achieves decentralisation of the system so that the need for a central authority to certify the validity of data, users and transactions is eliminated. This discourages illicit and malicious behaviour within the blockchain network. Any attempt at fraud becomes very costly and unprofitable.

From a technological point of view, blockchain is a means of massively revolutionising industries and offering new opportunities. From a legislative, legal and administrative point of view, the field is at an early stage, requiring the resolution of novel challenges that may influence the global adoption of this technology. As a technology in itself may not be subject to legislative regulation, the ways in which blockchain technology can be exploited and its areas of application will be subject to legislative treatment.

3. Parties' will reflected in the language of codes - possible obstacle in implementing blockchain technology

First of all, legal practitioners naturally wonder "who" exactly has the attribute of designing a procedure for establishing the rights and obligations of the participants who decide to conclude such a smart agreement, "who" can determine the degree of access of the parties and guarantee their equality or even "who" exactly validates the operation itself? Almost certainly, an IT-ist, as we are already used to, would answer: "the system administrator". But "who" is this administrator and how can he correctly inform the participants on the whole range of organisational, technical or fundamental rights protection measures?

Also, a lawyer representing the client must intuit, in the absence of a coherent regulatory framework, the reason for the client's decision to opt for a smart contract by removing the guarantees provided by the traditional one and also other possible errors that may arise.

A first possible answer would be to keep costs down or to eliminate the

[21] Hongwu Qin, Yuntao Cheng, Xiuqin Ma, Fei Li, Jemal Abawajy, *Weighted Byzantine Fault Tolerance consensus algorithm for enhancing consortium blockchain efficiency and security*, „Journal of King Saud University - Computer and Information Sciences", Volume 34, Issue 10, Part A, 2022, p. 8370-8379, ISSN 1319-1578, https://doi.org/10.1016/j.jksuci.2022.08.017.
[22] Ibid, p. 8370.

time allocated to negotiation stages involving physical meetings or even the time for contract enforcement, as this can usually lead to years-long disputes. A chain of preventive legal logic, of reasonable due diligence, would, however, be impossible to tie up from the position of a lawyer who, through diligence, cannot foresee in the other party the existence or otherwise of attempts to manipulate the legal activity in order to direct it towards a possible illicit benefit, nor the guarantee that once such an intelligent agreement has been entered into, the other signatory may or may not have the possibility of illicit modification within his reach. And this in the absence of the possibility of direct communication with the 'someone' in charge of validating the transaction, who even in conditions of open communication cannot mediate the possibility of overvaluing the product or service purchased by confirming the transaction.

In order to give substance to a regulatory framework, the institutions responsible under the agreement to which our country is also a party on information technology (*with reference to the World Trade Organization - WTO*)[23], must work together at European level so that blockchain technology is embraced in the legislative machinery and therefore accepted by the Member States of the Union.

On the one hand, yes, this is the only way, for example, that customs and tax authorities can track and identify illicit financial flows and blockchain technology can prove its potential and absorb the confidence of international compliance. *But on the other hand, we don't have the conferral right from the start, or at least not yet*:

- a guarantee of the security of the system on the portion of cyber protection of public and even private law persons with possibly critical valences in the context of the use of smart technologies;

- an alignment of the technical (coding) component on the unitary legislative aspects applicable to the European economic sphere;

- the absence of an uncertainty on the quality of the authorized enterprise; and what is more important, total transparency therefore proof of the requirement of trust regarding the finality of the electronically sealed operation and the carrying out of the obligations by self-execution[24].

Concluding from the point of view of the parties and their representatives, related to the functioning of the blockchain technology platform implementing the function of smart contracts, we consider that one thing is certain, and here we quote and support the author Victor Marcusohn who in his article "Smart contracts, a new stage in contract law?" has accurately captured the reality of the too close nuance of technology codes in relation to human will: "*The force of law lies in the power of the judicial system to apply flexible rules, taking into account*

[23] See http://dce.gov.ro/poli-com/omc/25.pdf, consulted on 1.03.2023.

