ANALELE ŞTIINŢIFICE
ALE
UNIVERSITĂŢII „ALEXANDRU IOAN CUZA” DIN IAŞI
(SERIE NOUĂ)

ŞTIINŢE JURIDICE

TOM LXX / 2, 2024

Editura Universităţii „Alexandru Ioan Cuza” din Iaşi

Redactor: dr. Marius-Nicuşor GRIGORE
Tehnoredactare: Florentina CRUCERESCU

ISSN: 1221-8464
ISSN-L: 1221-8464

Adresa redacţiei:
Universitatea „Alexandru Ioan Cuza" din Iaşi
Facultatea de Drept
Bd. Carol I, nr. 11
Iaşi, România, 700506

Cuprins

Playing God: Human Digital Twin. A Legal Approach
Carmen Tamara UNGUREANU, **Ștefan Răzvan TATARU** 5

Dispatch of the Court Decision by E-mail
Cătălin LUNGĂNAȘU, **Claudia ROȘU** 25

AI Ethics: The Bias Puzzle
Alexandru CHISTRUGA 37

Evolution of Legal Systems in the Digital Era: An Analysis of Artificial Intelligence in E-Business
Elena SÂRGHI, **Marian ILEANA** 53

AI Use in the Workplace. Some Legal Risks and Challenges
Dana VOLOSEVICI 65

Digitalizarea pieței imobiliare și a notariatului prin tehnologia *blockchain* / The Digitalization of the Real-estate Market and the Civil Law Notary Using *Blockchain* Technology
Răzvan ANTOHIE 79

Datele cu caracter personal: *res digitalis* în sfera actelor încheiate *inter vivos* și a actelor *mortis causa* / Personal Data: *res digitalis,* Object of Acts Concluded *inter vivos* and of Acts Concluded *mortis causa*
Crina-Maria STANCIU, **Codrin-Alexandru ȘTEFĂNIU** 91

The European Battle for Data in Tax Administration:
Balancing Innovation and Compliance
Laura-Elena IONAȘCU (POSTOLACHE) 107

General Considerations and Perspectives on New Artificial Intelligence (AI) Systems. Influence of AI Systems in the Area of Criminal Liability for Breaches of Integrity Rules in Public Office
Carmen Lorena VLĂDUȚ 123

ANALELE ŞTIINŢIFICE ALE UNIVERSITĂŢII „ALEXANDRU IOAN CUZA" DIN IAŞI
TOM LXX, 2, ŞTIINŢE JURIDICE, 2024

DOI: 10.47743/jss-2024-70-2-1

Playing God: Human Digital Twin. A Legal Approach

Carmen Tamara UNGUREANU[1], Ștefan Răzvan TATARU[2]

Abstract: Human Digital Twins (HDTs) seem futuristic, but the technology behind them is already a reality. Two elements make up HDTs technology: the real person and his or her digital counterpart/twin, as well as two-way communication between them. Furthermore, the actual surroundings and people that the twin interacts with in real life are transferred into cyberspace. A complete HDT does not exist, yet. In most cases, only certain aspects of human attributes are used in a particular context for specific purposes. But the technology will be able, sooner or later, to „create" a "full" HDT. This endeavour could be equated with a God creation, if we admit that God exists. To prepare to face the future, which is already here, everybody should be at least well informed. Therefore, in this article we will try to depict a comprehensible portrait of the HDTs. We will start by making a brief presentation of what Digital Twins (DTs) and HDTs technologies mean, their functioning, and their practical applications. We will focus afterwards on the legal issues concerning HDTs in an EU legal context. We will try to clarify the applicable rules and the HDTs ownership and other possible proprietary rights, such as intellectual property ones. Last, we will name a few legal and other concerns connected with HDTs.

Keywords: digital twin, human digital twin, artificial intelligence, personal data.

Introduction

Human Digital Twins systems, along with innovative technologies such as Self-aware AI, could be considered the peak of the advancement of the digital age, long characterized as disruptive, emerging or cutting-edge technologies[3]. In this

[1] Professor PhD, Faculty of Law, "Alexandru Ioan Cuza" University of Iasi, e-mail: carmen.ungureanu@uaic.ro.

[2] Lawyer PhD, e-mail: razvantataru@gmail.com.

[3] See, Gartner website, *30 Emerging Technologies That Will Guide Your Business Decisions*, [Online] at https://www.gartner.com/en/articles/30-emerging-technologies-that-will-guide-your-business-decisions, accessed July 14th, 2024; McKinsey Digital, *Tech at the edge: Trends reshaping the future of IT and business,* 21 october 2022, [Online] at https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/tech-at-the-edge-trends-reshaping-the-future-of-it-and-business, accessed July 14th, 2024; KPMG website, *The Chaning landscape of disruptive technologies – Part 2: Innovation convergence unlocks new paradigms*, 2017, [Online] at https://assets.kpmg.com/content/dam/kpmg/br/pdf/2017/07/disruptive-tech-2017.pdf, accessed July 14th, 2024; V.D. Păvăloaia, S.C. Necula,

era, the concept of Human Digital Twins (HDTs) is redefining the way we understand and interact with technology and the way we relate to the human being.

The idea of Digital Twins (DTs) and HDTs is not new. The novelty consists, above all, in its practical application rather than in the idea itself. For example, as early as 2008, in the movie Iron Man the protagonist, Tony Stark, creates a digital model of his equipment that, during actual use, gives him updates on the performance of the various systems built into the suit. Iron Man thus incorporated both DTs (which gave him real-time information and predictions about the suit's performance) and HDTs technology (which helped in collecting information about the human user, analyzing it and generating predictions about his health). Systems such as DTs or HDTs are based on Artificial Intelligence, and in Iron Man movie this is easily noticeable through the presence of Jarvis - the interactive AI system that assists and alerts the protagonist.

In a broad sense, the HDT or Personal Digital Twin[4] is a digital representation of a person that integrates biological, behavioral, and contextual data to create a holistic and dynamic picture of the individual[5]. This concept transcends the simple idea of a digital profile or virtual avatar, moving beyond static representation to capture human complexity and dynamics in real time. Through the continuous analysis of data and patterns, HDTs can provide relevant information and predictions about the health status, behavior and performance of the individual, bringing with it a potentially transformative effect in fields such as personalized medicine or the sports industry[6].

Artificial Intelligence as a Disruptive Technology—A Systematic Literature Review in Electronics 2023, 12, 1102, https:// doi.org/10.3390/electronics12051102, pp. 1-2.

[4] M. Teller, *Legal aspects related to digital twin*, in Philosophical Transactions of the Royal Society A, 4 October 2021, volume 379, Issue 2207, https://doi.org/10.1098/ rsta.2021.0023; R. Saracco, *Personal Digital Twins. A third evolution step for humankind?*, eBook, 2022, p. 23, [Online] at https://digitalreality.ieee.org/images/ files/pdf/4-2022personal-digital-twins-ebook-final.pdf, accessed on April 4th, 2024.

[5] See also: Y. Naudet, A. Baudet, M. Risse, *Human Digital Twin in Industry 4.0: Concept and Preliminary Model*, in IN4PL - Proceedings of the International Conference on Innovative Intelligent Industrial Production and Logistics, 2021, https://doi.org/ 10.5220/0010709000003062, pp. 138-140; Miller M.E., Spatz E., *A unified view of a human digital twin*, in Human-Intelligent Systems Integration, (2022) 4, https://doi.org/ 10.1007/s42454-022-00041-x, pp. 24, 28, 31; M. Miller, *Human Digital Twin and Modeling Guidebook*, in Air Force Institute of Technology - Technical Report, December 19, 2022, [Online] at https://apps.dtic.mil/sti/trecms/pdf/AD1188552.pdf, accessed on April 4th, 2024, pp. 7-8; W. Shengli, *Is Human Digital Twin possible?*, in Computer Methods and Programs in Biomedicine Update, volume 1, 2021, https://doi.org/10.1016/ j.cmpbup.2021.100014, pp. 2-4.

[6] W. Shengli, *op. cit.*, p. 2; M.E. Miller, E. Spatz, *op. cit.*, pp. 28-31; E.O. Popa, M. van Hilten, E. Oosterkamp, M.-J. Bogaardt, *The use of digital twins in healthcare: socio-ethical benefits and socio-ethical risks*, in Life Sciences, Society and Policy, issue 17, 2021, https://doi.org/10.1186/s40504-021-00113-x, p. 2; T. Liu, C. Weng, Q. Jiang, L. Jiao, Z. Ni, *Modelling Human Digital Twins Based on Physical and Mental Fusion*, in NSFC-RGC

Fortunately, a "full"/complete HDT does not exist, yet. In most cases, only certain aspects of human attributes are used in a particular context for specific purposes. The human being is too complex to be „captured" in its entirety in a HDT[7]. But, the technology will be able, sooner or later, to „create" a complete HDT. This endeavour could be equated with a God creation, if we admit that God exists.

To prepare to face the future, which is already here, everybody should be at least well informed. We will make a brief presentation of what DTs and HDTs technologies mean, their functioning, and their practical applications. We will focus afterwards on the legal issues concerning HDTs in an EU legal context. We will try to clarify the applicable rules and the HDTs ownership and other possible proprietary rights, such as intellectual property ones. Last, we will name a few legal and other concerns connected with HDTs.

1. From digital twins to human digital twins

Despite appearing to be something out of the future, DTs technology has been present and in use for a while. However, these new technologies are only „adopted" by sectors of the economy that have the resources to invest significantly in the creation of new goods or services, such as the life sciences and health care sector, the military sector, the medical field, or the automotive sector, until they are ready for widespread adoption.

Since the ideas behind DTs, and particularly HDTs, are controversial, new technologies require advertising campaigns that highlight their advantages and pique consumers' interest in using them. Disruptive technologies like HDTs are incorporated into society gradually and with a focus on opportunities and benefits rather than by means that incite distrust or anxiety.

1.1. What is a digital twin?

The DT is a virtual replica of a physical system, process or product that is periodically updated with data collected from the real-world twin and the environment in which it is located[8]. By replicating the behavior of the real-world twin under different conditions and analyzing the results, DTs technologies can be used to optimize performance, prevent hardware failures, anticipate maintenance

Conference 2023, 10.13140/RG.2.2.23742.77121, [Online] at: https://www.researchgate.net/publication/370230449_Modelling_Human_Digital_Twins_Based_on_Physical_and_Mental_Fusion, accessed on April 4th, 2024.

[7] Y. Song, *Human Digital Twin, the Development and Impact on Design,* in Journal of Computing and Information Science in Engineering, vol. 23, issue 6, 2023, Paper No: JCISE-23-1076, pp. 4-5, https://doi.org/10.1115/1.4063132.

[8] B. Tekinerdogan, *On the Notion of Digital Twins: A Modeling Perspective,* in Systems 11, issue 1, 2023, https://doi.org/10.3390/systems11010015; E.O. Popa, M. van Hilten, E. Oosterkamp, M.-J. Bogaardt, *op. cit.*, p. 2; W. Shengli, *op. cit.*, p. 2; M. Miller, *op. cit.,* p. 2.

needs and streamline processes by sending reports and suggestions to the real-world twin[9].

In the specialized literature[10], the concept of DTs has been extended to what is called Augmented Digital Twins, a complex system that interacts not only with its real-world twin but also with its environment and with other digital twins. The Augmented Digital Twins system includes, on the one hand, the physical object or system, its surroundings and the relationship with other physical entities, and on the other hand the digital twin, the environment and other digital twins corresponding to those in the real environment. The two dimensions within the Augmented Digital Twins system communicate, change concurrently, interact, and mutually influence each other.

The rationale behind the concept of Augmented Digital Twins is the desire to extend the applicability of DTs technology to humans, living beings, who come into contact with different goods and equipment and are influenced by their environment and interaction with their fellow beings.

1.2. What is meant by Human Digital Twin (HDT)?

The HDT is based on the Augmented Digital Twin model. The system comprises two components: the actual person and his/her digital counterpart, as well as two-way communication between them. Additionally, the real environment and people that the real-life twin interacts with are also included and transposed into cyberspace. The effects of situations, human contact, and environmental influences on persons justify the development of the HDT system by including these components[11].

HDT is a copy or a counterpart in cyberspace of a real person in the physical world, being a model based in principle on personal data such as age, height, weight, gender, medical data etc. [12].

The conceptual model of the DT primarily consists of three main components[13]: the real-world twin, located in the physical space; the digital twin, in cyberspace; the data and information communication interface between the twins, which ensures a two-way data transfer between physical and cyber space.

[9] H. Pascual, X. Masip-Bruin, A. Alonso, J. Cerdá, *A Systematic Review on Human Modeling: Digging into Human Digital Twin Implementations*, 2023, arxiv Publisher, https://doi.org/10.48550/arxiv.2302.03593; M. Miller, *op. cit.*, p. 2.

[10] W. Shengli, *op. cit.*, pp. 1-2.

[11] *Ibidem*, p. 4.

[12] See also the definitions provided by the specialized literature: M.E. Miller, E. Spatz, *op. cit.*, p. 28;

[13] W. Shengli, *op. cit.,* p. 2; M.E. Miller, E. Spatz, *op. cit.*, p. 25; B.R. Barricelli, E. Casiraghi, J. Gliozzo, A. Petrini, S. Valtolina, *Human digital twin for fitness management,* in IEEE Access, volume 8, 2020, pp. 26637–26664, https://doi.org/ 10.1109/ACCESS.2020.29 71576; M. Grieves, *Digital twin: manufacturing excellence through virtual factory replication*, in White paper, 2015, [Online] at: https://www.researchgate.net/ publication/ 275211047_Digital_Twin_Manufacturing_Excellence_through_Virtual_Factory_Replication, accessed on April 4th, 2024.

The communication of information within the HDT system is bidirectional and in real-time so that a change in the real-world twin produces changes in the digital twin and vice versa[14].

A HDTs system could include the digital representation of an individual or of a human class, where this class represents a group of people with various traits, characteristics, behaviours etc. [15].

Therefore, we could define a HDT as an integrated model that facilitates the description, prediction or visualization of one or more characteristics of a person or class of persons, over time and in a real environment. A HDT system is an association between the real-world twin and the human digital twin; it consists of a model of the real world twin's physical, physiological, psychological, perceptual, cognitive, emotional, and ethical aspects. The two components are integrated so that any changes made to the real world person or his digital representation also affect the other[16].

To put it in another way, as Roberto Saracco (the vice president of the *IEEE-Institute of Electrical and Electronics Engineers - Digital Reality Initiative)* said: ”*The Personal Digital Twin can act as a butler (assisting the physical entity) as an avatar (impersonating the physical entity) as an agent (like harvesting information on behalf of its physical entity). In certain situations, it can act as the digital placeholder (like in storing the person's health record).*”[17]

1.3. How does the Human Digital Twin work?

The use of advanced data collection and analysis technologies such as biometric sensors, wearable devices, 3D scanning techniques or machine learning algorithms is essential for the creation and operation of HDTs. These technologies enable the continuous collection and processing of data about the functioning of the human body and mind, thus creating a comprehensive digital counterpart to the real-world twin. Sensors are used to provide real-time information about the real twin and its environment. The data provided by the sensors can be supplemented with other categories of data such as: information obtained directly from medical personnel or medical equipment[18]; information of a subjective nature,

[14] M.E. Miller, E. Spatz, *op. cit.*, p. 29.

[15] M. Miller, *op.cit.,* p. 7-8; M.N. Kamel Boulos, P. Zhang, *Digital Twins: From Personalised Medicine to Precision Public Health*, in Journal of Personalized Medicine, volume 11, issue 8, 2021, https://doi.org/10.3390/jpm11080745, p. 4.

[16] *Ibidem*, p. 8.

[17] R. Saracco, *op. cit.,* p. 23.

[18] J. Corral-Acero, F. Margara, M. Marciniak, C. Rodero, F. Loncaric, Y. Feng, A. Gilbert, J.F. Fernandes, H. Bukhari, A. Wajdan, M.V. Martinez, M.S. Santos, M. Shamohammdi, H. Luo, P. Westphal, P. Leeson, P. DiAchille, V. Gurev, M. Mayr, L. Geris, P. Pathmanathan, T. Morrison, R. Cornelussen, F. Prinzen, T. Delhaas, A. Doltra, M. Sitges, E.J. Vigmond, E. Zacur, V. Grau, B. Rodriguez, E.W. Remme, S. Niederer, P. Mortier, K. McLeod, M. Potse, E. Pueyo, A. Bueno-Orovio, P. Lamata, *The 'Digital Twin' to enable the vision of precision cardiology*, in European Heart Journal, Volume 41, Issue 48, 21 December 2020, https://doi.org/10.1093/eurheartj/ehaa159, pp. 4556–4564.

entered directly by the real-world twin (manual data logging), such as mood, emotions or sensations; information that is difficult to track and often requires manual data entry, for example, nutrition information[19].

To develop the digital model, multiple categories of characteristics of the real twin can be collected and processed, including at least one of the following categories: physical characteristics (e.g., anthropometric or biomechanical specifications); physiological characteristics (e.g., heart rate, blood oxygen level); perceptual performance data (e.g., auditory sensitivity, visual acuity); cognitive performance data (e.g., knowledge, skills, or abilities); personality traits; emotional state (e.g., depression, anxiety); behaviour[20].

The bidirectional exchange between the digital and real-world twins provides the digital twin with the ability to sense the real world, create an understanding of the world, and act upon it through the information and predictions transmitted to the real-world twin. More specifically, communication within the HDT system involves a repetitive process with the following seven steps[21]:

- The sensors used by the real-world twin collect data on his/her state, actions and performance, as well as relevant information on the environment in which he/she operates.
- The data communication interface transmits the collected information to the digital twin.
- The data is analyzed to determine if the digital twin accurately matches the real-world twin. If inconsistencies are identified in the digital representation or in the forecasts previously made by HDT then, as appropriate, the data is updated or adjusted and the differences are explained.
- The digital twin generates and tests scenarios of future behaviour in a virtual environment.
- Predictions of future behaviour are compared to a desired state determined by the proposed objective.
- Based on this analysis, the system determines whether a modification in the structure or behavior of the system is likely to lead it towards a desired state and, if so, formulates proposals for modifications to the real twin or his/her behavior to achieve the objective.
- The proposed change is forwarded to the real-world twin and, depending on the latter's decision, is implemented or not.

This series of steps is repeated, with the real-world twin able to make decisions based on the information and predictions generated by the digital twin, in order to achieve the initial goal[22].

[19] B.R. Barricelli, E. Casiraghi, J. Gliozzo, A. Petrini, S. Valtolina, *op. cit.*, pp. 2, 8-9.

[20] M. Miller, *op. cit.*, 8; M.E. Miller, · E. Spatz, *op. cit.*, p. 28.

[21] M.E. Miller, E. Spatz, *op. cit.*, p. 25.

[22] *Ibidem.*

2. Applications of the Human Digital Twin Technology

HDTs has been implemented in various fields, such as personalized medicine, performance sports, military, industry, smart cities, or product design[23]. We will briefly present several aspects of each of these fields.

a. Personalized medicine

In the medical field, the HDT creates digital replicas of the entire human body, of a single body system or function, or of a single organ[24]. To develop a digital model, it is necessary to collect data from various sources, such as sensors, wearables, medical devices, medical records or information entered by the real-world twin[25].

The digital twin makes it possible to gain a detailed understanding of the "replicated" patient, predict the evolution of the patient's health, anticipate ineffective or potentially dangerous treatments, test the human body's reactions to different stimuli and medications. This use of digital twins is in line with researchers' desire to develop "4P medicine" – personalized, predictive, preventive and participatory[26].

Based on data released by the US Food and Drug Administration (FDA)[27], patients with diseases ranging from depression to cancer have between 38% and 75% of their prescriptions being unsuccessful. Variability amongst people taking identical medications is the cause of this. Personalized medicine aims to develop and prescribe the right drug, in the right dose, at the right time for each unique patient. With the capability to analyze in detail the characteristics and conditions of each person individually, digital twins can contribute to the implementation of personalized medicine[28].

Moreover, the medical databases collected by HDTs can be used in the development and streamlining of clinical trials, thus minimizing the participation of human subjects and their exposure to experimental treatments.

In light of the potential for gathering and keeping human digital twins in HDTs banks – which function as structured data warehouses complete with audit trail systems[29] – performing clinical research in the digital setting using data from these banks may one day become a possibility.

[23] See M.E. Miller, E. Spatz, *op. cit.*, p. 23; M. Miller, *op. cit.* pp. 8-10; H. Pascual, X. Masip-Bruin, A. Alonso, J. Cerdá, *op. cit.*, pp. 1-2.

[24] M.N. Kamel Boulos, P. Zhang, *op. cit.,* p. 4.

[25] C. Tang, W. Yi, E. Occhipinti, Y. Dai, S. Gao, L.G. Occhipinti, *Human Body Digital Twin: A Master Plan*, 18 July 2023, last revised 12 September 2023, https://doi.org/10.48550/arXiv.2307.09225, [Online] at https://arxiv.org/abs/2307.09225, accessed on July 14th, 2024, pp. 5-10; H. Pascual, X. Masip-Bruin, A. Alonso, J. Cerdá, *op. cit.*, p. 2.

[26] M. Teller, *op. cit.*, p. 2.

[27] M.N. Kamel Boulos, P. Zhang, *op. cit.*, p. 2.

[28] See W. Shengli, *op. cit.*, pp. 1, 3.

[29] According to European Medicines Agency, "*an audit trail is a secure, computer generated, time-stamped electronic record that allows reconstruction of the events relating to*

b. Performance sports

HDT could bring added value to the sports industry and performance sports by monitoring, analyzing and developing programs to improve athletes' performance, as well as assisting coaches in optimizing the behaviour and development of athletes or teams[30].

The data generated by HDT models, developed to understand human performance in the medical or high-performance sports fields, can also be utilized for product design innovation. For example, data collected from high-performance athletes and processed through the HDT system can contribute to the development of equipment that optimizes athletic performance (*product design*).

At the Olympic Games in 2024 nine of the American swimmers were guided by their digital twins[31], within a project started in 2015 by teams of researchers at Emory University and the University of Virginia.

c. Military field

HDTs also find applicability in the military field, contributing to the monitoring of troops, the development of their performances, and also to their "synchronization" with advanced military technology. For instance, a project funded by the US Air Force seeks to employ HDTs technology for aircraft pilots, aiming to develop personalized training models that enhance pilot performance, reduce injury risk, improve physiological predictions, and optimize cockpit and equipment ergonomics[32].

d. Manufacturing industry

In industry, HDTs aim to enhance productivity, ensure worker safety, and minimize manufacturing errors. For example, a digital twin system in a manufacturing environment consists of an operator handling various materials and multiple data collection systems. In this system, the model can be used to identify material handling steps that induce substantial fatigue, allowing these steps to be evaluated and redesigned. In this example, the real-world twin includes the

the creation, modification, or deletion of an electronic record." See, European Medicines Agency, *Guideline on computerised systems and electronic data in clinical trials*, March 9th, 2023, [Online] at https://www.ema.europa.eu/en/documents/regulatory-procedural-guideline/guideline-computerised-systems-and-electronic-data-clinical-trials_en.pdf, accessed on April 4th, 2024.

[30] Also, see H. Pascual, X. Masip-Bruin, A. Alonso, J. Cerdá, *op. cit.*, p. 8.

[31] K. Douglass, A. Lamb, J. Lu, K. Ono, W. Tenpas, The Mathematical Intellinger, *'Digital Twins' Give Olympic Swimmers a Boost*, July 8, 2024, [Online] at https:// www.scientificamerican.com/article/training-with-digital-twins-could-boost-olympic-swimmer-speeds/, accessed on July 14th, 2024.

[32] Z. Cheng, Z., *Human digital twin with applications*, in Proceedings of the 7th International Digital Human Modeling Symposium 7(1): 41, 2022, https:// doi.org/ 10.17077/dhm.31783; H. Pascual, X. Masip-Bruin, A. Alonso, J. Cerdá, *op.cit.*, p. 7.

production environment, the operator and data collection subsystems, and the digital twin[33].

e. Smart cities

DT technology can play a crucial role in urban development and public health decision-making by being used in various applications, such as road traffic management and flood and emergency monitoring services, in the context of smart and healthy cities. These digital twin cities go beyond traditional 3D city models, enabling smart cities to dynamically integrate key factors like time and human behaviour to better monitor indicators of interest, test different intervention scenarios, and predict how the city's system will react to changes and how its population will be affected[34].

For example, with the help of AI, DTs and HDTs technologies, the digital twin of the city of Boston helps architects and developers to visualize proposed buildings, especially very tall ones, and anticipate their impact on healthy living and working conditions in the neighboring districts[35].

3. Legal issues on HDTs in a European Union Law context

At the heart of the HDTs are data and AI systems. This means that the legal issues revolve around data and AI. Next, we will only address broadly the legal concerns, as each application of HDTs involves a specific approach.

3.1. What data needs a HDTs technology?

The symbiosis[36] between the real twin and the digital twin involves a constant supply of data, which circulates on a two-way path. The vast majority of data are personal data, hence the name Personal Digital Twin, as an alternative to HDT. The real twin, as a rule, does not have the necessary technology to take the initiative of creating the digital twin. Therefore, the "creator" is a third party, a company/organization, which pursues a specific purpose; the purpose differs depending on the field where the digital twin is used. The "creator" has the technology or has the necessary resources to get it. This technology requires data to be able to work.

What kind of data? The diversity and volume of data collected, generated and processed may vary depending on the complexity of the digital twin to be created, but in most cases at least four categories of data can be identified[37]:

- data that contributes to the creation of the model of the real twin in the digital space (for example, the model of the heart);

[33] For more examples of HDT implemented in the manufacturing industry, see: H. Pascual, X. Masip-Bruin, A. Alonso, J. Cerdá, *op. cit.*, p. 4.

[34] M. N. Kamel Boulos, P. Zhang, *op. cit.*, p. 8.

[35] *Ibidem.*

[36] M. Teller, *op. cit.*, p. 2.

[37] R. Saracco, *op. cit.*, p. 28.

- data obtained from monitoring (shadowing) of the real twin (for example, the heart rate in real time, by using trackers/wearables);

- metadata derived from the analysis of several data streams (for example, establishing the physical state of the real twin, using data such as age, weight, health, environmental, etc.); metadata is what gives "meaning" to the first two categories of data: no one is interested in what pulse a person has at any given time, but rather in whether or not that pulse is normal. This information can be obtained by analyzing various personal and ambiental data, such as, for example, the route that the real twin jogs on (at the gym, on a straight or inclined plane, outside, on mountain paths, etc.)[38];

- synthetic data; „*synthetic data is data generated through machine learning algorithms from original real-world data (i.e. data relating to existing individuals or events*)"[39]; the synthetic data is an abstract model inspired by the data of the digital twin together with the data of several other people, to establish, for example, how a person, who has a certain physical state, would react in certain circumstances[40].

What is the source of this data? The question concerns the first two categories of data, since metadata comes from their analysis/processing, and synthetic data is generated by AI, so its provenance is known.

A small part of this data is the data provided directly by the real twin, through various devices, wearables, such as smart watches, fitness trackers, smart tattoos, etc.[41]. We consider that these data are the most truthful and relevant in the digital model development process. However, most data is collected by interested third parties with whom the real twin interacts online in his/her daily activities: online shopping, payments using digital banking applications, online video games, online entertainment activities such as listening to music, watching a movie on a platform, booking a hotel using short term rentals platforms, buying a plane ticket, accessing a public service, making an appointment with a doctor online for a routine medical check-up and so on.

This information, or raw data, is worthless in its raw state. However, all the real digital twin actions leave a *digital footprint*, and the interested parties collect and process that data using AI; this way, the data becomes valuable, has a meaning and contributes to the creation of the digital twin[42].

What is the legal basis for the collection and processing of (personal) data that the algorithms making HDTs work are fed on?

[38] *Ibidem,* p. 29.

[39] A. Beduschi, *Synthetic data protection: Towards a paradigm change in data regulation?*, in Big Data & Society, 11(1), 2024, https://doi.org/10.1177/ 20539517241231277.

[40] R. Saracco, *op. cit.*, p. 29.

[41] Also, see: H. Pascual, X. Masip-Bruin, A. Alonso, J. Cerdá, *op.cit.*, p. 2; Y. Dai, J. Wang, S. Gao, *Advanced Electronics and Artificial Intelligence: Must-Have Technologies Toward Human Body Digital Twins*, in Advanced Intelligent Systems, Influence Series, vol. 4, issues 2, 2022, 2100263 (1-11), https://doi.org/10.1002/aisy.202100263.

[42] R. Saracco, *op. cit.*, pp. 28-29.

3.2. Data & applicable rules: GDPR and beyond

It is indisputable that for personal data the applicable rules are those of the GDPR[43]. HDTs technology, though, is not limited only to personal data. As we have already shown, the collected and processed data concern the status, the actions, the performance of the real twin, as well as relevant information regarding the environment in which the real person acts and interacts, including with other people. Therefore, the data cannot only be personal data, but can also be mixed data and non-personal data[44].

In EU there are a few regulations which could be useful to HDTs in certain circumstances among which: Data Act[45], Data Governance Act (DGA)[46], Artificial Intelligence Act[47], Medical Device Regulation[48], Regulation proposal on the European Health Data Space[49].

As to GDPR, this piece of transnational European legislation is applicable to both personal data and mixed data. Indirect references to mixed data exist only in the Regulation 2018/1807[50], according to which when a data set is composed of both personal data and non-personal data, Regulation 2018/1807 applies to non-

[43] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016.

[44] C.T. Ungureanu, *Proprietatea asupra datelor digitale: realități, neliniști și posibile soluții*, in Revista Română de Drept Privat no. 2/2023, pp. 75-90.

[45] Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act), OJ L, 2023/2854, 22.12.2023.

[46] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act), OJ L 152, 3.6.2022.

[47] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), OJ, L series, 12.7.2024.

[48] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC, OJ L 117, 5.5.2017.

[49] Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space, Strasbourg, 3.5.2022, COM(2022) 197 final, 2022/0140(COD), [Online] at https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex:52022PC0197, accessed on April 4th, 2024.

[50] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, OJ L 303/59, 28.11.2018.

personal data from the data set, and GDPR applies to personal data. If the personal and non-personal data in the set are inextricably linked, the entire data set is subject to the rules of the GDPR [art. 2 (2) of Regulation 2018/1807]. Data can be considered to be inextricably linked when the separation of the two types of data is either impossible or considered by the data controller to be economically inefficient or technically infeasible. The Regulations do not impose any obligation on professionals who collect, process or control data to separate personal data from non-personal data in a mixed data set. Accordingly, a mixed data set will generally be subject to GDPR rules[51].

The creation and operation of HDTs involve, above all, the collection and processing of personal data. Organizations which develop HDTs must ensure transparency about how personal data is collected and processed, respect the data subjects' rights and provide easy ways to exercise them. At the same time, HDTs developers must implement adequate technical and organizational protection measures, considering the risks involved in the use of AI in data processing.

For the lawfulness of the personal data processing, two legal grounds can be used: the *consent* of the person concerned (data subject) [art. 6 (1) a) GDPR], in the form of the standard consent, as provided in art. 7 GDPR or of the *explicit* consent (for sensitive data) [art. 9 GDPR] and the *contract* [art. 6 (1) b) GDPR].

How could data subject consent be obtained? The easiest way is to use specialized platforms. Thus, in the context of HDTs, the controller interested in processing personal data outsources the activity of obtaining the consent of the data subject *to Consent Management Platforms (CMPs)*[52]. There are a lot of CMPs[53], with OneTrust at the top of the list in 2024[54].

HDTs technology also uses a lot of sensitive personal data. According to art. 9, art. 4 (13), (14) and (15) GDPR, the following personal data is considered 'sensitive' and is subject to specific processing conditions: *personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs; trade-union membership; genetic data, biometric data processed solely to identify a human being; health-related data; data concerning a person's sex life or sexual orientation.* For these types of data, the real twin must express an explicit consent, as a mandatory and prior condition to the collection and processing of the data[55].

[51] C.T. Ungureanu, *Proprietatea asupra datelor digitale…op. cit.*, pp. 80-81.

[52] M.I. Khalid, M. Ahmed, J. Kim, *Enhancing Data Protection in Dynamic Consent Management Systems: Formalizing Privacy and Security Definitions with Differential Privacy, Decentralization, and Zero-Knowledge Proofs*, in Sensors 2023, 23, 7604, https://doi.org/10.3390/s23177604.

[53] C. Santos, M. Nouwens, M. Toth, N. Bielova, V. Roca, *Consent Management Platforms Under the GDPR: Processors and/or Controllers?*, in: N. Gruschka, L.F.C. Antunes, K. Rannenberg, P. Drogkaris(eds), *Privacy Technologies and Policy*, APF 2021, Lecture Notes in Computer Science, vol. 12703. Springer, Cham., https://doi.org/10.1007/978-3-030-76663-4_3.

[54] *Best Consent Management Platforms for 2024*, [Online] at https://www.playwire.com/blog/top-cmp-partners, accessed on April 4th, 2024.

[55] European Data Protection Board, Guidelines 05/2020 on consent under Regulation

The processing of personal data, which does not require an explicit consent, can be carried out on the legal basis of the performace of the contract concluded by the data subject (the real-world twin) with the developer of the HDT system.

The contract, as a legal basis for data processing, is not only provided for in the GDPR, but also in the Data Act, which concerns the data generated by smart devices or related services. In the Data Act (recital 5), it is stated that at the heart of data sharing are the rules of private law and the principle of freedom of contract applies.

According to Data Act at least three contacts should be concluded for the sharing of data (personal, non-personal and mixed). Initially, a contract is made between the smart product/service users and the legal or natural person that sold, rented, or leased the product/service to them (i.e., the data holder). A separate agreement is made between the smart product/service user and the third party (the data recipient) with whom the user wishes to share the data generated by the smart product/service; the purposes of the data sharing are outlined in this agreement (art. 6.1.). The user requests that the data holder make the relevant data available to the recipient rather than giving the recipient immediate access to the data. A contract that complies with the FRAND requirements ('fair, reasonable, and non-discriminatory terms') is also reached between the data holder and the recipient; this contract also includes a reasonable price [and the EC will adopt guidelines on the calculation of reasonable compensation (art. 8 and 9 DA)].

The Data Act clarifies within art. 1(5) how it interacts with other regulations, in particular with the GDPR, stating that Data Act *is without prejudice to Union and national law on the protection of personal data,* and in the event of a conflict between Data Act and the legislation on data protection the latter prevails.

As to DGA and HDTs, the rules in the DGA must be followed when certain data, which may contribute to the creation/operation of the digital twin, are shared by a data subject (who shares his personal data) or by a data holder (which can be a natural or a legal person, a public body, an international organization, which has the right to grant access to personal or non-personal data) to a data user for the purpose of joint or individual use of such data. In order to data sharing, contracts may be concluded, based on the contractual freedom of the parties, directly or through an intermediary, in exchange for a price or free of charge. The data user has the right to use the respective data for commercial or non-commercial purposes [art. 2(8)-2(10) DGA]. The notion of data user in the DGA is similar to that of data recipient in the Data Act (In European regulations there is no uniformity of terms, which can lead to confusion).

The Artificial Intelligence Act must be considered by the developer/"creator" of HDTs with regard to the use of AI systems in the formation

2016/679, version 1.1, adopted on 4 May 2020, section 4 - Obtaining Explicit Consent, [Online] at https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf, accessed on April 4th, 2024.

and operation of HDTs, having the obligation to comply with all its provisions (from the date of its application)[56].

In the situation where HDT systems are used for medical purposes or to improve the performance of the real twin, they can be included in the concept of medical devices[57], making the Regulation (EU) 2017/745 on medical devices applicable. Essentially, the application of the Regulation involves ensuring that these HDT technologies are developed in accordance with EU standards for medical devices, thus guaranteeing their safety and effectiveness for patients/users.

In the scenario where the HDTs system is based on AI technologies capable of autonomously making decisions that directly and irreversibly affect the real twin, HDTs technology developers will be required to perform an appropriate assessment of the risks and benefits associated with use in medical practice[58].

3.3. Who owns the HDT and who benefits from it?

Data ownership is a long-debated issue in the legal literature[59]. At the EU level, the approach goes beyond the idea of property rights, although data as a resource (perhaps more important than other resources, such as oil, precious stones, mineral deposits) would imply that access to it is based on a property right. European regulations use other rights that allow data sharing, namely, the *right of access* and the *right to control* the data, without making any reference to the data ownership.