[24] See Capisizu Larisa Antonia, *Contractul juridic inteligent (smart legal contract) în dreptul privat român*, pp. 11-14, PhD Thesis - Titu Maiorescu University, Faculty of Law - Doctoral School, Bucharest, 2022.

the circumstances of the case, such as the position and relationship of the contracting parties. In contrast, computers and other 'smart' equipment are ill-equipped to make such an assessment because they are rigid, deterministic and isolated from their commercial context. Furthermore, the level of 'learning' of smart equipment has not reached the stage of understanding and implementing natural language and is still limited to executing some codes. Consequently, by not understanding the meaning of some contractual terms and strictly executing a code, one can end up in the undesirable situation where the result produced by entering into a smart contract is different from the real intention of the parties. This inadvertence is even more obvious when considering the situation where the smart contract code is not written by the parties. In practice, the person writing the code may not have entered the elements of the parties' intention correctly, and the parties, not being professional programmers, will not be able to check for themselves whether the code is consistent with their intention!"[25]

4. Professionals in public office - possible obstacle in implementing blockchain technology?

The procedures specific to world trade, to the international business environment, are subject to control by the tax, customs and intellectual property authorities, who, through their interface officials, carry out their duties of verifying the origin of the products, the place of manufacture, the characteristics and quantities declared in correspondence with the accompanying documentation and, if necessary, even with the accounting records. For the physical procedure so far, the officials are trained, their competences and skills are continuously developed, namely in order to cope with particular situations, various bottlenecks or even malfunctions. The Advocate General's Opinion in Case C-446/09, in response to the preliminary question referred by the Court of Appeal (England and Wales), gives the following example: *"Non-Community goods bearing a Community trade mark which are subject to customs supervision in a Member State and which are in transit from a third country to another third country may be inspected by those customs authorities if there are sufficient grounds for suspecting that they are counterfeit goods and that, in particular, they are intended to be placed on the market in the European Union, either in accordance with a customs procedure or by unlawful diversion, even if there is no evidence as to their destination.*"[26]

So, without any power of silence, but only through concrete actions, the officials involved in the actual transit of non-Community products bearing the

[25] Access and browse: https://www.juridice.ro/813312/contractele-inteligente-o-noua-etapa-in-cadrul-dreptului-contractelor.html#_ftn5.

[26] Access and browse: https://curia.europa.eu/juris/document/document_print.jsf;jsessionid=9ea7d2dc30db4f10f9f562d74f5d9de794d29adec8b5.e34KaxiLc3qMb40Rch0SaxuMb3v0?doclang=RO&text=&pageIndex=0&part=1&mode=DOC&docid=84313&occ=first&dir=&cid=86616.

Community trademark can take action in case of suspicion. *Will these powers change, for example, in the case of a smart contract involving a supply chain*? *These officials are not an actual party to a smart contract concluded for example between two companies trading in a supply chain operation**, but** neither can they access the contract at the moment the goods are found in customs, as it is rendered in codes as part of blockchain technology.* And then, in the context of the above case, where the recommendation is clear, i.e., to verify "*even if there is no evidence as to where they are going*", *how is verification carried out when blockchain technology has not been approved at government level for such transactions of an economic and commercial nature*?

Due to the above considerations and the situations that are beginning to emerge in the actual work of the authorities involved, the Commission organised to deal with the issues in the industry, energy and research segments has made a recommendation to the Commission dealing with international trade to invite the European Commission "*to consider the role of blockchain technology in the development of smart intellectual property rights*", even suggesting that this technology is capable of providing an alternative to the central supervisory authority in situations where this institution would not be reliable. Accepting the first part of the recommendation, we would also say that we are facing an *invitation that is* too strong and perhaps too bold in terms of the functioning of a central authority, all the more so as we do not even have the practical meaning of the concept of ***smart** IPR, let alone the* ability to include it in a process of professional development for the officials involved and to explain to them the transformation of the professional interventions traditionally carried out until now.

The reasoning set out in the above statements takes on substance and substance if we also refer to other types of smart contract[27], which involve supervision and control prerogatives on the part of public institutions or authorities. *As a first step, we envisage a gradual digitisation of the entire range of public administrations at national level, which are designed to deal with businesses and citizens, and then the step towards automation through digital identity. And this second big step would certainly involve several components running in parallel and in connection, such as upgrading civil servants respectively aligning with government initiatives to embrace blockchain technology*.