Nevertheless, a HDT could be subject of proprietary rights if it is seen as a digital asset. A *digital twin entity* was considered as „*A digital asset* which implements digital representation and digital execution of a certain view of a *target entity*, and achieves *state* synchronization with the *target entity* at an appropriate rate and *credibility* through single direction or bidirectional communication."[60].

[56] C. Novelli, P. Hacker, J. Morley, J. Trondal, L. Floridi, *A Robust Governance for the AI Act: AI Office, AI Board, Scientific Panel, and National Authorities*, in Centre for Digital Ethics (CEDE) Research Paper Series, May 5, 2024, http://dx.doi.org/ 10.2139/ssrn.4817755.

[57] According to Regulation (EU) 2017/745 - art 2, *'medical device' means any instrument, apparatus, appliance, software, implant, reagent, material or other article intended by the manufacturer to be used, alone or in combination, for human beings for one or more of the following specific medical purposes: i. diagnosis, prevention, monitoring, prediction, prognosis, treatment or alleviation of disease; ii. diagnosis, monitoring, treatment, alleviation of, or compensation for, an injury or disability; iii. investigation, replacement or modification of the anatomy or of a physiological or pathological process or state; iv. providing information by means of in vitro examination of specimens derived from the human body, including organ, blood and tissue donations; and which does not achieve its principal intended action by pharmacological, immunological or metabolic means, in or on the human body, but which may be assisted in its function by such mean*s. For details on medical devices, see Ș.R. Tataru, *Soluționarea litigiilor referitoare la contractele de comerț internațional cu produse farmaceutice*, Ed. Hamangiu, 2020, p. 28.

[58] See Regulation (EU) 2017/745 - art. 2 (27) and chapters VI-VII.

[59] For a synopsis, see, C.T. Ungureanu, *op. cit.*

[60] H. Duan, S. Gao, X. Yang, Y. Li, *The development of a digital twin concept system*,

According to UNIDROIT Principles on Digital Assets and Private Law, 2023[61], a digital asset *means an electronic record which is capable of being subject to control* [art. 2(2)]. *A digital asset can be the subject of proprietary rights* [art. 3(1)]. It is not clear what kind of proprietary rights, but the authors of the Principles rely on the rule of *nemo dat quod non habet* (one cannot give what one does not have[62]): *a person can transfer only the proprietary rights that it has in a digital asset, if any, and no greater proprietary rights* [art. 9(1)]. While this does not really assist in recognizing the proprietary right on an HDT, it does demonstrate that the ownership dispute over digital assets is still far from resolved.

UK, which seems to be an appealing jurisdiction for technology related cases[63], is prepearing for legislative reforms on personal property issues, the digital assets being accomondated as property[64]. So, under English Law, a HDT could be object of personal property.

Another possible solution related to HDT ownership is that of the intellectual property rights. HDT, as a data collection, could be protected by intellectual property rights: database copyright and a *sui generis* right on the content of the database. According to Directive 96/9 on the legal protection of databases[65] (transposed into the Romanian legislation by inclusion in the Law no. 8/1996 on copyright and related rights[66]), databases which, through the choice or arrangement of elements, constitute the author's own intellectual creation are protected as such by copyright (art. 3.1.). The content of the database is protected by a *sui generis* right, according to art. 7. In order to obtain *sui generis* protection, it must be proven that a substantial qualitative or quantitative investment (financial, material and/or human) has been made either in obtaining the content or in verifying and presenting the content of the database.

Legal protection of the database does not work in all cases, however. For example, according to art. 43 of the Data Act, the *sui generis* right over the content of the database, made up of data obtained or generated by smart products or related services, cannot be recognized. The purpose of this provision is to prevent data holders from invoking the *sui generis* right, thus preventing users of smart

in Digital Twin 2023, 2:10, https://doi.org/10.12688/digitaltwin.17599.2.

[61] UNIDROIT Principles on Digital Assets and Private Law, [Online] at https://www.unidroit.org/wp-content/uploads/2024/01/Principles-on-Digital-Assets-and-Private-Law-linked.pdf, accessed on July 14th, 2024.

[62] This principle is a general one, included also in the Romanian Civil Code – art. 17(1): *Nimeni nu poate transmite sau constitui mai multe drepturi decât are el însuși/ No one can transfer or constitute more rights than he himself has.*

[63] M. Lehmann, *Seeking an Edge in Judicial Competition: England is Becoming the Leading Crypto Litigation Hub*, 11 July 2024, [Online] at https://eapil.org/2024/07/11/, accessed on July 13th, 2024.

[64] UK Law Commission. Reforming the Law, *Digital Assets*, [Online] at https://lawcom.gov.uk/project/digital-assets/, accessed on July 13th, 2024.

[65] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, OJ L 77, 27.3.1996.

[66] Law no. 8/1996 regarding copyright and related rights, OG no. 60, 26.3.1996.

products/services from exercising the *right to access and use data and the right to share data with third parties*[67].

If the HDT has a commercial use, it could be protected as a trade secret. According to the European Directive 2016/943 on the protection of *know-how* and trade secrets[68], to be protected as a trade secret the HDT should consist in information that is secret (not *generally known or easily accessible to people in the circles that normally deal* with the type of information in question); that have commercial value by being secret (having the ability to generate economic benefits to the one who controls it); that have been subject of reasonable measures, under given circumstances, for keeping it secret[69].

Anyway, only the HDTs developer, who collects data, raw or not, processes it, then creates and maintains the two-way operation of the HDTs system can benefit from legal protection. *The real twins have nothing* (unless they have the technology to create their own digital twins). The real twins don`t even have a right to access their digital twins. According to the Data Act the user of smart products/services, who could be the real twin, has the right of access only to the raw data, not to the processed data[70]. The user has the right to access and share with third parties *all raw and pre-processed data generated from the use of a connected product or a related service that is readily available to the data holder. This applies to both personal and non-personal data, including relevant metadata*[71].

Even though the real twin has no rights on his/her own digital twin, the former can benefit from the latter in one way or another.

For instance, such benefits could be related to health and the provision of adequate medical care. In this sense, a European project, launched on December 21, 2023, the *European Initiative Virtual Human Twins*[72], may be relevant. A virtual human twin (VHT) – according to this initiative – „*is a digital representation of a human health or disease state. They refer to different levels of human anatomy (e.g. cells, tissues, organs or organ systems). VHTs are built using software models and data and are designed to mimic and predict behaviour of their physical counterparts, including interaction with additional diseases a person may have. The key potential in health and care of this technology is related to targeted prevention, tailored clinical*

[67] Recital 112 DA.

[68] 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 their unlawful acquisition, use and disclosure, OJ L 157, 15.6.2016.

[69] For details, see C.T. Ungureanu, S.R. Tataru, *The legality of reverse engineering or how to legally decipher trade secrets,* SHS Web of Conferences vol. 177/2023, article number 02001, *Legal Perspectives on the Internet. COPEJI 6.0,* http://doi.org/10.1051/ shsconf/202317702001, pp. 2-6.

[70] See Data Act explained, [Online] at https://digital-strategy.ec.europa.eu/ en/ factpages/data-act-explained , accessed on April 4th, 2024.

[71] *Idem.*

[72] European Commission, *Shaping Europe's digital future. European Virtual Human Twins Initiative,* [Online] at https://digital-strategy.ec.europa.eu/en/policies/virtual-human-twins, accessed on July 4th, 2024.

pathways, and to supporting healthcare professionals in virtual environments. Examples include implementation of clinical trials for medicines and devices, medical training, surgical intervention planning, and several other potential use cases in virtual world environments."[73].

Connected to VHT project there is a regulation proposal from 2022 on European Health Data Space[74], having as a goal the provision of *rules, common standards and practices, infrastructures and a governance framework for the primary and secondary use of electronic health data* (art. 1.1.).

3.4. Legal and other concerns connected with HDTs

HDTs technology raises a few legal challenges which go beyond data privacy (that we have already addressed). We will name just those which seem of great importance to us, without delving into their detailed analysis[75]:

- data security; effective protection systems against cyber threats must be used, so that personal data cannot be accessed or disclosed to unauthorized persons;

- liability for improper operation of HDTs; since HDTs can make predictions, recommendations or even make decisions under certain conditions, which could be erroneous, with more or less serious effects on the real twin or the community, the question of liability arises; tracing the person responsible can be difficult, given the multiple actors involved;

- discrimination in access to HDT technology;

- the psychological impact on the real twin; the real twin can suffer psychological trauma, determined by the permanent surveillance (from the fact that he/she becomes „transparent") and assists his own transformation and the aging process; this awareness can affect *self-esteem, self-perception, and mental health*[76]; therefore, the real twin may need psychological counseling.

Conclusions

The prospects provided by the HDTs concept are impressive, even though it presents a number of legal and other challenges. HDTs create new avenues for innovation in a wide range of sectors by demonstrating the sophisticated integration of digital technology into the study and understanding of the human body and mind, as well as their interaction with the environment and other people.

[73] *Idem.*

[74] Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space, Strasbourg, 3.5.2022, COM(2022) 197 final, 2022/0140(COD), [Online] at https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex:52022PC0197, accessed on April 4th, 2024.

[75] M. Cellina, M. Cè, M. Alì, G. Irmici, S. Ibba, E. Caloro, D. Fazzini, G. Oliva, S. Papa, *Digital Twins: The New Frontier for Personalized Medicine?*, in Applied Sciences 13, no. 13/2023, https://doi.org/10.3390/app13137940, p. 12; M. Teller, *op. cit.*, pp.1-5.

[76] *Ibidem*, p. 12.

New technologies also involve risks. There are situations when the intended outcome is very different from the original aim. *Will your heart's digital twin become a health coach or an agent of the insurance company that refuses your life insurance*? [77] Since the real-world twin does not have a right of control over his/her digital twin, any scenario can be possible. The rules adopted or in the process of being adopted are intended to correct possible deviations from the use of HDTs technology for purposes contrary to good faith and the well-being of the real-world twin and the community he/she is part of.

Despite the negative connotation associated with „playing God," which stems from human manipulation through technology and human limitations in controlling situations beyond their comprehension, we think HDT's technology has potential benefits for humanity. "The beast" could be tamed if the rules are followed.

References

Barricelli B.R., Casiraghi E., Gliozzo J., Petrini A., Valtolina S., *Human digital twin for fitness management*, in IEEE Access, volume 8, 2020, 26637–26664, https://doi.org/10.1109/ACCESS.2020.2971576.

Beduschi A., *Synthetic data protection: Towards a paradigm change in data regulation?*, in Big Data & Society, 11(1), 2024, https://doi.org/10.1177/20539517241231277.

Cellina M., Cè M., Alì M., Irmici G., Ibba S., Caloro E., Fazzini D., Oliva G., Papa S., *Digital Twins: The New Frontier for Personalized Medicine?*, in Applied Sciences 13, no. 13/2023, https://doi.org/10.3390/app13137940, p. 12.

Cheng, Z., *Human digital twin with applications*, in Proceedings of the 7th International Digital Human Modeling Symposium 7(1): 41, 2022, https://doi.org/10.17077/dhm.31783.

Corral-Acero J., Margara F., Marciniak M., Rodero C., Loncaric F., Feng Y., Gilbert A., Fernandes J.F., Bukhari H., Wajdan A., Martinez M.V., Santos M.S., Shamohammdi M., Luo H., Westphal P., Leeson P., DiAchille P., Gurev V., Mayr M., Geris L., Pathmanathan P., Morrison T., Cornelussen R., Prinzen F., Delhaas T., Doltra A., Sitges M., Vigmond E.J., Zacur E., Grau V., Rodriguez B., Remme E.W., Niederer S., Mortier P., McLeod K., Potse M., Pueyo E., Bueno-Orovio A., Lamata P., *The 'Digital Twin' to enable the vision of precision cardiology*, in European Heart Journal, Volume 41, Issue 48, 21 December 2020, https://doi.org/10.1093/eurheartj/ehaa159, pp. 4556–4564.

Dai Y., Wang J., Gao S., *Advanced Electronics and Artificial Intelligence: Must-Have Technologies Toward Human Body Digital Twins*, in Advanced Intelligent Systems, Influence Series, vol. 4, issues 2, 2022, 2100263 (1-11), https://doi.org/10.1002/aisy.202100263.

Douglass K., Lamb A., Lu J., Ono K., Tenpas W., The Mathematical Intellinger, *'Digital Twins' Give Olympic Swimmers a Boost*, July 8, 2024, [Online]

Duan H., Gao S., Yang X., Li Y., *The development of a digital twin concept system*, in Digital Twin 2023, 2:10, https://doi.org/10.12688/digitaltwin.17599.2.

[77] KU Leuven, *The pitfalls of digital twins*, in KU Leuven Stories – The power of wonder, 2023, [Online] at https://stories.kuleuven.be/en/stories/the-pitfalls-of-digital-twins, accessed on April 4th, 2024

European Commission, *Shaping Europe's digital future. European Virtual Human Twins Initiative,* [Online]

European Medicines Agency, *Guideline on computerised systems and electronic data in clinical trials*, March 9th, 2023, [Online]

Grieves M., *Digital twin: manufacturing excellence through virtual factory replication*, in White paper, 2015, [Online]

Kamel Boulos M.N., Zhang P., *Digital Twins: From Personalised Medicine to Precision Public Health*, in Journal of Personalized Medicine, volume 11, issue 8, 2021, https://doi.org/10.3390/jpm11080745, pp. 2-8.

Khalid M.I., Ahmed M., Kim J., *Enhancing Data Protection in Dynamic Consent Management Systems: Formalizing Privacy and Security Definitions with Differential Privacy, Decentralization, and Zero-Knowledge Proofs*, in Sensors 2023, 23, 7604, https://doi.org/10.3390/s23177604.

KU Leuven, *The pitfalls of digital twins*, in KU Leuven Stories -The power of wonder, 2023, [Online]

Lehmann M., *Seeking an Edge in Judicial Competition: England is Becoming the Leading Crypto Litigation Hub*, 11 July 2024, [Online] at https://eapil.org/2024/07/11/, accessed on July 13th, 2024.

Liu T., Weng C., Jiang Q., Jiao L., Ni Z., *Modelling Human Digital Twins Based on Physical and Mental Fusion*, in NSFC-RGC Conference 2023, https://doi.org/ 10.13140/RG.2.2.23742.77121, [Online]

Miller M., *Human Digital Twin and Modeling Guidebook*, in Air Force Institute of Technology – Technical Report, December 19, 2022, pp. 2-8, [Online]

Miller M.E., Spatz E., *A unified view of a human digital twin*, in Human-Intelligent Systems Integration, (2022) 4, https://doi.org/10.1007/s42454-022-00041-x, pp. 23-29.

Naudet Y., Baudet A., Risse M., *Human Digital Twin in Industry 4.0: Concept and Preliminary Model*, in IN4PL - Proceedings of the International Conference on Innovative Intelligent Industrial Production and Logistics, pp. 137-144, 2021, https://doi.org/10.5220/0010709000003062.

Novelli C., Hacker P., Morley J., Trondal J., Floridi L., *A Robust Governance for the AI Act: AI Office, AI Board, Scientific Panel, and National Authorities*, in Centre for Digital Ethics (CEDE) Research Paper Series, May 5, 2024, http://dx.doi.org/10.2139/ssrn.4817755.

Pascual H., Masip-Bruin X., Alonso A., Cerdá J., *A Systematic Review on Human Modeling: Digging into Human Digital Twin Implementations*, 2023, arxiv Publisher, https://doi.org/10.48550/arxiv.2302.03593, pp. 1-8.

Păvăloaia V.D., Necula S.C., *Artificial Intelligence as a Disruptive Technology—A Systematic Literature Review,* in Electronics 2023, 12, 1102, https:// doi.org/10.3390/ electronics12051102, pp. 1-2.

Popa E.O., van Hilten M., Oosterkamp E., Bogaardt M.-J., *The use of digital twins in healthcare: socio-ethical benefits and socio-ethical risks*, in Life Sciences, Society and Policy, issue 17, 2021, https://doi.org/10.1186/s40504-021-00113-x.

Santos C., Nouwens M., Toth M., Bielova N., Roca V., *Consent Management Platforms Under the GDPR: Processors and/or Controllers?*, in: Gruschka N., Antunes L.F.C., Rannenberg K., Drogkaris P. (eds), *Privacy Technologies and Policy*, APF 2021, Lecture Notes in Computer Science, vol. 12703. Springer, Cham., https://doi.org/10.1007/978-3-030-76663-4_3.

Saracco R., *Personal Digital Twins. A third evolution step for humankind?*, eBook, 2022, p. 23-29, [Online]

Shengli W., *Is Human Digital Twin possible?*, în Computer Methods and Programs in Biomedicine Update, volume 1, 2021, pp. 1-4, https://doi.org/10.1016/j.cmpbup.2021.100014.

Song Y., *Human Digital Twin, the Development and Impact on Design*, in Journal of Computing and Information Science in Engineering, vol. 23, issue 6, 2023, Paper No: JCISE-23-1076, pp. 4-5, https://doi.org/10.1115/1.4063132.

Tang C., Yi W., Occhipinti E., Dai Y., Gao S., Occhipinti L.G., *Human Body Digital Twin: A Master Plan*, 18 July 2023, last revised 12 September 2023, https://doi.org/10.48550/arXiv.2307.09225, [Online]

Tataru S.R., *Soluționarea litigiilor referitoare la contractele de comerț internațional cu produse farmaceutice*, Ed. Hamangiu, București, 2020, p. 28.

Tekinerdogan B., *On the Notion of Digital Twins: A Modeling Perspective*, in Systems 11, volume 15, issue 1, 2023, https://doi.org/10.3390/systems11010015.

Teller M., *Legal aspects related to digital twin*, in Philosophical Transactions of the Royal Society A, 4 October 2021, volume 379, Issue 2207, https://doi.org/10.1098/rsta.2021.0023.

Ungureanu C.T., *Proprietatea asupra datelor digitale: realități, neliniști și posibile soluții*, în Revista Română de Drept Privat nr. 2/2023, pp. 75-90.

Ungureanu C.T., Tataru S.R., *The legality of reverse engineering or how to legally decipher trade secrets,* SHS Web of Conferences vol. 177/2023, article number 02001, *Legal Perspectives on the Internet. COPEJI 6.0,* http://doi.org/10.1051/shsconf/202317702001.

ANALELE ŞTIINŢIFICE ALE UNIVERSITĂŢII „ALEXANDRU IOAN CUZA" DIN IAŞI
TOM LXX, 2, ŞTIINŢE JURIDICE, 2024

DOI: 10.47743/jss-2024-70-2-2

Dispatch of the Court Decision by E-mail

Cătălin LUNGĂNAȘU[1], **Claudia ROȘU**[2]

Abstract: The conclusion of a civil lawsuit takes place by issuing the court decision. The way in which the court decision is served is particularly important because of the consequences it generates: the starting point for the time limit for lodging an appeal; determining the date when it became final; its binding and enforceability. In this study, the authors appreciate the legislative change of communication of court decisions by e-mail, because there is a need in court for those tools that contribute to the speed and simplification of the civil process.

Keywords: court decision, communication, the principle of availability, email; confirmation message.

1. Brief details of the court decision

All judicial work is carried out with the aim of resolving a concrete civil conflict. Because of this, the court decision – designating precisely the result of judicial activity – is undoubtedly the most important act of justice[3]. Therefore, the culmination of the judicial phenomenon is considered the „judicial act", generically called „judgment" and meaning „utterance of the right" (*iuris dictio*). At the same time, it is the conclusion formulated to an approach having as object a litigious legal situation, as well as the enshrining of an irrevocable state of law by the force attached to the act under the name of „power of res judicata"[4].

The content of the judgment, as regulated by art. 425 C. pr. civ., is of considerable practical importance having regard, on the one hand, to the effects of the judicial act, but – in my view – also to a broader spectrum defined by the purpose of justice and the guarantee of the right to a fair trial. Starting the analysis with the provision contained in Art. 425 para. 1 lit. b) C. proc. civ., we recall that the judgment must contain the recitals, namely the part in which the subject matter of the application is set out and the brief submissions of the parties, the statement

[1] Asisstant Professor PhD, West University of Timișoara, Faculty of Law, e-mail: catalin.lunganasu@e-uvt.ro

[2] Professor PhD, West University of Timișoara, Faculty of Law, e-mail: claudia.rosu@e-uvt.ro

[3] I. Leş, *Noul Cod de procedură civilă. Comentariu pe articole*, Editura C. H. Beck, Bucureşti, 2013, p. 550.

[4] I. Deleanu, *Tratat de procedură civilă, vol. II*, Editura Servo-Sat, Arad, 2004, p. 11.

of the facts adopted by the court on the basis of the evidence administered, the factual and legal reasons on which the decision is based, showing both the reasons for admitting them, as well as those for which the parties' claims have been rejected. Although quantitatively it occupies the bulk of the judgment, the recitals tend to be overshadowed by the operative part because it encompasses the court's absolution of the disputed legal relationship and, essentially, the command that can usually be enforced.

However, in the report and the regulation contained in Art. 401 – 403 C. pr. civ., in reality the parties first get to know the solution given by the court, without finding out at the same time the reason for such a resolution of the disputed issue that formed the subject of the file. Consequently, I consider that, once the judicial decision has been drafted, the central element to which we should turn our attention is precisely the recitals of the judgment. Thus, referring to the provisions of art. 425 para. 1 lit. b) C. pr. civ. mentioned above, we note that it is only with the drafting of the judgment that the reasons for which the parties' applications were admitted or rejected are revealed, thus making known the court's reasoning. We recall in this regard that, according to the ECHR judgment ordered in Albina vs. Romania (Application no. 57808/00, Decision of 28.04.2005 published in the Official Gazette of Romania, no. 1049 of 25.11.2005) "the obligation imposed by art. 6 paragraph 1 (of the European Convention on Human Rights) on national courts to give reasons for their decisions does not require a detailed answer to every argument (Perez, v. France (GC), Application No. 47.287/99, par. 81; Van der Hurk v. the Netherlands, judgment of 19 April 1994, paragraph 61; Ruiz Torija and Hiro Balani v. Spain, judgment of 9 December 1994, paragraph 29; see also Jahnke and Lenoble v. France, Application No. 40.490/98, CEDH 2000-IX]". However, the Court recalls that, according to its case-law, 'the concept of a fair trial presupposes that a domestic court which has given only brief reasons for its judgment must nevertheless have genuinely examined the essential questions submitted to it, and not merely repeat the conclusions of a lower court (Helle v. Finland, of 19 December 1997, ECR 1997-VIII, p. 2.930, paragraph 60)".

It is precisely from this perspective that we consider that the importance of the considerations of the judicial decision is not limited to the effect mentioned in Art. 430 para. 2 C. pr. civ. where reference is also made to the considerations on which the operative part is based or by which a litigious question has been resolved as enjoying the authority of res judicata, but also propagates on the purpose of civil proceedings, being the effective manner of justice. For such reasons, moreover, the requirements established by case-law by the European Court of Human Rights emerge, the lack of an effective motivation of the problems with which the court has been vested in a specific case being equivalent to disregarding the right to a fair trial. Consequently, in such a context, I consider that the existence of sufficient considerations encompassing the court's reasoning for its decision is a *sine qua non condition* for ensuring fundamental guarantees in civil proceedings. However, we mention that such a requirement is not sufficient because the desideratum is not achieved if the result does not reach the addressees of the act of justice, namely the parties to the case. As such, the actual communication of the court decision constitutes, in the same approach, a stage of the same significance as the very pronouncement and drafting of the procedural act of disvestment, and the exceptions to the rule are of strict interpretation, expressly provided for by law and justified by objective reasons[5].

2. General aspects regarding the service of the judgment

After the decision has been drafted and signed in accordance with the law, it will be communicated ex officio to the parties, in copy, even if it is final, as provided by art. 427 C. pr. civ. The text of the law mentions that this communication will be made "immediately", a notion that imprints not only an urgency in the sequence of procedural moments, but also the indissoluble link between the delivery of the judgment, drafting it and bringing it to the attention of the parties. Moreover, in relation to the effects they produce, certain court decisions shall be communicated ex officio to persons other than the litigants, respectively final decisions ordering an entry in the land register or, as the case may be, in other public registers shall also be communicated ex officio to the institution or authority keeping those registers[6]. Also, final decisions ordering the annulment, in whole or in part, of a notarial act shall be communicated ex officio immediately to the instrumenting notary public, directly or through the chamber of notaries public in whose district it operates. Last but not least, judgments by which the court rules on provisions contained in the Treaty on the Functioning of the European Union and in other legal acts of the European Union shall also be communicated, ex officio, even if they are not final, to the national authority or institution with regulatory powers in the matter.

We note that, although art. 427 C. pr. civ. regulates precisely the „service of the judgment”, in reality it does not contain any reference to the service procedure, i.e. the manner in which it is carried out, but only rules concerning the obligation to communicate and the subjects to which it will be transmitted. Consequently, the general rules on summoning and service of procedural documents also apply in this case, Art. 154 C. proc. civ. stating that such rules apply not only to the service of summonses, but also to all procedural documents, including judgments. However, as regards the modalities of effective communication of court decisions by Law no. 192/2022 for the completion of Law

[5] In this regard, we recall the provisions of art. 144 para. 2 C. pr. civ. as an exception to the reasoning of the decision justified by the grounds on which the removal of a case may be requested or the provisions of Art. 667 C. pr. civ. postponing the service of the conclusion by which the court granted the application for a declaration of enforceability precisely in order to give the creditor time to commence enforcement without the risk of hindrance on the part of the debtor, if he were notified immediately of the imminent enforcement of enforcement acts against him.

[6] C. Roșu, *Drept procesual civil. Partea generală,* Editura C. H. Beck, București, 2016, p. 320.

no. 134/2010 on the Code of Civil Procedure[7], certain express provisions have been inserted.

Thus, after art. 154 Art. 1541 C. pr. civ. according to which service of judgments shall be made, ex officio, by electronic mail if the party has indicated to the court the appropriate data for this purpose directly or at the express request of the court during the trial. The communication will be accompanied by the court's extended electronic signature, which will replace the court's stamp and the signature of the court clerk.

We note that, in accordance with the new technologies of distance communication, communication by electronic mail was given efficiency, obviously, if the party expressly indicated its e-mail address. We consider that the possibility of communicating the court decision by electronic mail represents a form of ensuring the speed of the civil process, but also a concrete application of the principle of availability of the parties in the process, bringing as an additional benefit a reduction in litigation costs.

Paragraph 1 of Art. 1541 C. pr. civ. establishes the obligation of the extended electronic signature of the court in communication by electronic mail. The attachment of the extended electronic signature is intended to demonstrate the authenticity and veracity of the court decision, thus replacing the stamp of the court and the signature of the court clerk that would have been used in the case of a common law communication on paper. We recall in this regard that, according to art. 4 point 4 of Law nr. 455/2001 regarding electronic signature[8], extended electronic signature represents that electronic signature that cumulatively meets the following conditions: a) is uniquely linked to the signatory; b) ensure the identification of the signatory; c) it is created by means controlled exclusively by the signatory; d) is linked to data in electronic form, to which it relates in such a way that any subsequent modification thereof is identifiable.

With particular relevance to the studied topic, we mention that, prior to the adoption of Law no. 192/2022, the High Court of Cassation and Justice was seized on 1 February 2022 by the Dolj Court – Administrative and Tax Section, for a preliminary ruling on the following points of law:

'The provisions of Article 154 (1) shall not be exceeded. (6) in relation to the provisions of Article 158, Article 163 para. (3), (5), (8), (111), Art. 164 para. (4) of the Code of Civil Procedure may be interpreted as meaning that the request does the applicant's compliance with the procedure for summoning and serving procedural documents by e-mail require the court, as the only way to carry out this procedure, to serve by electronic mail?

If, under these circumstances, the summons procedure carried out by postal agent, in accordance with the provisions of the Code of Civil Procedure, is null and void, in the absence of use by the applicant of the guarantees provided by

[7] Law nr. 192/2022 for the completion of Law no. 134/20210 on the Code of Civil Procedure was published in the Official Gazette of Romania, no. 643 of 29.06.2022.

[8] Law nr. 455/2001 regarding the electronic signature was republished in the Official Gazette of Romania, no. 316 of 30.04.2014, as amended.

Art. 163 para. (5) and Art. 164 para. (4), respectively the registration in forgery against the report drawn up in accordance with art. 164 of the Code of Civil Procedure'.

By Decision No. 75/2022, the High Court of Cassation and Justice – Panel for ruling on legal issues,[9] admitted the complaint filed by the Dolj Court – Administrative and Tax Division regarding a preliminary ruling and, in interpreting and applying the provisions of art. 154 para. (1), (6) and (6)1, Art. 163 para. (5), Article 164 para. (4) and Art. 175 para. (1) of the Code of Civil Procedure, established that carrying out the summons procedure, in accordance with the provisions of Art. 154 para. (6) of the Code of Civil Procedure, if the party has requested and indicated the appropriate data for this purpose, constitutes a principal method of service of procedural documents, without being conditioned by the performance of the procedure in letter format, as provided for in Art. 154 para. (1) of the same enactment.

The act of summoning the party to proceedings, in a manner other than that invoked by the application addressed to the court, is null and void pursuant to the provisions of Art. 175 para. (1) of the Code of Civil Procedure, if failure to comply with the method of service of the procedural document has caused the party an injury which can only be removed by its abolition, without being conditioned by the use of the procedure of false entry, pursuant to the provisions of Art. 163 para. (5) and Art. 164 para. (4) of the Code of Procedure.

In order to adopt this solution, the supreme court held that a fundamental principle of civil procedural law is that of availability, regulated by Art. 9 of the Code of Civil Procedure, which implies not only the claimant's right to initiate civil proceedings, to use the remedies provided for by law or to waive the action or right, but also the parties' right of disposition regarding the exercise of their procedural rights.

However, in so far as it is established that the transmission of procedural documents, in accordance with the provisions of Article 154 para. (6) of the Code of Civil Procedure, by e-mail, if the party has requested and indicated the appropriate data for this purpose, constitutes a primary means of communication, then the principle of availability allows the party to request electronic service, the court being obliged to do so in civil proceedings.

The Supreme Court also noted the opinion transmitted by the Faculty of Law of the West University of Timișoara according to which summoning by means other than those expressly indicated by the applicant does not meet the requirements of a correct and legal summoning, so that the summons procedure cannot be considered fulfilled. Only if, compared to the specifics of a dispute, the method of communication chosen by the parties would lead to the prolongation of the process, the court could choose another way, in order to ensure the resolution of the case in an optimal and predictable time. Communication by e-mail fulfills

[9] Decision No. 75/2022 pronounced by the High Court of Cassation and Justice – Panel for ruling on legal issues, was published in the Official Gazette of Romania no. 182 of 3 March 2023.

the function of being a much faster and safer means than communication by procedural agent or postal agent.

On this issue, under the conditions of Art. 520 para. 11 and Art. 516 para. 6 C. pr. civ. I have expressed my view that the question of law does not raise any difficulty of interpretation having regard to the specific nature of the summons procedure and its role, as well as the way in which that matter is regulated. For example, in the hypothesis envisaged by art. 158 para. 1 C. pr. civ., the legislature is quite clear, meaning that, by virtue of the principle of availability, service is effected at the address indicated by the party as the domicile/seat of proceedings chosen. However, failure to comply with this procedure and, possibly, summoning the party to an address other than that indicated, without applying the provisions of art. 161 para. 1 or 2 C. pr. civ. will inevitably lead to the conclusion that the summons procedure is flawed, and the provisions of Art. 160 C. pr. civ. or, as the case may be, the possibility of appeals on that very ground. As in the case of indicating the domicile / procedural seat chosen, there is no dilemma in considering that failure to comply with the summons procedure in the version chosen by the party will lead to the nullity of the summons procedure, I consider that the same reasoning applies if the party has chosen the method of communicating the court decision, namely by electronic means.

In this respect, the correct and legal interpretation was considered that the court is obliged to follow the method of summons chosen by the parties, and the act of summons performed in another way is null.

We note the anchoring of the Supreme Court to today's reality, which in its decision noted that the technological evolution of society offers new possibilities for communicating procedural documents that correspond to the legitimate needs and interests of the parties, which is, moreover, among others, the purpose of Law no. 134/2010 on the Code of Civil Procedure, republished, with subsequent amendments and completions, namely to modernise and make the procedure more flexible, so that it can be carried out expeditiously, in an optimal and predictable time.

3. Particularities of service of the court decision by email

Returning to Law nr. According to Regulation (EC) No 192/2022, a very important aspect is to determine exactly when the time limit for lodging appeals runs or, in the absence thereof, when the final judgment remains.

In this respect, para. 2 of § 1541 C. pr. civ. provides that judgments are deemed to have been served at the time they have received a message from the system used that they have reached the addressee according to the data provided by him. In this aspect of service, namely the moment at which the service procedure is deemed to have been completed, I note that the legislature has adopted the same reasoning applied in other cases where the actual delivery of the procedural document to be served is not made personally, namely neither to the addressee itself nor to any other person empowered or empowered by law to receive the document subject to service. As examples in this regard, we mention the provisions of art. 158 para. 2 or Art. 163 para. 8 in conjunction with Art. 163 para. 3 sentence I C. proc. civ. Thus, the mere deposit in the mailbox or mailbox will mean that the service procedure was carried out at that time, as indicated in the proof of delivery pursuant to Art. 164 C. pr. civ., even if, in reality, the party was not actually handed over the document subject to service, but was merely made available to him. As such, the legislature's choice of establishing a legal presumption of service and acknowledgement precisely from the date of receipt by the addressee's electronic system represents an application adapted to that method of communication of the rules which also applied under ordinary law. Just as the procedural period running from the service of the document will be counted from the date on which the envelope is deposited in the mailbox or mailbox, being irrelevant the moment when the party actually received the document served, the same will be calculated in the case of service by electronic mail, namely from the moment when a message was received from the system used that they had reached the addressee according to the data provided by it. Similarly, from the point of view of the course of the procedural period, it will be completely irrelevant when the communicated email is actually accessed, just as, in the case of letter communication, the date of actual opening of the envelope is irrelevant.

Moreover, we consider this particular solution applied to service by electronic mail (drawn from the general rules on service of procedural documents) to be natural since, particularly in the field of procedural time limits, a right of option cannot be granted to the parties. Thus, the starting point of the period cannot be left to the party's discretion or choice, that is to say, it cannot be considered that the period could begin to run only from the moment when the party chooses to become actually aware of the content of the procedural document served. Just as it has no procedural relevance when the party actually opens the envelope delivered to him or her in the mailbox, so it is irrelevant when the party opened the email addressed to him. In other words, the legislature establishes the same rules regarding the service of the court decision by mail as in the general case of service of procedural documents in letter format, the relevance being strictly the moment of service itself. As a consequence, although the information system distinguishes and can highlight both the moment when the email is received by the addressee (by arriving in his electronic mail) and the moment when it actually opens – that is to say, the date of access to the electronic communication – nevertheless only the former has legal significance since, otherwise, it would lead to the same situation expressly avoided by the legislature in which the parties choose the starting date of the procedural period. This is the reason why Art. 1541 para. 2 C. pr. civ. expressly states when judgments sent to the parties by electronic mail are deemed to be served.

What is essential in this matter is the fact that, in all variants of letter communication, the procedural agent or other employee designated for this purpose is involved, the provisions of Art. 164 para. 4 C. pr. civ. relating to the evidential power of what was personally ascertained by the person drawing up the report. That is why it is so easy to establish the presumption provided for in Art.

165 C. pr. civ. relating to the date of service. For example, the fact that the procedural agent mentions a specific date in the report drawn up when the envelope is deposited in the mailbox will provide proof, subject to Art. 164 para. 4 C. pr. civ., that communication was made precisely at that time. On the other hand, in the case of communication by electronic mail, ab *initio* no longer involves any such official, meaning that his ex *proprius sensibus findings* and their evidential power cannot exist until they are entered in forgery. All this is replaced by a computer system. Consequently, we may consider that the legislation contained in Art. 1541 para. 2 C. pr. civ. must also be seen as a practical necessity since, in the absence of the procedural agent, the presumption as to the date of service would have remained unsupported and the only categorical date on which service would have been made became that chosen by the addressee when he accessed his electronic mail. Thus, through the legislation introduced, the legislature maintains the general rules in the field and assimilates the response sent by the information system regarding the communication with the personal findings of the procedural agent in the letter method of communication. Moreover, in the explanatory memorandum of Law nr. Regulation (EC) No 192/2022 states that there is no difference between the situation where the procedural agent or postman leaves the correspondence in the parties' mailbox by filling in a report to that effect and the situation where the court's system firmly indicates that electronic correspondence has arrived in the parties' virtual box[10].