5. Reflection of findings by reference to the case study - Structural Equation Modelling method

The case study highlights the current situation in Romania regarding the acceptance and integration of the concepts of new blockchain technologies and smart contracts in the perception of the actors in the economic-legal environment.

[27] Such as those related to insurance or even purchase of electricity or purchase of real estate.

The study was administered electronically and consisted of a survey of 271 respondents in Romania whose professional activity includes elements of the legal, administrative, governmental and business environment. As these technologies are still in the testing phase in Romania, we chose to use the SEM (Structural Equation Modelling) method for the analysis. Descriptive data analysis and analytical calculations were performed using the Python language and the Google Colaboratory editor, and the SEM model was developed using Smart-PLS version 4.

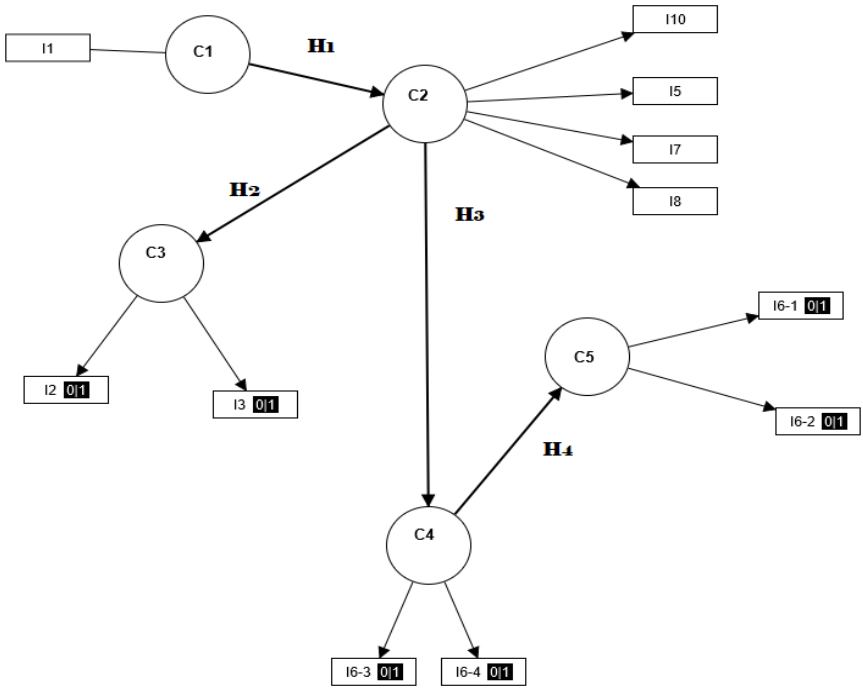

Figure 3 - Outline of the conceptual model proposed for analysis

Figure 3 shows the schematic diagram of the conceptual model proposed for analysis. The model contains five latent variables (C1, C2, C3, C4 and C5) constructed on the basis of the variables under observation using the questionnaire (questionnaire questions, I1, ..., I10). The latent variables are linked to each other by the hypotheses desired to be validated by the analysis (see Table 1). The analysis was carried out in two steps. The first stage consisted of measuring parameters reflecting the quality of the link between variables. The density of the analysed data is shown in Figure 4 by means of histograms. The second stage consisted in analysing the causal relationship between the hypotheses tested before applying the bootstrapping technique.