Only if communication by e-mail cannot be carried out, the methods of communication enshrined in art. 154 C. pr. civ. Thus, in para. 3 of § 1541 C. pr. civ. states that if communication by electronic mail is not possible due to lack of data in this regard or the system used indicates error in transmission by electronic mail, service of court decisions shall be made in accordance with section 154.

In the legal literature it was considered that the difference from service of other documents would be that, at least from the wording of the text, service by electronic mail would be mandatory if the party indicated the corresponding data, not being a mere alternative for the court[11].

We consider that we need to make a nuance, the communication of the court decision becomes mandatory by electronic mail when the party has expressly formulated this request, not when it has only indicated the e-mail address in the header or in the contents of the applications addressed to the court. We believe that such a clarification is necessary given that art. 1541 para. 1 C. pr. civ. expressly states that this method of service is effective when the party indicates to the court the appropriate data for that purpose, that is to say, precisely so that the decision may be served on it by electronic mail. Moreover, the general rules applicable to the service of summonses and other procedural documents provide for the same

[10] R.- M. Necula, *Comunicarea hotărârii judecătorești prin e-mail. Reflecții cu privire la reglementarea art. 154^1 din Codul de procedură civilă,* Revista „Dreptul" Nr. 12/2022, p. 114.

[11] V. M. Ciobanu, T. C. Briciu, C. C. Dinu, *Drept procesual civil, Ediție revăzută și adăugită, Curs de bază pentru licență, seminare și examene,* Editura Universul Juridic, București, 2023, p. 412, footnote 2.

specificity[12], an aspect contained in Art. 154 para. 6 C. pr. civ. Thus, the indication of the corresponding electronic mail data is not sufficient to activate the court's obligation to serve the judgment in this way if the party's express request is absent. Such a rule represents a particular application of the principle of availability when the manifestation of will belongs to the party.

However, it has been pointed out in the legal literature that it would appear that the party does not enjoy the same freedom to assess whether he wishes to use electronic mail, since the court may expressly request the corresponding data. This last difference in regime is rather apparent, since there is no sanction for the party's refusal to comply with the court and, at least from a theoretical point of view, it is not excluded that a party does not routinely use email communication[13]. Thus, starting from the text of art. 1541 para. 1 C. pr. civ., it is concluded that the court may instruct the party to indicate the e-mail address in order to serve the judgment in such a manner when the party has not indicated it on its own initiative. If the party complies, it follows that the court will be able to use this means of communication even in the absence of an express request by the litigant. However, I consider that the party's right of option remains because, in complying with the court's request, it is presumed to want such a communication procedure since the refusal to comply does not produce any legal consequences and certainly does not entail any sanction. As such, it is obvious that the party remains to exercise the right to choose or reject such a form of communication, just as provided by the initial sentence of Art. 1541 para. 1 C. pr. civ. when the party expressly requests. On the other hand, where the party has indicated his electronic mail address but has not made an express request, the court cannot assume that the party would like the judgment to be served electronically, nor can it envisage him or her to specify the corresponding data (as they are already initially submitted by the party), meaning that the presumption of agreement due to the party's compliance cannot be operative either.

In the same vein, it was stated that in relation to the provisions of Article 154 para. 6 C. pr. civ., service of summons or other procedural documents may be affected by e-mail only if the party has expressly indicated that he wishes to serve those procedural documents in this way and has provided the court with the necessary data for this purpose[14].

We appreciate the changes made by Law nr. 192/2022 on how to communicate court decisions that are consistent with the new realities regarding the digitalisation of the civil process. However, we find it useful to mention that, despite the progressive nature of the regulation established by Art. 1541 C. pr. civ., in reality we consider that legislative advance is almost non-existent since, according to art. 154 para. 6 and para. 61 C. pr. civ., such methods of

[12] N.-H. Țiț, *Considerații cu privire la comunicarea prin e-mail a actelor de procedură în procesul civil*, în Analele Științifice ale Universității „Alexandru Ioan Cuza” din Iași, Tomul LXVI/Supliment, Științe Juridice, 2020, p. 202 și urm.

[13] *Ibidem.*

[14] R.- M. Necula, *op. cit.*, p. 116.

communication were also provided for prior to Act No. 192/2022. Thus, even if they refer to the service of summonses and other procedural documents, thus being of a general nature, the abovementioned texts apply accordingly also to the service of judgments. As such, the usefulness of a special regulation seems to be seriously mitigated given that, apart from expressly stating that it also applies to court decisions, it does not bring into substance anything new, art. 1541 para. 1 and 2 reproducing exactly the provisions contained in art. 154 para. 6 and 61 C. pr. civ. At most we could positively appreciate the provision contained in para. 3 of Art. 1541 C. pr. civ. because it establishes ex officio the recommunication of the judgment by ordinary means when the computer system is not functional either because of lack of data in this regard or when an error occurs in the transmission by e-mail.

It was considered that, if the aim is to digitize the judicial system as much as possible, the legislator should introduce a provision similar to Art. 1541 para. 1 C. pr. civ., i.e. to make it compulsory to serve all procedural documents by e-mail, if the party has indicated the appropriate data for this purpose, Service of procedural documents, in classic format, by procedural agent or postal agent, to be carried out only if communication by electronic mail is not possible due to lack of data in this regard or if the system used by the courts indicates error in transmission by electronic mail[15].

As a topography of the provisions relating to the service of judgments, we consider that the new provisions should have been inserted in Art. 427 C. pr. civ., in order to avoid overlapping the same title, but with different but consistent content. The legislative technique is objectionable and we consider it wrong as long as there is the same title in different parts of the Code of Civil Procedure.

Last but not least, we mention that, being still at the beginning, such a way of communicating court decisions may encounter technical problems, such as situations in which the file cannot be opened, copied or listed, but we believe that these inherent difficulties are surmountable and over time the errors encountered will be rarer.

Conclusions

We believe that it was necessary to adapt the Code of Civil Procedure to the progress made in recent years regarding digitalization and the use of technical progress instruments in the field of justice.

One of the particularly important aspects is precisely that of the communication of court decisions, since the 'classic' methods cannot be the only ones allowed.

Technological progress is inevitable and it is incumbent on the legislator to implement also in the judiciary those instruments that contribute to the speed and simplification of the civil process.

[15] *Idem*, p. 118.

References

Ciobanu V. M., Briciu T. C., Dinu C. C., *Drept procesual civil, Ediție revăzută și adăugită, Curs de bază pentru licență, seminare și examene,* Editura Universul Juridic, București, 2023.

Deleanu I., *Tratat de procedură civilă, vol. II*, Editura Servo-Sat, Arad, 2004.

Leş I., *Noul Cod de procedură civilă. Comentariu pe articole*, Editura C. H. Beck, București, 2013.

Necula R.-M., *Comunicarea hotărârii judecătorești prin e-mail. Reflecții cu privire la reglementarea art. 154^1 din Codul de procedură civilă,* Revista „Dreptul” Nr. 12/2022, pp. 112-119.

Roșu C., *Drept procesual civil. Partea generală,* Editura C. H. Beck, București, 2016.

Țiț N.-H., *Considerații cu privire la comunicarea prin e-mail a actelor de procedură în procesul civil*, în Analele Științifice ale Universității „Alexandru Ioan Cuza” din Iași, Tomul LXVI/Supliment, Științe Juridice, 2020, pp. 197-211.

Analele Ştiinţifice ale Universităţii „Alexandru Ioan Cuza” din Iaşi
TOM LXX, 2, Ştiinţe Juridice, 2024

DOI: 10.47743/jss-2024-70-2-3

AI Ethics: The Bias Puzzle

Alexandru CHISTRUGA[1]

Abstract: The advantages of artificial intelligence are extensively discussed in specialized literature, which claim that technology has the power to fundamentally change society. However, rapid development of artificial intelligence does carry some serious risks, the most important of which is the spread of false and discriminatory information. Since artificial intelligence is "fed" with data from many sources, there is an increased risk that some of the data contains extremist or xenophobic literature. In such circumstances, artificial intelligence could spread extremely dangerous theories and ideas. Thus, government intervention is required to preserve control over the different data categories that developers have access to. As an example, we would like to bring up the fact that during testing, one of the most well-known AI interfaces, GPT-4, provided "advice" on how to murder a huge amount of people for a single dollar and what messages to promote in order to attract people to join Al-Qaeda.

Keywords: artificial intelligence; disinformation, data.

Introduction

Artificial intelligence is constantly evolving, making it difficult to find a field in which it is not used. For instance, in medicine, AI is used *„to help process medical data and give medical professionals important insights, improving health outcomes and patient experiences”*[2]. In some cases, the analysis provided helps clinicians to detect the onset of a disease in a timely manner, including situations in which artificial intelligence has proven to be more efficient than professionals in the area. As a rule, *„the most common role for AI in medical settings are clinical decision support and imaging analysis*[3]*”*. The initial phase involves examining the data concerning a specific patient's case, followed by correlating the obtained information with prior knowledge, ultimately providing a response that may manifest in the form of a treatment proposal.

[1] PhD Student, Faculty of Law, „Alexandru Ioan Cuza” University of Iaşi, e-mail: alexandruchistruga98@gmail.com

[2] IBM, *What is artificial intelligence in medicine?*, online at https://www.ibm.com/topics/artificial-intelligence-medicine#:~:text=Artificial%20intelligence%20in%20medicine%20is%20the%20use%20of,important%20insights%2C%20improving%20health%20outcomes%20and%20patient%20experiences, accessed on 08.05.2024.

[3] *Ibidem.*

Until recently, it was considered that artificial intelligence would eventually remain a robot incapable of creativity, preventing a part of the occupations from being replaced. But, „*a recent study suggests that large language model artificial intelligence chatbots excel beyond the average human in creative tasks*”[4]. Moreover, another study shows that business is anticipating „*that new technologies will destroy jobs faster that creating new ones over the next five years – with a net negative of 14 million roles”*. For these reasons, some of the most important players in the IT sector, among them Elon Musk and Steve Wozniak, urged „*all AI labs to immediately pause for at least 6 months the training of AI systems more powerful than GPT-4”*[5]. Some of these concerns are legitimate, but in this work, we will focus on a lesser-known risk: the spread of discriminating or biased responses by artificial intelligence.

1. Exploring AI Biases

Most artificial intelligence systems, such as ChatGPT, provide, in addition to useful information, a set of responses that reflect and perpetuate human biases, which can lead to incorrect findings in fields such as medicine, human resources, and justice[6]. In specialized literature, biases are defined as an „*effect that deprives a statistical result of representativeness by systematically distorting it, as distinct from a random error, which may distort on any one occasion but balances out on the average”*[7]. Typically, this category includes discriminatory practices that have resulted in unequal treatment of individuals in identical situations based on traits like gender or race.

The reasons behind the emergence of biases have a direct connection to the data that artificial intelligence-based platforms are able to obtain[8]. In this

[4] *New Study: AI Chatbots Surpass the Average Human in Creativity,* SciTechDaily, 15 September 2023, online at https://scitechdaily.com/new-study-ai-chatbots-surpass-the-average-human-in-creativity/#:~:text=A%20recent%20study%20published%20in%20the%20journal%20Scientific,common%20items%20%E2%80%93%20a%20reflection%20of%20divergent%20thinking, accessed on 08.05.2024.

[5] Future of life Institute, Pause Giant AI Experiment: An Open Letter, 22 Marth 2023, online at https://futureoflife.org/open-letter/pause-giant-ai-experiments/, accessed on 08.05.2024.

[6] *Declaration on Ethics and Data Protection In Artificial Intelligence,* 40 th International Conference of Data Protection and Privacy Commissioners, 23 October 2018, online at: https://www.privacyconference2018.org/system/files/2018-10/20180922_ICDPPC-40th_AI-Declaration_ADOPTED.pdf, accessed on 08.05.2024.

[7] R. Schwartz, A. Vassilev, L. Perine, A. Burt, P. Hall, *Towards a Standard for Identifying and Managing Bias in Artificial Intelligence,* NIST Special Publication 1270, online at https://doi.org/10.6028/NIST.SP.1270, accessed on 08.05.2024.

[8] M. Rijmenam, *Privacy in the Age of AI: Risks, Challenges and Solutions,* The Digital Speaker, 17 February 2023, online at https://www.thedigitalspeaker.com/privacy-age-ai-risks-challenges-solutions/, accessed on 12.05.2024.

regard, for its development, AI is trained on a large amount of data that is specific to the field in which it is used[9]. As a rule, artificial intelligence system developers should collect only representative data. However, in practice, they „*amass their training sets through automated tools that catalog and extract data from the Internet"*[10]. Simply put, AI has access to any kind of content, including pirated books[11], public Facebook and Instagram posts[12] or information from Wikipedia or Reddit. Despite the fact that the vast majority of the information provided is correct, there is a risk of „infiltrating" a set of fake information[13]. So, in some circumstances, artificial intelligence is „fed" data that does not match reality, perpetuating false responses[14].

AI biases are classified into a variety of categories, the most prevalent of which are systemic. These types of biases occur unintentionally as a result of institutional policies that favour particular social categories. At the same time, biases may arise as a result of incorrect analysis of data sources used to train artificial intelligence systems. One example in this sense are the results provided by image-generating platforms, which associate men with the most well-paid jobs, such as doctors or programmers, while women are associated with activities particular to previous centuries, such as housekeepers. In this regard, Stable Diffusion, a platform that converts text into images, has generated images in which women are underrepresented in the majority of industries. Thus, „*women made up a tiny fraction of the images generated for the keyword judge – about 3% – when in reality 34% of US judges are women, according to the National Association of Women*

[9] ET Online, *AI and Privacy: The privacy concerns surrounding AI, its potential impact on personal data*, The Economic Times, 25 April 2023, online at https://economictimes.indiatimes.com/news/how-to/ai-and-privacy-the-privacy-concerns-surrounding-ai-its-potential-impact-on-personal-data/articleshow/99738234.cms?from=mdr, accessed on 12.05.2024.

[10] L. Leffer, *Your Personal Information Is Probably Being Used to Train Generative AI Models,* Scientific American, 19 October 2023, online at https://www.scientificamerican.com/article/your-personal-information-is-probably-being-used-to-train-generative-ai-models/, accessed on 12.05.2024.

[11] A. Reisner, *Revealed: The Authors Whose Pirated Books Are Powering Generative AI,* The Atlantic, 19 august 2023, online at https://www.theatlantic.com/ technology/archive/2023/08/books3-ai-meta-llama-pirated-books/675063/, accessed on 12.05.2024.

[12] K. Paul, *Meta s new AI assistant trained on public Facebook and Instagram posts*, Reuters, 29 september 2023, online at https://www.reuters.com/technology/metas-new-ai-chatbot-trained-public-facebook-instagram-posts-2023-09-28/, accessed on 13.05.2024.

[13] M. Khatri, *Data Privacy in the Age of Artificial Intelligence (AI),* Linkedin, 18 august 2023, online at https://www.linkedin.com/pulse/data-privacy-age-artificial-intelligence-ai-mousam-khatri, accessed on 13.05.2024.

[14] R. Healey, *Data Privacy Compliance a Significant Challenge to AI Technology,* Formiti Data International, online at https://formiti.com/data-privacy-compliance-a-significant-challenge-to-ai-technology/, accessed on 16.05.2024.

Judges and the Federal Judicial Centre"[15]. This example demonstrates that historical data takes precedence over current statistics, with artificial intelligence prioritizing quantity over quality of data. In other words, artificial intelligence is now incapable of distinguishing between historical data and reality.

Apart from gender-related biases, artificial intelligence also generates erroneous replies based on the race of the individuals engaged[16]. Hence, Stable Diffusion „*generated images of people with darker skin tones 70% of the time for keyword fast-food worker, even though 70% of fast-food workers in the US are white*"[17]. At the same time, „*more than 80% of the images generated for the keyword inmate were of people with darker skin, even though people of colour make up less than half of the US prison population, according to the Federal Bureau of Prisons*"[18]. Therefore, once again, biases occur because AI does not take into account the statistical data currently available, which leads to the appearance of biases[19].

This situation is not unique to the Stable Diffusion platform. Even now, Midjourney and Dall-e, the two most popular text-to-image AI platforms, still generate biased images. In a test, the researcher requested Midjourney to generate images of Barbie dolls, each of which had to represent a specific state. The outcomes were full of biases, „*several of the Asian Barbies were light-skinned, Thailand Barbie, Singapore Barbie, and the Philippines Barbie all had blonde hair, and Germany Barbie wore military-style clothing*"[20]. Similar results were obtained when the platform was asked to submit 100 images of citizens living in particular states. In this regard, „*an Indian person is almost always an old man with a beard, a Mexican person is usually a man in a sombrero, while American person appeared to be overwhelmingly portrayed by the presence of U.S. flags"*[21].

While the number of biases perpetuated by artificial intelligence is immense, we will focus on those that already affect us directly, notably in domains such as recruitment, public security, and medicine. Furthermore, we will discuss results from an experiment that demonstrated humans' predisposition to embrace and spread AI-generated incorrect responses.

[15] L. Nicoletti, D. Bass, *Humans are Biased. Generative AI is even worse,* Bloomberg Technology, 9 June 2023, online at https://www.bloomberg.com/graphics/2023-generative-ai-bias/, accessed on 17.05.2024.

[16] T.J. Thomson, R.J. Thomas, *Ageism, sexism, classism and more: 7 examples of bias in AI-generated images*, The Conversation, 10 iuly 2023, online at https://theconversation.com/ageism-sexism-classism-and-more-7-examples-of-bias-in-ai-generated-images-208748, accessed on 17.05.2024.

[17] L. Nicoletti, *op. cit.*

[18] *Ibidem.*

[19] S. Kapoor, A. Narayanan, Quantifying ChatGPT's gender bias, AI Snake, 26 April 2023, online at https://www.aisnakeoil.com/p/quantifying-chatgpts-gender-bias, accessed on 18.05.2024.