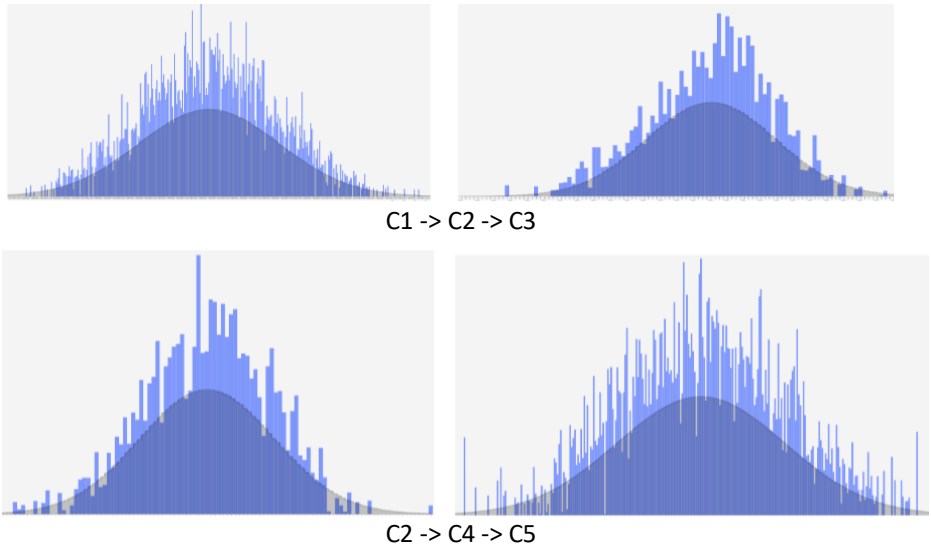

Figure 4 - Histograms of relationships between latent variables in the proposed model

Given the values obtained for the p variable, less than 0.05[28], the confirmation of the hypotheses tested can be seen in Table 1.

However, from the analysis of the responses, one aspect that needs to be highlighted is the early and timid stage of familiarity with blockchain technology and smart contracts of people working in the legal area compared to people working in the administrative area.

This can be used to promote education of the population in key economic, legal and administrative areas on the use of new technologies. We consider that the parameters of the proposed model do not show strong correlations also due to this situation of familiarization of the population with the technology under study.

Table 1 - presentation of tested hypotheses

Hypothesis Tested	Latent variable	Description of the Hypothesis	P	Result
H1	C1->C2	The category calls for professional skills compatible with new technologies, adapted to the dynamic nature of activities in the area of services carried out using blockchain technology	**0.012**	**Accepted**

[28] Hurbean, L.; Dospinescu, O.; Munteanu, V.; Danaiata, D., *Effects of Instant Messaging Related Technostress onWork Performance andWell-Being.* Electronics 2022, 11, 2535. https://doi.org/10.3390/electronics11162535.

H2	C2->C3	The need to adapt university qualifications by including in the curriculum subjects that combine IT and legal knowledge at an applied level so that the services offered subsequently as a professional are in line with the commercial practices of the future.	**0.000**	**Accepted**
H3	C2->C4	Awareness of risks plus the responsibility of assuming the application of a system in the presence of the likelihood of not being mastered in full percentage, all the more so as human control is removed from the moment of initialisation.	**0.003**	**Accepted**
H4	C4->C5	Blockchain technology being understood and perceived at the application level including on the risk side will impose its progress on the evolution of smart contracts so that legislative measures will continue to adapt to these changes in a timely manner	**0.000**	**Accepted**

6. Conclusions in relation to necessary public policies

Smart contracts are one of the most promising directions for blockchain technology outside of cryptocurrencies. Smart contracts are computer programs that automatically start executing when certain conditions are met on the network. They are technologically based on blockchain networks, but differ from cryptocurrency systems[29] .

Cryptocurrency systems allow for programming codes that are limited in size and that exclude repetitive structures to avoid infinite execution loops leading to possible flow bottlenecks in the system. Systems for smart contracts focus on programming paradigms such as decision structures[30]. If contract data cannot be written using decision structures, it is not recommended to use smart contract technology[31].

There are currently several platforms that allow smart contracts to be run and two categories of programming languages that facilitate the writing of a smart

[29] Bin Hu, Zongyang Zhang, Jianwei Liu, Yizhong Liu, Jiayuan Yin, Rongxing Lu, Xiaodong Lin, *op. cit.*, 2021, p. 10-12.

[30] Nadia-Ariadna Sava, Dacian Dragoș, *The Legal Regime of Smart Contracts in Public Procurement*, „Transylvanian Review of Administrative Sciences", No. 66 E/2022, p. 99-112, DOI: http:// dx.doi.org/10.24193/tras.66E.6.

[31] Ibid, p, 101. Raskin, Max. The *law and legality of smart contracts*, „Georgetown Law Technology Review", Vol 1:2 (2017), 305-341; https://georgetownlawtechreview.org/wp-content/upload s/2017/05/Raskin-1-GEO.-L.-TECH.-REV.-305-.pdf.

contract[32]. Smart contract programming languages fall into two categories: high-level languages - near-human language, can be used by non-specialist programmers; intermediate representation languages - allow for more robust contract compilation and security and efficiency analysis. Programming languages dedicated to smart contracts can be further technically classified into: procedural languages - the states of a contract are changed using multiple statements; and functional languages - the states of a contract are changed using multiple predefined functions[33].