[20] V. Turk, *How AI reduces the world to stereotypes,* Rest of World, 18 October 2023, online at https://restofworld.org/2023/ai-image-stereotypes/, accessed on 19.05.2024.

[21] *Ibidem.*

1.1. AI Biases in Recruitment: Challenges and Implication

As noted earlier, artificial intelligence is fed a vast amount of data and is capable of processing all the information really quickly. In light of these capabilities, a number of companies have begun developing systems that let them streamline the hiring process.

As a rule, the recruitment process involves several stages, including the search phase, screening, interviews, and candidate selection. The search phase can be almost entirely automated, with artificial intelligence capable of analyzing the profiles of candidates who have posted their resumes on recruitment websites. Following the analysis of public data, artificial intelligence could suggest to the company to make job offers to candidates who best match the established requirements. At the same time, artificial intelligence could also be used in the screening phase, where it would analyse candidate profiles to identify the most suitable person for a particular position. In both cases, at least in theory, the human factor that might reject candidates due to biases against a certain group of people would be eliminated. Furthermore, since artificial intelligence can review hundreds of resumes in a short amount of time, it would take less time to review candidate profiles.

Artificial intelligence may suggest hiring some applicants over others without adequate justification. For example, Amazon developed a platform to review candidate resumes for specific technology industry positions[22]. The computer models „*were trained to vet applicants by observing patterns in resumes submitted to the company over a 10-year period*,” most of which came from men[23]. As a result, the artificial intelligence „learned” that male candidates were preferable, rejecting resumes submitted by women. This behaviour can be explained by the quality of the data Amazon used to develop the platform, which was unrepresentative. In other words, because the platform was trained with information that no longer reflects reality, it adopted biased behaviour, even though none of the parties involved intended for this to happen[24].

1.2. AI Biases in Healthcare and Public Security

Public security is another area where artificial intelligence may be used. For example, officials in the United States identify people who might be involved in criminal behaviour using facial recognition technology. This technology is „*an artificial intelligence-powered technology that tries to confirm the identify of a person*

[22] IBM Data and AI Team, *Shedding light on AI bias with real world examples,* 16 October 2023, online at Shedding light on AI bias with real world examples – IBM Blog, accessed on 19.05.2024.

[23] J. Dastin, *Insight – Amazon scraps secret AI recruiting tool that showed bias against women*, Reuters, 11 October 2018, online at https://www.reuters.com/article/idUSKCN1MK0AG/, accessed on 20.05.2024.

[24] C. Kerry, *Protecting privacy in an AI-driven world,* Brookings, 10 February 2020, online at https://www.brookings.edu/articles/protecting-privacy-in-an-ai-driven-world/, accessed on 20.05.2024.

from an image"[25]. So, the mechanism involves providing a description of the potential offender to the artificial intelligence system, which uses databases maintained by authorities to generate a list of possible suspects. Due to the overrepresentation of people of colour in law enforcement databases, artificial intelligence sometimes provides incorrect answers, identifying these individuals as potential suspects even when the police officers do not specify the race of the offenders. Consequently, there are situations where individuals with no connection to the investigated case are detained. Because of these kinds of errors, cities like Boston and San Francisco have banned the use of facial recognition technology to identify criminals[26].

If in the case of databases used for training facial recognition technologies, the category of people of colour is overrepresented, in the case of platforms used in the medical field, the situation is diametrically opposite[27]. Thus, in the United States, the databases provided for the development of platforms used in hospitals come from three states, namely California, Massachusetts, and New York, and these are not representative, with only 8.7% of respondents reporting their race and ethnicity. The same situation is valid in the United Kingdom, where out of 500,000 patients, only 6% are non-European. As a result, the use of artificial intelligence is not effective when called upon to provide answers regarding patients from categories underrepresented in the databases with which it was trained.

For example, artificial intelligence is used to identify melanoma, a form of skin cancer, and it performs quite well when the images provided are of white individuals. However, the chances of melanoma being identified in Hispanics and people of colour are reduced, which can be explained by the lack of databases in which these categories of people are represented in a sufficient numbers[28].

In this regard, the specialized literature refers to the „Asan" database and the "Dermofit" database to demonstrate that the underrepresentation of certain categories of people can lead to a decrease in the accuracy with which artificial intelligence identifies melanoma[29]. Thus, the „Asan" database contains images

[25] T.L. Johnson, N.N. Johnson, *Police Facial Recognition Technology Can't Tell Black People Apart,* Scientific American, 18 May 2023, online at: https://www.scientificamerican.com/article/police-facial-recognition-technology-cant-tell-black-people-apart/, accessed on 20.05.2024.

[26] *Ibidem.*

[27] T. Zack, E. Lehman, M. Suzgun, J. A. Rodriguez, et. al., *Accessing the potential of GPT-4 to perpetuate racial and gender biases in health care: a model evaluation study*, The Lancet Digital Health, Volume 6, Issue 1, E12-E22, January 2024, online at: https://doi.org/10.1016/S2589-7500(23)00225-X, accessed on 21.05.2024.

[28] J. Buolamwini, T. Gebru, *Gender Shades: Intersectional Accuracy Disparties in Commercial Gender Classification,* Proccedings of Machine Learning Research, 81: 1-15, Conference on Fairness, Accountability, and Transparency, January 2018, online at https://proceedings.mlr.press/v81/buolamwini18a.html, accessed on 21.05.2024

[29] M. Gayal, *Artificial intelligence-based image classification methods for diagnosis of skin cancer: Challenges and opportunities*, Computers in Biology and Medicine, Volume 127,

specific to the Asian population, while the "Dermofit" database contains images specific to Caucasians. The authors of the study asked the artificial intelligence to identify people from Asia who are predisposed to melanoma, with a result of 80% for platforms that used the „Asan" database and only 56% for the platform that was trained on the „Dermofit" database[30]. Through this study, it was demonstrated that artificial intelligence cannot apply the algorithms it uses to identify medical conditions in one group of patients to other categories of people for which it does not have sufficient data. However, artificial intelligence does not refuse to provide an answer, citing a lack of data.

1.3. Perpetuating AI-Generated Biased Responses

Unfortunately, even when artificial intelligence makes recommendations that are obviously incorrect, people still have a tendency to follow them. In an experiment[31], 169 students had to decide if the people who appeared in the images provided had Lyndsay syndrome or not. The students were split up into two groups. The first group was assisted by artificial intelligence, while the other group had to make decisions without external help. In order to find out if student decisions may be influenced, artificial intelligence was programmed to provide 10 incorrect answers[32]. As anticipated, the artificial intelligence-assisted students made more errors and provided incorrect answers far more frequently than the students in the other control group.

The second experiment involved dividing the students into two distinct groups again, but the novelty was adding 25 additional images for the students to analyse independently. Thus, in the first phase, the conditions were similar to those of Experiment 1, with one group of students assisted by artificial intelligence and another not, but in the second phase both groups were placed in equal conditions, with the participation of artificial intelligence excluded. The purpose of this experiment was to see if students would repeat the incorrect answers that artificial intelligence had recommended in similar contexts. As before, the students who received artificial intelligence assistance produced lower-quality findings than the other group, indicating that people are more likely to spread mistakes that are made while interacting with AI.

December 2020, online at: https://doi.org/10.1016/j.compbiomed.2020.104065, accessed on 22.05.2024

[30] *Ibidem.*

[31] L. Vicente, H. Mature, *Humans inherit artificial intelligence biases*, Scientific reports, 3 october 2023, online at https://www.nature.com/articles/s41598-023-42384-8, accessed on 22.05.2024.

[32] Duesto University, *Trapped in a Dangerous Loop: Humans Inherit Artificial Intelligence Biases*, SciTechDaily, 3 October 2023, online at https://scitechdaily.com/trapped-in-a-dangerous-loop-humans-inherit-artificial-intelligence-biases/#:~:text=People%20can%20adopt%20biases%20from%20artificial%20intelligence%20in,%28systematic%20errors%20in%20AI%20outputs%29%20in%20their%20decisions, accessed on 23.05.2024.

In the last experiment, both groups used artificial intelligence to answer 80 questions divided into two sets of 40 questions each. In the first phase, artificial intelligence supported one group, while in the second phase, it was utilized by the other group. In other words, the researchers wanted to verify if students who were not initially assisted by artificial intelligence would provide more correct answers compared to those who were assisted from the beginning. The results demonstrate, once again, that humans are predisposed to perpetuate the erroneous responses suggested by artificial intelligence[33]. Thus, students who were assisted by artificial intelligence in the first phase continued to make errors in the second phase, unlike the other group of students who made errors only when assisted by artificial intelligence.

Summarizing the points presented, we appreciate that we have managed to demonstrate that artificial intelligence can unintentionally provide responses containing erroneous information. Furthermore, the last example also shows how humans are inclined to have too much trust in artificial intelligence, adopting its logical errors. This fact is extremely concerning, especially because artificial intelligence is widely used in fields such as medicine and law enforcement. Consequently, there are cases in which the answers given by artificial intelligence violate individual freedoms or make it more difficult for them to get the care they need[34]. However, artificial intelligence cannot be entirely held liable since humans are the ones who make the final decisions.

At the same time, we chose to present as many examples from different domains as possible to demonstrate that the premises leading to biased responses are diverse, making it extremely difficult to identify a universal solution. However, a common element can be identified, namely the existence of a disproportionality in the information from the databases used to train artificial intelligence. In this regard, the suggestion of lower-paying professions for women and people of colour is the result of the prevalence of historical data suggesting that white men have held professions such as judges or directors. On the other hand, providing erroneous responses regarding the identification of diseases such as skin cancer is the result of the underrepresentation of certain categories of people. In other words, the lack of balance in the information with which artificial intelligence is trained leads to the perpetuation of biases and the provision of wrong solutions.

[33] L. Leffer, *Humans Absorb Bias from AI—And Keep It after They Stop Using the Algorithm*, Scientific American, 26 October 2023, online at https://www.scientificamerican.com/article/humans-absorb-bias-from-ai-and-keep-it-after-they-stop-using-the-algorithm/, accessed on 23.05.2024.

[34] H. Zhang, A.X. Lu, M. Abdalla, M. McDemott, M. Ghassemi, *Hurtful Words: Quantifying Biases in Clinical Contextual Word Embeddings,* ACM Conference on Health, Inference and Learning, 11 Marth 2020, online at https://doi.org/10.1145/3368555.3384448, accessed on 24.05.2024.

2. Exploring Potential Legislative Solutions for AI Biases

In the first section of this paper, we addressed a number of concerns that artificial intelligence could bring to society, with a particular focus on the biased answers it may generate across a variety of fields. These potential concerns have already caught the attention of national authorities in a number of states, leading to the adoption of artificial intelligence-related regulation. We opted to investigate legislative measures developed in two of the world's main economies, the European Union and the United States of America, to evaluate potential actions taken, with a particular focus on whether regulations address or not the issue of biased responses.

2.1. EU Strategies for Mitigating AI Biases

Most of the risks mentioned in the previous section have been acknowledged by the bodies of the European Union[35], leading to the development of the of the Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonized Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts[36]. For example, according to recital 18, „*the use of AI systems for 'real-time' remote biometric identification of natural persons in publicly accessible spaces for the purpose of law enforcement is considered particularly intrusive in the rights and freedoms of the concerned persons, to the extent that it may affect the private life of a large part of the population, evoke a feeling of constant surveillance, and indirectly dissuade the exercise of the freedom of assembly and other fundamental rights*". So, the European Union seeks to restrict the use of artificial intelligence in sensitive domains like public space surveillance.

However, according to Article 5, recital 1, letter d), „*the use of real-time remote biometric identification systems in publicly accessible spaces*" is permitted for targeting searches „*for specific potential victims of crime, including missing children*" or for „*the prevention of a specific, substantial, and imminent threat to the life or physical safety of natural persons or of a terrorist attack.*" The use of artificial intelligence to locate victims of crimes or prevent threats could be beneficial, especially considering that authorities currently use various methods involving surveillance of publicly accessible spaces, such as consulting recordings from CCTV cameras. Furthermore, unlike the United States, artificial intelligence is intended to be used for victim identification, with situations where erroneous

[35] European Commision, *AI Act*, Shaping Europe's digital future, online at https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai, accessed on 25.05.2024.

[36] Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonized Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, online at: https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0001.02/DOC_1&format=PDF, accessed on 26.05.2024.

answers based on biased information can be provided being limited. In this regard, most likely, artificial intelligence will obtain data characterizing the victim, such as a photo or a sufficiently detailed description, with the platform focusing only on finding a clearly identified person.

The situation is diametrically opposite in the second situation, governed by Article 5(1)(d) of the proposed regulation. The legal provision addresses two unique situations: the use of artificial intelligence to prevent specific, significant, and imminent dangers to people's lives or physical safety, and the use of artificial intelligence to prevent a terrorist attack. In the last case, artificial intelligence will most likely be deployed in scenarios where there is sufficient proof that a terrorist act is likely to occur, with artificial intelligence serving just as a tool to streamline the work of the participating authorities.

We appreciate that it would be extremely difficult for artificial intelligence to be used for such a purpose, as the data provided would in most cases be extremely vague, not allowing for the clear identification of individuals who may be preparing a terrorist attack, and there is also the risk that artificial intelligence may provide biased suggestions. In this regard, the training data provided to artificial intelligence could indicate that individuals with a certain appearance have most often committed terrorist attacks[37]. As a result, there is a possibility that individuals identified by artificial intelligence may have no connection to potential terrorist acts, resulting in the misallocation of human resources. We believe that artificial intelligence should only be used once potential terrorists have been identified through other methods, with the platform being used to ensure their traceability.

Regarding the second case covered by Article 5(d)(2) of the Proposed Regulation, we recognize that the legal provision's formulation is exceedingly ambiguous, providing a danger of abuse by authorities. Thus, under the concept of specific dangers to people's lives or physical safety, any violent acts or activities may be included, and it is unclear how artificial intelligence may be utilized to prevent them. In this sense, the real-time remote biometric identification system has been defined as a *„system whereby the capturing of biometric data, the comparison, and the identification all occur without a significant delay. This comprises not only instant identification but also limited short delays in order to avoid circumvention”*. We believe that artificial intelligence will have access to surveillance cameras, allowing it to monitor in real time if there is cause for a specific action that could be categorized as a threat to individuals. Such 'surveillance' should be authorized in advance by a judicial or administrative authority.

It is difficult for us to identify a situation where compelling reasons could be presented to allow artificial intelligence access to devices collecting biometric data for the purpose of preventing acts of violence. Perhaps the provision provided

[37] A. Abid, M. Farooqi, J. Zou, *Persistent Anti-Muslim Bias in Large Language Models,* AAAI/ACM Conference on AI, Ethics, and Society, 14 January 2021, online la https://doi.org/10.1145/3461702.3462624, accessed on 26.05.2024.

in Article 5 (d) (2) of the Proposed Regulation could be used in a situation where competent authorities have information regarding the preparation of a potential assassination and artificial intelligence would be used to timely identify suspects. However, similar to the prevention of terrorist attacks, the use of artificial intelligence could only be useful if there is sufficient data regarding the individuals who need to be identified; otherwise, there is a risk of providing erroneous responses.

In addition to the above, the Proposed Regulation mentions that artificial intelligence systems which are „*used in education or vocational training, notably for determining access or assigning persons to educational and vocational training institutions or to evaluate persons on tests as part of or as a precondition for their education should be considered high-risk, since they may determine the educational and professional course of a person's life and therefore affect their ability to secure their livelihood*". Even though a series of highly dangerous risks have been identified, the use of artificial intelligence in the field of education will not be prohibited. Classifying these systems as having a high level of risk is intended to limit potential disadvantages.

Developers of artificial intelligence systems will be required to comply with the requirements set out in Article 9 of the Proposed Regulation, including periodic testing of systems to identify, eliminate, or reduce risks. In close connection with the theme of this article, it is explicitly stated that „*training, validation, and testing data sets shall be relevant, representative, free of errors, and complete. They shall have the appropriate statistical properties, including, where applicable, as regards the persons or groups of persons on whom the high-risk AI system is intended to be used. These characteristics of the data sets may be met at the level of individual data sets or a combination thereof.*" We consider this legal provision beneficial, as it eliminates the risk of biased responses.

Meanwhile, the legal provision is extremely restrictive, which could slow down the development of artificial intelligence in the European Union. In other words, developers are required to identify representative databases for each Member State separately, which is why we believe that AI systems will only be developed in those states where compliance with the rules set out in the proposed regulation would be financially justified.

The same conclusions apply to AI systems used in „*employment, workers management and access to self-employment, notably for the recruitment and selection of persons, for making decisions on promotion and termination and for task allocation, monitoring or evaluation of persons in work-related contractual relationships, should also be classified as high-risk, since those systems may appreciably impact future career prospects and livelihoods of these persons*". We have already demonstrated that attempts to use artificial intelligence for personnel recruitment have not been successful, as the solutions offered have been influenced by unrepresentative databases[38].

[38] N. Hanacek, *There's More to AI Bias Than Biased Data, NIST Report Highlights*,

Furthermore, in the field of workforce management, the notion of representative databases should be nuanced. In this regard, there are sufficient professions where the number of male employees outweighs the number of female employees, and vice versa. Training artificial intelligence on databases where the number of employees of a certain gender prevails could lead to the promotion of biases, with Amazon's example being illustrative. For these reasons, we believe that artificial intelligence may not be effectively used in the field of employee recruitment. One possible solution could be to program artificial intelligence to identify one candidate from different categories based on a set of predefined criteria, such as race or gender, allowing the employer to decide which of the suggested individuals best meets the requirements.

2.2. U.S. Initiatives to Combat AI Biases

Regarding the United States of America, on October 30, 2023, President Biden signed the Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence[39]. In its preamble, it explicitly states that the irresponsible use of artificial intelligence could „*exacerbate societal harms such as fraud, discrimination, bias, and disinformation; displace and disempower workers; stifle competition; and pose risks to national security*". At the same time, artificial intelligence systems „*have reproduced and intensified existing inequities, caused new types of harmful discrimination, and exacerbated online and physical harms*".

Therefore, the competent authorities in the U.S. have identified the main risks generated by artificial intelligence, which is why they proposed the adoption of a legislative act aimed at eliminating or at least reducing them. Unlike the regulation adopted at the European Union level, the executive order explicitly addresses the most risky areas where artificial intelligence can have more negative effects than positive ones.