Because smart contract applications have only been available for a few years, they present both opportunities and challenges[34]. There is a wide range of work in the literature[35] discussing technical and economic elements of smart contracts. However, the main challenges of this technology are of a legal nature and concern how to integrate smart contracts into the traditional concept of a legally enforceable contract[36]. The fundamental element of contract law is the *promise*. Because of the blockchain structure on which they are based, smart contracts retain this feature. Moreover, the blockchain structure imposes permanence and immutability on smart contracts. Once launched on the network (executed), smart contracts cannot be changed and the effects generated remain permanent[37]. Although these characteristics make the blockchain network highly secure and difficult to attack, in the case of smart contracts, there are authors in the literature who highlight the need to create the possibility to modify contracts in certain circumstances where the law or certain parts of the contract are not being respected[38].

Given the imprint of technological progress on economic and social processes (analogue contracts and documents have become digital, digital signatures

---

[32] Hongwu Qin, Yuntao Cheng, Xiuqin Ma, Fei Li, Jemal Abawajy, *op. cit.*, 2022, p. 8370-8379; Nadia-Ariadna Sava, Dacian Dragoș, *op. cit.*, 2022, p. 102; Raskin, Max, *op. cit.*, 2017, p. 307; Ante Lennart, *Smart Contracts on the Blockchain - A Bibliometric Analysis and Review* (April 15, 2020). Available at SSRN: https://ssrn.com/abstract=3576393 or http://dx.doi.org/10.2139/ssrn.3576393, p. 45.

[33] Bin Hu, Zongyang Zhang, Jianwei Liu, Yizhong Liu, Jiayuan Yin, Rongxing Lu, Xiaodong Lin, *op. cit.*, 2021, p. 12.

[34] Ante Lennart, *op. cit.*, 2020, p. 43; Ene, Charlotte. *Smart contracts - the new form of the legal agreements*, Proceedings of the International Conference on Business Excellence, vol.14, no.1, 2020, pp.1206-1210. https://doi.org/10.2478/picbe-2020-0113.

[35] Bin Hu, Zongyang Zhang, Jianwei Liu, Yizhong Liu, Jiayuan Yin, Rongxing Lu, Xiaodong Lin, *op. cit.*, 2021, p. 15; Hongwu Qin, Yuntao Cheng, Xiuqin Ma, Fei Li, Jemal Abawajy, *op. cit.*, 2022, p. 8370-8379; Nadia-Ariadna Sava, Dacian Dragoș, *op. cit.*, 2022, p. 98; Raskin, Max. *op. cit.*, 2017, p. 308; Ante Lennart, *op. cit.*, 2020, p. 43; Taherdoost, H. Smart, *Contracts in Blockchain Technology: A Critical Review*. „Information" 2023, 14, 117. https://doi.org/10.3390/info14020117.

[36] Raskin, Max, *op. cit.*, 2017, p. 308.

[37] Nadia-Ariadna Sava, Dacian Dragoș, *op. cit.*, 2022, p. 98.

[38] Debono, P., *'Transforming Public Procurement Contracts into Smart Contracts'*, 2019, „International Journal of Information Technology Project Management", vol. 10, no. 2, pp. 16-28; Taherdoost, H. Smart, *op. cit*., 2023, p. 117.

have become accepted and legally recognised[39]) we consider it demonstrated according to the statistical study that blockchain technology will impose its progress on the evolution of smart contracts so that legislative measures will continue to adapt to these changes. The first step towards a general legal framework for the application of smart contracts is to clarify and understand the regulatory dimension of this innovation and implement the generalised legal foundations in this direction[40].

Therefore, while the case law of the European courts does not yet provide guidelines on smart contracts for the purchase *of electricity, real estate or insurance services*, at a first glance of the concept and from the point of view of the duties of public officials, these types of contracts would not pose acute problems as long as there is a legal framework facilitating access and use of blockchain technology, which also supports the possible restoration of a document in its original form according to a certain date. Situations characterised by the use of fraudulent documents may, however, open the way to fraud, and the vigilance of the authorities in the area of financial market supervision may be affected even in relation to any simple entrepreneur. However, given that the authority or public institution with a supervisory role, i.e., the representative official, understands that the rights and responsibilities of the parties to a smart agreement involve inclusion in the structure of the network code in a way that does not subsequently allow any further operations on them, this aspect in itself would be a plus.

When it comes to smart deals involving *food chains*, trade policy has a whole different set of rules that play out in both online and physical environments, where the will of the individual directly concerned or in office can manifest itself. Online, the contract is concluded via blockchain technology and when the final product is handed over to the recipient, payment is automatically executed. Between the two moments, however, the powers of the customs, tax, etc. official are applicable, which cover and can trigger checks on private registers, accounting, correspondence, registers containing sensitive data, phytosanitary measures ordered, and categorically on goods in terms of origin or destination, without this list being exhaustive.

A review of the statistical study, which is the significant support of the present material, concluded that there are public issues in the real professional world where the combination of elements of private and public law is evidence of the emergence of ***new technology law*** as a ***discipline linking computer science, law and economics***. And from this we have deduced public policies necessary to be developed and found as finality in the body of normative acts aiming to ensure a constructive applicability of blockchain technology in close connec-

[39] Agata Ferreira, *Regulating smart contracts: Legal revolution or simply evolution?*, „Telecommunications Policy", Volume 45, Issue 2, 2021, p. 102081, ISSN 0308-5961, https://doi.org/10.10 16/j.telpol.2020.102081.

[40] Ene, Charlotte, *op. cit.*, 2020, pp.1206-1210; Agata Ferreira, *op. cit.*, 2021, p. 102081.

tion with the current mechanisms of the market economy, profit-making operations, customs activities, in relation to possible solutions in the national, European and international legislative context. *These solutions, which we have deduced from all our research, are aimed at an in-depth analysis of blockchain technology, which makes it imperative to develop them in the context of public policy options*:

- the favourable but untapped economic, social and legal impact of this technology, which can guarantee access permission for the time of interest to the database, benefiting in this respect from a time stamp;

- the possibility of allowing through blockchain technology a clear level of access by public authorities with prior notification to all participants, the aim being to prevent and detect and combat tax evasion, corruption, money laundering, etc;

- a thorough analysis of cyber security risks not only today but also in the not too distant future;

- organisation of refresher courses to facilitate the interface between officials, the assimilation of digital skills and the ability to analyse and synthesise the whole according to the legal limits of action.

Bibliography

1. Agata Ferreira, *Regulating smart contracts: Legal revolution or simply evolution?*, „Telecommunications Policy", Volume 45, Issue 2, 2021, 102081, ISSN 0308-5961, https://doi.org/10.1016/j.telpol.2020.102081.
2. Ante Lennart, *Smart Contracts on the Blockchain - A Bibliometric Analysis and Review* (April 15, 2020). Available at SSRN: https://ssrn.com/abstract=3576393 or http://dx.doi.org/10.2139/ssrn.3576393.
3. Bejan, C.A., Bucerzan, D., Crăciun, M.D. (2023). *Perspectives of Cryptocurrency Price Prediction*. In: Ciurea, C., Pocatilu, P., Filip, F.G. (eds.) *Education, Research and Business Technologies. Smart Innovation, Systems and Technologies*, vol. 321. Springer, Singapore. https:// doi.org/10.1007/978-981-19-6755-9 27.
4. Bejan, Crina Anina, Dominic Bucerzan, and Mihaela Daciana Crăciun. *Bitcoin price evolution versus energy consumption; trend analysis.* „Applied Economics" (2022): 1-15.
5. Bin Hu, Zongyang Zhang, Jianwei Liu, Yizhong Liu, Jiayuan Yin, Rongxing Lu, Xiaodong Lin, *A comprehensive survey on smart contract construction and execution: paradigms, tools, and systems*, „Patterns", Volume 2, Issue 2, 2021, ISSN 2666-3899, https://doi.org/10.1016/j. patter.2020.100179.
6. Bucerzan, D., Bejan, C.A. (2021). *Blockchain. Today Applicability and Implications*. in: Balas, V., Jain, L., Balas, M., Shahbazova, S. (eds.) *Soft Computing Applications. SOFA 2018. Advances in Intelligent Systems and Computing*, vol. 1221. Springer, Cham, https://doi.org/10. 1007/978-3-030-519 92-6_13.
7. Capisizu Larisa Antonia, *Contractul juridic inteligent (smart legal contract) în*