For instance, in the medical sector, as we presented earlier in this paper, artificial intelligence provides a series of biased responses, leading either to the establishment of inappropriate treatment or to limiting the right to access quality services[40]. To mitigate these disadvantages, competent authorities have to develop

National Institute of Standards and Technology, 16 Marth 2022, online at https://www.nist.gov/news-events/news/2022/03/theres-more-ai-bias-biased-data-nist-report-highlights, accessed on 25.05.2024.

[39] WH.GOV, *Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence,* Presidential Actions, 30 October 2023, online at https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence /, accessed on 25.05.2024.

[40] C. Grant, Algorithms Are Making Decisions About Health Care, Which May Only Worsen Medical Racism, ACLU Speech, Privacy, and Technology Project, 3 October 2022, online at https://www.aclu.org/news/privacy-technology/algorithms-in-health-care-may-worsen-medical-racism, accessed on 25.05.2024.

„a strategic plan that includes policies and frameworks – possibly including regulatory action, as appropriate – on responsible deployment and use of AI and AI-enabled technologies in the health and human services sector (including research and discovery, drug and device safety, healthcare delivery and financing, and public health)”. In this regard, the strategies to be adopted must ensure the use of representative databases and the exclusion or reduction of biased and discriminatory responses, both by current systems and those under development. At the same time, special attention is paid to identifying the erroneous responses provided by artificial intelligence at the present time.

Indeed, the reduction of discrimination and bias is likely to be achieved through the development of representative databases tailored to the intended purpose. We acknowledge that there is a risk that the development of artificial intelligence systems may not proceed as rapidly, as the quantity of training data will be significantly reduced. At the same time, it remains to be seen how developers of artificial intelligence systems will eliminate the unrepresentative data that has already been used to train the platforms. By „extracting” databases, it is likely that some systems will experience a downgrade, requiring them to restart their training processes.

In addition to the medical sector, the executive order stipulates that competent authorities must develop regulatory acts to govern the use of artificial intelligence in areas such as recruitment, access to credit, and other domains where the technology's impact could lead to discrimination.

We appreciate that the legislation developed in the United States will likely respond better to the risks posed by artificial intelligence, as it attempts to directly address the most significant disadvantages, unlike the Regulation adopted at the European Union level, which has established a series of domains in which artificial intelligence cannot be used and has stipulated a series of restrictive obligations that platform developers must adhere to. On the other hand, the regulatory acts mentioned in the executive order have yet to be written, so creators of artificial intelligence-based systems are uncertain of how restrictive the legal restrictions would be, leading to hesitancy in making choices. The Regulation established at the European Union level is scheduled to go into effect in June 2024, giving predictability for those affected, who will be able to adjust considerably more rapidly to the new requirements.

Conclusions

Artificial intelligence has a significant impact on society, with the number of benefits, in our opinion, outweighing the existing disadvantages. However, both in specialized literature and in the public sphere, a series of risks have been presented that indeed seem justified. In this paper, we chose to focus only on the replication and spread by artificial intelligence of biased and discriminatory responses in various fields, such as medicine or public security[41]. From what has been presented, it emerges that there are situations in which the use of artificial intelligence has had a negative impact on the fundamental rights of the individuals involved, limiting either their freedom or their right to access quality medical services.

The mentioned risks have been recognized by both AI system developers and European and American legislators, leading to the adoption of several regulatory acts directly governing the use of artificial intelligence. The adopted legal provisions are likely to have a negative impact on the development of artificial intelligence. In this regard, imposing restrictions on the quality of data used to train artificial intelligence systems will primarily result in additional costs. Developers will be required to identify representative databases for the sector in which artificial intelligence is to be used, no longer being able to simply access unverified information resources. Consequently, the operating costs of artificial intelligence will increase, likely resulting in its use only in sectors that offer a sufficiently high return on investment to justify the costs. At the same time, cost escalation implies limiting the number of companies that could participate in the development of the sector, potentially leading to its monopolization by Big Tech.

However, we appreciate that adopting regulatory acts in the early stages of artificial intelligence development is beneficial, as it eliminates the risk of AI system developers having to start the process from scratch in the future. In any case, the subjects targeted by the Regulation adopted at the European Union level have had access to relevant information since 2021, having sufficient time to adapt. Due to the new regulations, both existing platforms and those yet to emerge will offer far fewer biased and discriminatory responses, making artificial intelligence an extremely useful tool for society.

References

Abid A., Farooqi M., Zou J., *Persistent Anti-Muslim Bias in Large Language Models,* AAAI/ACM Conference on AI, Ethics, and Society, 14 January 2021, https://doi.org/10.1145/3461702.3462624.

Schwartz R., Vassilev A., Perine L, Burt A., Hall P., *Towards a Standard for Identifying and Managing Bias in Artificial Intelligence,* NIST Special Publication 1270, https://doi.org/10.6028/NIST.SP.1270.

Zack T., Lehman E., Suzgun M., Rodriguez J.A., et. al., *Accessing the potential of GPT-4 to perpetuate racial and gender biases in health care: a model evaluation study*, The Lancet Digital Health, Volume 6, Issue 1, E12-E22, January 2024, https://doi.org/10.1016/S2589-7500(23)00225-X.

Zhang H., Lu A.X., Abdalla M., McDemott M., Ghassemi M., *Hurtful Words: Quantifying Biases in Clinical Contextual Word Embeddings,* ACM Conference on Health, Inference and Learning, 11 MAarth 2020, https://doi.org/10.1145/ 3368555.3384448.

[41] Information Commissioners Office (ICO), *Guidance on AI and data protecion,* 15 Marth 2023, online at https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/ ?template=pdf&patch=17#link1, accessed on 29.05.2024.

Information Commissioner s Office (ICO), *Guidance on AI and data protecion,* 15 Marth 2023, [Online]

Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonized Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, [Online]

WH.GOV, *Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence,* Presidential Actions, 30 October 2023, [Online]

ANALELE ŞTIINŢIFICE ALE UNIVERSITĂŢII „ALEXANDRU IOAN CUZA" DIN IAŞI
TOM LXX, 2, ŞTIINŢE JURIDICE, 2024

DOI: 10.47743/jss-2024-70-2-4

Evolution of Legal Systems in the Digital Era: An Analysis of Artificial Intelligence in E-Business

Elena SÂRGHI[1], **Marian ILEANA**[2]

Abstract: The paper examines the changes in the legal field brought about by digital technology, especially artificial intelligence. Focusing on how these changes have impacted the online business environment. The study wants to analyze how tools such as contract analysis algorithms, virtual legal assistance systems, and other solutions based on artificial intelligence bring new challenges to this field. At the same time, the article highlights the opportunities and challenges brought by these technological developments. Among the most important issues are data security, privacy, legal liability, and how traditional legal systems adapt to new digital requirements. It also examines how legal professionals are prepared to adapt to the changes brought about by the growth of e-commerce. The analysis shows how well artificial intelligence can ease legal processes specific to e-commerce. Access to justice and the costs and time needed to resolve disputes can be significantly reduced with the help of new technologies. The article helps to understand how changes in legal systems are directly influenced by the digitization of the online commerce environment.

Keywords: Artificial intelligence, E-Business, Digital Legal Systems, Digital Jurisprudence, Cyber Laws

Introduction

Socio-economic paradigms, including the legal system, have been completely redefined by the rapid developments of technology in the modern world. Given the context of digitization, legal systems are changing rapidly. This has created a number of unique issues and opportunities that have a significant impact on the business environment. This transformation involves a significant integration of artificial intelligence in the legal field, especially in the field of e-business.

E-business is a new sector of the economy that emerged and grew as a result of the transformation of a significant number of business processes in the

[1] „Alexandru Ioan Cuza University" of Iași, Romania, e-mail: sarghielena7@gmail.com.

[2] National University of Science and Technology Politehnica Bucharest, Pitesti University Center, Romania, e-mail: marianileana95@gmail.com.

virtual environment[3]. E-business is a form of business that uses the Internet to modify a company's internal and external relationships in order to generate revenue[4]. In many economies around the world, e-business is continuously expanding.

Researchers claim that information and communication technology, machine learning, digitization, robotics, and artificial intelligence (AI) will lead to the fourth industrial revolution[5]. Computers will influence business marketing practices and society; they will be used for decision-making[6]. Compared to the industrial and digital revolutions, the artificial revolution will have a much more significant impact in the next twenty years[7]. The latest studies have shown that the development of smart products and services is not just a marketing business, as they have seen significant growth and improvement, and according to studies, they have the ability to transform the world[8].

Before discussing artificial intelligence, it is important to understand the concept of "intelligence". It represents a person's ability to learn, think abstractly, cope with new situations, and use information to control the environment[9]. Intelligence is the ability to understand, reason, facts, opinions, judgment, skills, calculations, information, and language to memorize, apply, and generalize knowledge, experience, understanding, planning, abstract thinking, problem solving, rapid learning, overcoming difficulties, and adapting to change[10].

The extent to which machines can partially or completely replace humans in performing specific tasks is what led to the idea of AI[11]. So, marketing research uses the term "human intelligence" to describe artificial intelligence. For example, researchers consider artificial intelligence to imitate intelligent human behavior, to

[3] L. Chen, C.W. Holsapple, *E-business adoption research: state of the art, Journal of Electronic Commerce Research*, *14*(3), 2013, p. 261.

[4] M. Ileana, M.I. Oproiu, C.V. Marian, *E-commerce solutions using distributed web systems with microservices-based architecture for high-performance online stores*, 2024 47th MIPRO ICT and Electronics Convention (MIPRO), IEEE, May 2024, pp. 994-999.

[5] M. Xu, J.M. David, S.H. Kim, *The fourth industrial revolution: Opportunities and challenges. International Journal of Financial Research*, *9*(2), 2018, pp. 90-95.

[6] Y.K. Dwivedi, L. Hughes, E. Ismagilova, G. Aarts, C. Coombs, T. Crick, M.D. Williams, *Artificial Intelligence (AI): Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. International Journal of Information Management*, *57*, 2021, p. 101.

[7] S. Makridakis, *The forthcoming Artificial Intelligence (AI) revolution: Its impact on society and firms. Futures*, *90*, 2017, pp. 46-60.

[8] N. Soni, E.K. Sharma, N. Singh, A. Kapoor, *Artificial intelligence in business: from research and innovation to market deployment. Procedia Computer Science*, *167*, 2020, pp. 2200-2210.

[9] N. Brody, *What is intelligence?, International Review of Psychiatry*, *11*(1), 1999, pp. 19-25.

[10] *Idem*, pp. 19-25.

[11] F.D. Weber, R. Schütte, State-of-the-art and adoption of artificial intelligence in retailing. Digital Policy, Regulation and Governance, 21(3), 2019, pp. 264-279.

imitate human intelligence, or to imitate non-biological intelligence[12]. In the same way, McCarthy[13] defines artificial intelligence as "the science and engineering of making intelligent machines, especially intelligent computer programs". Using computers to understand human intelligence is a similar task for AI; however, AI is not limited to only observable biological methods. Such definitions make human intelligence essential to artificial intelligence[14].

AI can identify trends, intents, and patterns beyond human intelligence with the help of big data and deep learning. Machines have the capacity to interpret billions of pieces of data, but the human brain can only do a small part of that[15]. The "four processes of intelligence"—that is, from analytical to emotional thinking—have been used by artificial intelligence to develop complex capabilities such as planning, conceptual learning, creativity, common sense, cross-domain thinking, reasoning, and even elf-awareness itself. Companies involved in e-commerce perform a variety of business processes, such as marketing, buying, selling, and servicing of products and services. These businesses rely entirely on e-commerce applications and Internet-based technologies to do marketing, research, processing, transactions, and providing customer and product services [16].

Finally, this article aims to provide an in-depth analysis of the changes in legal systems in the digital age, with increased attention to the impact of artificial intelligence in the e-business environment. A thorough analysis of these elements provides a complex picture of the changes taking place, but it will also lay the foundations for evaluating how new technologies directly influence the legal environment and business.

Normative framework

In this section we will analyze the main elements of the national and European normative framework in the matter of e-business, highlighting the implications of artificial intelligence in the business field, the way in which the legislator facilitates the development of trade through the various tools created around AI.

[12] M.H. Huang, R.T. Rust, *Artificial intelligence in service. Journal of service research, 21*(2), 2018, pp. 155-172.

[13] J. McCarthy, From here to human-level AI. Artificial Intelligence, 171(18), 2007, pp. 1174-1182.

[14] M. Rusoaie, E-business models in Romania, dissertation work, Polytechnic University of Timișoara, Faculty of Management in Production and Transport, Timișoara, 2008, p. 8, available online at: https://www.academia.edu/23738388/Modele_e_business_%C3%AEn_Rom%C3%A2nia, accessed on December 17, 2023.

[15] K.B. Forrest, *Being "Human" in the Age of Artificial Intelligence. Ct. Rev., 59*, 2023, p. 4.

[16] D.E. Bock, J.S. Wolter, O.C. Ferrell, *Artificial intelligence: disrupting what we know about services. Journal of Services Marketing, 34*(3), 2020, pp. 317-334.

We start with the internal regulation, bringing into discussion Law no. 365/2002 on electronic commerce,[17] we will note that this is the main normative act that regulates the way of organizing business in a manner simplified by the digital factor. Thus, according to this law, there is a derogation from certain provisions of common law regarding the negotiation of distance contracts, namely art. 1.193 Civil Code, the offer made to an absent person, followed by negotiation, acceptance and conclusion of the contract, as art. 9 provides that the conclusion is made by accepting the offer, without referring to the negotiation, and art. 7 para. (1) stipulates that the agreement of the parties on the use of electronic means is not necessary, an aspect likely to accelerate the conclusion of these electronic contracts and preventing the recipient from invoking in court the failure to express prior agreement regarding, for example, the platform agreed by the trader.

At the same time, art. 8 of the same law requires the merchant to comply with an information obligation with a broader content than a simple contractual provision, the legislator's will be being to guarantee both parties of the legal act a certain degree of certainty and predictability on the operations that will be carried out. The minimum required by the legislator in terms of information refers to the technical steps that must be followed to conclude the contract, whether the contract, once concluded, is stored or not by the service provider and whether it is accessible or not, the technical means that the service provider provides the addressee with the language in which the contract can be concluded, the relevant codes of conduct to which the service provider subscribes, as well as information on how these codes can be consulted by electronic means, for the identification and correction of errors occurring during data entry.

Closely related to this normative act and the commercial operations regulated by them is Law no. 455/2011 regarding the electronic signature,[18] as the probation of these commercial documents will be carried out in compliance with the provisions of this regulation. According to this normative act, the electronic signature designates data in electronic form, which is attached or logically associated with other data in electronic form and which serves as a method of identification. This definition, quite general, is completed by the one regarding the extended electronic signature, a type of signature, alongside simple and advanced ones. Of these last mentioned, the one that offers the highest degree of certainty on the identity of the contractor, being thus requested by the majority of contractual partners, is the extended electronic signature, defined as the signature that, cumulatively, meets the following conditions: it is uniquely linked of the signatory, ensures the identity of the signatory, is created by means exclusively controlled by the signatory and is linked to the data in electronic form, to which it is related in such a way that any subsequent modification is identifiable.

Therefore, we find a legislative requirement both in the matter of the legal regime of electronic commerce and in regard to the electronic signature, being

[17] M. Of. no. 959/29.11.2006.

[18] M. Of. no. 429/31.07.2001.

ensured, in this way, the premises for carrying out operations of a commercial nature at a distance.

At the European level, there is a variety of normative acts, some regulations, others directives, the choice of the European legislator in adopting a certain legal instrument and not another arises precisely from his desire to ensure either uniformity, when there is a risk of an impossibility of the member states to achieve a uniform framework regarding the means by which a certain result would be reached, or, on the contrary, the achievement of the result is desired more, not placing so much emphasis on the means, the latter being harmonization [8].

The first relevant normative act in the e-business issue is the Directive on electronic commerce,[19] whose principles are: the exclusion of prior authorization, according to which the member states have the obligation to ensure that these information companies carry out their activity without a prior formality, an aspect that would make it difficult significantly the running of these operations, the principle of informing the supplier of some minimum aspects, such as the way of communication, the identity of the parties, the promotional offers. At the same time, an essential principle is the one provided for in art. 9, which concerns the treatment of contracts, an aspect that refers to the relationship between the state and the trader. According to this provision, the member states ensure in particular that the legal regime applicable to the contractual process does not create obstacles to the use of electronic contracts and does not lead to the lack of effect and legal validity of contracts due to their conclusion by electronic means. We observe, therefore, the genesis of the e-commerce law and all the legislative changes that facilitated, to a certain extent, the development of these commercial acts, the source of the state's obligation are of European origin.

Regarding the way in which the recognition of traders will be achieved, we bring to the discussion the Regulation on electronic identification,[20] which defines electronic identification in the following way: the process of using the identification data of individuals in electronic format, uniquely representing either a natural or legal person, or a natural person who represents a legal entity, and the means of identification are represented by a material and/or immaterial unit that contains personal identification data and that is used for the purpose of authenticating an online service. Specifically, one method of identification is the electronic signature, regulated in art. 26 of the Regulation, which imposes exactly the same conditions as those of the Electronic Signature Law. At the same time, identification can also be achieved through advanced electronic seals, electronic temporary marks or qualified registered electronic distribution services.

[19] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, on the internal market, J.O. no. L 178/1.

[20] Regulation (EU) no. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions on the internal market and repealing Directive 1999/93/EC, J.O. no. L 257/73.

Other relevant European normative acts in the field of e-business are the Regulation on cross-border parcel delivery services,[21] the Regulation on the single market for digital services,[22] the GDPR Regulation.[23]

Forms of AI involvement in business law

AI has transformed the field of business law, transforming many outdated methods and processes. These are just some of the ways in which artificial intelligence is involved in business law[24]:

- Contract Analysis and Interpretation: Automating the contract review process by using dedicated machine learning algorithms and training them to be capable of contract analysis and interpretation. This speeds up the review process and helps identify potential issues or critical provisions.
- Online legal assistance: Chatbots with legal capabilities, ready to provide basic legal assistance to customers and employees on a variety of business-related issues.
- Compliance and rule monitoring: Automated monitoring of legislative changes. AI helps companies keep up with legislative and regulatory changes that are relevant to business, ensuring a climate in compliance with the latest legal requirements.
- Conflict Management: Analyzing data for legal processes, using predictive analytics based on artificial intelligence to help make strategic decisions in legal processes.
- Hazard management: Risk analysis from a legal point of view. Implementing AI-based solutions to assess and manage legal risks associated with business decisions, including identifying potential legal issues and creating methods to significantly reduce them.
- Automation of legal processes involving a high degree of routine. Using process automation to handle repetitive legal tasks, such as filling out legal forms or sending documents.