dreptul privat român, pp. 11-14, PhD Thesis - Titu Maiorescu University, Faculty of Law - Doctoral School, Bucharest, 2022.
8. Debono, P., *'Transforming Public Procurement Contracts into Smart Contracts'*, 2019, „International Journal of Information Technology Project Management", vol. 10, no. 2.
9. Dominic Bucerzan, Crina Anina Bejan, *Wallet Key Management in Blockchain Technology*, Proceedings of the IE 2020 International Conference, ISSN 2284-7472, https://www.conferenceie.ase.ro/wp-content/uploads/2020/06/ProceedingsIE2020/wallet_key_management_in_blockcha in_technology.pdf.
10. Ene, Charlotte. *Smart contracts - the new form of the legal agreements*, Proceedings of the International Conference on Business Excellence, vol.14, no.1, 2020, https://doi.org/10.2478/picbe-2020-0113.
11. European Parliament motion for a resolution on the potential usefulness of blockchain technology, accessible at: https://www.europarl.europa.eu/doceo/document/A-8-2018-0407_RO.html.
12. Hongwu Qin, Yuntao Cheng, Xiuqin Ma, Fei Li, Jemal Abawajy, *Weighted Byzantine Fault Tolerance consensus algorithm for enhancing consortium blockchain efficiency and security*, „Journal of King Saud University - Computer and Information Sciences", Volume 34, Issue 10, Part A, 2022, ISSN 1319-1578, https://doi.org/10.1016/j.jksuci.2022.08.017.
13. Hurbean, L.; Dospinescu, O.; Munteanu, V.; Danaiata, D., *Effects of Instant Messaging Related Technostress on Work Performance and Well-Being*. „Electronics", 2022, 11, 2535. https://doi.org/10. 3390/electronics11162535.
14. Khan, S.N., Loukil, F., Ghedira-Guegan, C. et al., *Blockchain smart contracts: Applications, challenges, and future trends*. Peer-to-Peer Netw. Appl. 14, (2021). https://doi.org/10. 1007/s12083-021-01127-0.
15. Mark Giancaspro, *Is a 'smart contract' really a smart idea? Insights from a legal perspective*, „Computer Law & Security Review", Volume 33, Issue 6, 2017, ISSN 0267-3649, https://doi.org/10.1016/j.clsr.2017.05.007.
16. Nadia-Ariadna Sava, Dacian Dragoș, *The Legal Regime of Smart Contracts in Public Procurement*, „Transylvanian Review of Administrative Sciences", No. 66 E/2022, DOI: http://dx. doi.org/10.24193/tras.66E.6.
17. Rad, D.; Cuc, L. D.; Lile, R.; Balas, V.E.; Barna, C.; Pantea, M.F.; Bâtcă-Dumitru, G.C.; Szentesi, S.G.; Rad, G., *A Cognitive Systems Engineering Approach Using Unsupervised Fuzzy C-Means Technique, Exploratory Factor Analysis and Network Analysis-A Preliminary Statistical Investigation of the Bean Counter Profiling Scale Robustness*. „International Journal of Environmental Research and Public Health" 2022, 19, 12821. https://doi.org/10.3390/ij erph191912821.
18. Raskin, Max. The *law and legality of smart contracts*, „Georgetown Law Technology Review", Vol 1:2 (2017), https://georgetownlawtechreview.org/wp-content/uploads/2017/05/Raskin-1-GEO.-L.-TECH.-REV.-305-.pdf.
19. Szentesi, S. G., L. D. Cuc, R. Lile, and P. N. Cuc. 2021, *Internet of Things (IoT), Challenges and Perspectives in Romania: A Qualitative Research*. „Amfiteatru Economic" 23 (57).
20. Taherdoost, H. Smart, *Contracts in Blockchain Technology: A Critical Review*.

„Information” 2023, 14, 117. https://doi.org/10.3390/info14020117.