The use of artificial intelligence in business law is an example of the legal sector's continuous adaptation to technological advances, with the aim of improving processes, reducing risks, and providing faster, more accurate, and more efficient legal solutions for the increasingly complex and competitive[25].

[21] Regulation (EU) 2018/644 of the European Parliament and of the Council of 18 April 2018 on cross-border parcel delivery services, J.O. no. L 112/19.

[22] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a single market for digital services and amending Directive 2000/31/EC, J.O. no. L 277/1.

[23] 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/CE, J.O. no. L 119/1.

[24] B. Attard-Frost, A. De los Ríos, D.R. Walters, *The ethics of AI business practices: a review of 47 AI ethics guidelines. AI and Ethics, 3*(2), 2023, pp. 389-406.

[25] *Ibidem.*

Jurisprudence

In order to understand the vast concept of e-business, which is not, *per se*, an online or digital business, but a way of organizing business using information and communication technology tools,[8] in this section we will present some decisions of domestic courts, which analyze the facets of this way of business operation.

In this sense, we are starting with a facility offered by e-business, namely electronic invoicing, which allows the acceleration of debt payment procedures and the reduction of costs related to stationery elements. The problems that arise in relation to the electronic invoice reside in the meaning given by the domestic courts to this notion and the defenses raised by the debtor, in the sense that they would not include all the necessary elements or that they would not present the guarantees of accessibility, if digital programs are used that require certain applications or additional costs for receiving and opening the invoice, or simple technical incompatibility between the device used and the program that distributes the invoice. In this sense, in a case, the court resolved the aspect of defining the notion of electronic invoice, referring to the national provisions, namely the Fiscal Code, although the parts of the disputed civil report were private.

The electronic invoice is, therefore, an invoice that contains the information requested in this article and that was issued and received in electronic format, the information being: date of issue; the identification of the taxable person who delivered the goods or rendered the services, the identification of the type of goods or services provided, the amount of tax collected or the information necessary for its calculation. In the case of documents or messages treated as such, specific and clear reference to the original invoice and the specific details that change. Signing and stamping invoices are not mandatory elements that the invoice must contain.[26]

Specifically, the content that the electronic invoice can have does not differ in a significant way from the classic one, the distinction being the format, which can be a word, pdf or another electronic format, which is at the choice of the taxable person. At the same time, if the document is drawn up in paper format and then scanned and sent electronically, it will still be considered an electronic invoice, the relevance of the qualification referring to how the recipient receives the invoice, and not how it is drafted. Last but not least, if the recipient lists the invoice, in order to archive it in physical format, it will be considered an original copy.[27]

After issuing the invoice, the moment of payment follows, which in the e-business universe is carried out through digital payment systems, such as

[26] Iași Court, Civil Section, sentence no. 10963/2019 of 14.10.2019, available at the online address: http://www.rolii.ro/hotarari/5da91975e49009900a000046, accessed on 17.12.2023.

[27] Bucharest District Court 3, Civil Section, sentence no. 1571/2015 of 10.02.2015. The decision can be read at the online address: http://www.rolii.ro/hotarari/5ba73e04e49009a426000c68, accessed on 17.12.2023.

electronic banking transactions through e-banking. Thanks to the facilities offered by these online payment systems, payments are made through electronic applications not only in business. The main disadvantages relate to securing the services against cyber-attacks and the difficulties regarding the proof, when the amount is high, namely the visa of the paying bank, following that the moment of crediting the account is considered the moment of making the payment.[28]

Another useful tool brought by e-business refers to electronic auctions, which, in the sense of Law no. 98/2016 on public procurement[29] can only be organized in the following situations: as a final stage of the open tender, restricted tender or competitive negotiation procedure, upon the resumption of competition between the economic operators' party to a framework agreement, upon the submission of offers for the award of a public procurement contract within a dynamic procurement system. Judicial practice has revealed the fact that these electronic auctions are increasingly used, being a suitable tool to prevent expenses related to the logistics of classic auctions, while ensuring, at the same time, more extensive publicity. The main problem that could arise with regard to the electronic auction refers to the ease with which the bidding company modifies the information, the recipient having no real control over it, for reasons related to the encryption of the information by the one who modifies essential aspects, such as the price. Thus, we see ourselves in the hypothesis where technology offers us both benefits and serious disadvantages, leading to litigations in which the court does not appreciate, most of the time, that there was an injury to the legitimate interests of the exercise of a right by the offeror, namely to modify its commercial proposal.[30]

The judicial practice of the Court of Justice of the European Union is much more varied from the perspective of e-business sides, since the role of this court is, in most cases, to interpret EU law and the compatibility of some internal provisions with certain normative acts of primary or secondary law, in the light of the astonishing evolution of some legal institutions, such as this one of the ways of organizing business in electronic parameters, with the help of technology.

In this sense, the CJEU was notified regarding the interpretation of art. 41 paragraph (1) and with article 4 point 25 of the Directive on payment services within the internal market, stating that the information sent by a payment service provider to the customer's e-mail box related to the internet-banking service constitutes information on a «durable medium», provided that the said email box allows the user of the payment services to store information that is addressed to him personally, so that it is accessible for later consultation for a period appropriate to the purposes of the said information. In addition, the said email box must allow

[28] Bucharest Court of Appeal, Civil Section VI, decision no. 2291/2018 of 16.11.2018, at the electronic address: http://www.rolii.ro/hotarari/5c3ff1dfe49009101100026e, accessed on 17.12.2023.

[29] M. Of. no. 390/23.05.2016.

[30] Bucharest Court of Appeal, Section VIII administrative and fiscal litigation, decision no. 1973 of 27.09.2010, at the online address: http://www.rolii.ro/hotarari/58ab48ade49009c43e001982, accessed on 17.12.2023.

identical reproduction of the stored information, thus preventing the payment service provider from accessing, modifying or deleting said information.

The conclusion was that an email box of the internet banking service can also constitute an appropriate channel for the transmission of information in the form of electronic documents, if the documents in question comply with the requirement of being a « durable medium' and if such a system encourages the user to store by electronic means and/or print those documents with the help of an easily accessible function.[31] This aspect is of particular relevance regarding the way in which the provider must fulfill its obligation to inform, representing an important means of communication with the contractual partner.

Next, remaining within the scope of the obligation to communicate and the ways to fulfill this obligation, the CJEU ruled in another decision, establishing that art. 6(1)(c) of the Consumer Rights Directive must be interpreted as meaning that, on the one hand, it precludes a national regulation such as that at issue in the main proceedings, which requires the trader, before concluding a contract with a consumer a distance or off-premises contract to provide his telephone number under any circumstances. On the other hand, the said provision does not imply an obligation on the trader to set up a telephone or fax line or to create a new electronic mail address to allow consumers to contact him and does not require that this number or the fax or email address, unless this trader already has the respective means of communication with consumers. Consequently, other ways of providing this information may be used.[32]

Comparative Law

In the digital age, the progress of the legal system is strongly influenced by the technological process, with particular emphasis on the impact brought by artificial intelligence in e-commerce. The transformations brought to the business world had a strong advance thanks to digital technologies, and legal authorities were obliged to adapt their legislative framework[33]. Personal data protection and privacy rules are an essential part of this change, given the significant increase in personal data and its variety in the online environment. As data privacy standards become increasingly essential and complex to be able to maintain consumer trust

[31] CJEU, Case C-375/15 BAWAG PSK Bank für Arbeit und Wirtschaft und Österreichische Postsparkasse AG v. Verein für Konsumenteninformation, ECLI:EU:C:2016:695, online at: https://curia.europa.eu/juris/document/document.jsf?text=e-banking&docid=183345 &pageIndex=0&doclang=RO&mode=req&dir=&occ=first&part=1&cid=6741376#ctx1, accessed on 19.12.2023.

[32] CJEU, C-649/17, Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV v Amazon EU Sàrl, ECLI:EU:C:2019:576, online at: https://curia.europa.eu/juris/document/ document.jsf?text =mesagerie%2Belectronic%25C4%2583&docid=216039&pageIndex=0&doclang=RO&mode= req&dir=&occ=first&part=1&cid=6742162#ctx1, accessed on 19.12.2023.

[33] H. Taherdoost, *Legal, Regulatory, and Ethical Considerations in E-Business, E-Business Essentials: Building a Successful Online Enterprise*, 2023, pp. 379-402.

in the digital environment, an analysis of how different jurisdictions approach this issue is essential[34].

The increasing use of smart contracts and blockchain technology in general raises significant questions in the field of comparative law, in addition to privacy regulations[35]. There is a need to examine how different jurisdictions identify and control smart contracts, as well as identify their potential security issues. It underlines the importance of the rapid adaptation of legal systems to new technological realities[36]. This fosters the creation of a sustainable environment for e-commerce innovation and development.

In this sense, as we will see, the business mechanism is increasingly present in most legislations around the world, favoring the development of the entrepreneurial environment through the use of technology. In this vein, leveraging the comparative method, we propose the analysis of some contemporary legal systems in order to formulate proposals for ferenda law.

For example, the USA is more and more familiar with e-business, an aspect that is easy to observe by the fact that many businesses, regardless of the object of activity, prefer a self-service system[37], in other words a kind of business in which the customer ends up interacting with the electronic platform, and not with an employee, a method by which he requests a certain product or service, then the platform transmits the order to an employee, which can substantially influence the perspective of resources human resources in a business, which can, on the other hand, lead to a high level of unemployment.

In the UK, the pace of e-business development seems to be just as fast, as there are also plenty of strategies and techniques that directly or indirectly appeal to such a system, such as those based on substitution theory of the products, which presupposes, more precisely, that an attempt is made, as far as possible, to replace some products offered by some businesses that require the involvement of the human factor with ones that can be made by AI, in such a way that the consumer does not perceive an essential reconfiguration of the idea behind the business, thus operating a digitization of the result of the production process. This aspect may initially cause a change in the price of the product, since the quality will not be the same, but in time, the idea will be very profitable, since everything will run much easier, and some costs will no longer exist[38].

At the same time, there was the EDI system, Electronic Data Interchange, an e-marketplace between supply chain partners, which, due to the excessive costs

[34] *Ibidem.*

[35] *Idem.*

[36] *Idem.*

[37] W. Currie, *Value creation from e-business models*, Elsevier, Oxford, 2004, p. 175.

[38] T. Jelassi, A. Enders, F. J. Martínez-López, *Strategies for e-Business. Creating value through electronic and mobile commerce*, Pearson, Edinburgh, 2014, p. 59.

for implementation in most businesses, was abolished, with other systems taking its place, but using the same algorithms[39].

Artificial intelligence has become increasingly popular in modern society, being used successfully in a multitude of fields from health to transport, while raising concerns about the protection of personal data, as AI algorithms can easily collect and process large amounts of personal data[40].

Conclusions

In conclusion, the changes in legal systems in the digital age, which focus on the integration of artificial intelligence in the field of e-business, present both challenges and opportunities. The use of algorithms and legal assistance systems based on artificial intelligence improves the efficiency of processes, facilitates access to information, and reduces the costs associated with legal activities on the Internet. However, this transformation presents major challenges, such as ensuring data protection and privacy and adapting traditional law to digital changes.

As technology continues to develop, it is essential to develop appropriate legal frameworks to address these issues and create a fair and secure online business environment. To create innovative solutions and adapt legislation to technological developments, legislators, policymakers, and legal professionals must work together.

Finally, an essential step towards modernizing and streamlining procedures is the integration of artificial intelligence in the legal field of e-business. However, a balanced approach is needed to ensure that the fundamental principles of justice and the protection of individual rights are respected in this new digital age of business.

References

Chen L., Holsapple C.W., *E-business adoption research: state of the art, Journal of Electronic Commerce Research*, *14*(3), 2013, p. 261.

Ileana M., Oproiu M.I., Marian C.V., *E-commerce solutions using distributed web systems with microservices-based architecture for high-performance online stores*, 2024 47th MIPRO ICT and Electronics Convention (MIPRO), IEEE, May 2024, pp. 994-999.

Xu M., David J.M., Kim S.H., *The fourth industrial revolution: Opportunities and challenges. International Journal of Financial Research*, *9*(2), 2018, pp. 90-95.

Dwivedi Y.K., Hughes L., Ismagilova E., Aarts G., Coombs C., Crick T., Williams M.D., *Artificial Intelligence (AI): Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. International Journal of Information Management*, *57*, 2021, p. 101.

Makridakis S., *The forthcoming Artificial Intelligence (AI) revolution: Its impact on society and firms. Futures*, *90*, 2017, pp. 46-60.

[39] C. Combe, *Introduction to e-business. Management and strategy*, Elsevier, Oxford, 2006, p. 35.

[40] E. Sârghi, M. Ileana, *Protection of personal data within platforms developed in the context of artificial intelligence from the perspective of national and European law*, The Annals of “Dunarea de Jos” University of Galati. Legal Sciences. Fascicle XXVI, 2024; 7(1).

Soni N., Sharma E.K., Singh N., Kapoor A., *Artificial intelligence in business: from research and innovation to market deployment. Procedia Computer Science*, *167*, 2020, pp. 2200-2210.

Brody N., *What is intelligence?, International Review of Psychiatry*, *11*(1), 1999, pp. 19-25.

Weber F.D., Schütte R., *State-of-the-art and adoption of artificial intelligence in retailing. Digital Policy, Regulation and Governance,* 21(3), 2019, pp. 264-279.

Huang M.H., Rust R.T., *Artificial intelligence in service. Journal of service research*, *21*(2), 2018, pp. 155-172.

McCarthy J., *From here to human-level AI.* Artificial Intelligence, 171(18), 2007, pp. 1174-1182.

Rusoaie M., *E-business models in Romania,* dissertation work, Polytechnic University of Timișoara, 2008.

Forrest K.B., *Being "Human" in the Age of Artificial Intelligence. Ct. Rev.*, *59*, 2023, p. 4.

Bock D.E., Wolter J.S., Ferrell O.C., *Artificial intelligence: disrupting what we know about services. Journal of Services Marketing*, *34*(3), 2020, pp. 317-334.

Attard-Frost B., De los Ríos A., Walters D.R., *The ethics of AI business practices: a review of 47 AI ethics guidelines. AI and Ethics*, *3*(2), 2023, pp. 389-406.

Taherdoost H., *Legal, Regulatory, and Ethical Considerations in E-Business, E-Business Essentials: Building a Successful Online Enterprise*, 2023, pp. 379-402.

Currie W., *Value creation from e-business models*, Elsevier, Oxford, 2004.

Jelassi T., Enders A., Martínez-López, F. J. *Strategies for e-Business. Creating value through electronic and mobile commerce*, Pearson, Edinburgh, 2014.

Combe C., *Introduction to e-business. Management and strategy*, Elsevier, Oxford, 2006.

Sârghi E., Ileana M., *Protection of personal data within platforms developed in the context of artificial intelligence from the perspective of national and European law*, The Annals of “Dunarea de Jos” University of Galați. Legal Sciences. Fascicle XXVI, 2024; 7(1).

ANALELE ŞTIINŢIFICE ALE UNIVERSITĂŢII „ALEXANDRU IOAN CUZA" DIN IAŞI
TOM LXX, 2, ŞTIINŢE JURIDICE, 2024

DOI: 10.47743/jss-2024-70-2-5

AI Use in the Workplace. Some Legal Risks and Challenges

Dana VOLOSEVICI[1]

Abstract: As Artificial Intelligence (AI) advances, businesses benefit from its ability to exponentially enhance process effectiveness and efficiency, while also facing risks related to personal data protection, human dignity, and ultimately, human identity. This article aims to investigate two domains where AI is frequently employed in labor relations: recruitment and employee monitoring. In these areas, the article seeks to discuss aspects that could help clarify the conditions for the legitimate use of AI. A potential application of the ECJ's SHUFA case solution in recruitment is proposed, while the case of Amazon France Logistique is analysed concerning AI-based employee monitoring.

Keywords: AI, monitoring, recruitment, GDPR, workplace

Introduction

AI's impact on the concept of labor and its content is profound, reshaping the nature of work, skill requirements, and employment dynamics. The integration of AI into various industries has led to automation of repetitive and routine tasks, enhancing efficiency and productivity. This shift often results in the reduction of manual jobs but simultaneously creates opportunities for new roles that focus on managing, developing, and improving AI technologies. Employees now need to adapt by acquiring new skills and competencies, particularly in digital literacy, data analysis, and AI-related fields[2]. AI also influences workplace dynamics by enhancing decision-making processes. Employees benefit from AI-driven insights and analytics, which help in making informed decisions quickly. This can lead to increased efficiency, job satisfaction and performance, as employees are empowered with tools that enhance their capabilities. However, this reliance on AI also raises concerns about data privacy, ethical considerations, and the potential for bias in AI algorithms, which employees and employers must manage carefully[3].

This article aims to analyze the use of AI for two important aspects of the employment relationship, namely recruitment and performance monitoring. Both processes are considered high-risk AI systems by the AI Act. As expressly provided

[1] Ploiești Petrol-Gaze University, Romania, e-mail: dana.volosevici@vplaw.ro

[2] F. Butera, G. De Michelis, *Intelligenza artificiale e lavoro, una rivoluzione governabile*, Marsilio Editori, 2024, p. 25.

[3] M. Airoldi, *Machine Habitus. Socilogia degli algoritmi*, Luiss University Press, 2024, p. 71.

by recital (57), AI systems used in employment and workers management, in particular for the recruitment and selection of persons and for monitoring or evaluation of persons in work-related contractual relationships, should also be classified as high- risk, since those systems may have an appreciable impact on future career prospects, livelihoods of those persons and workers' rights. Moreover, these two processes have a transdisciplinary content, because they intersect with multiple fields of expertise, blending insights from human resources, psychology, law, data science, and organizational behavior. As a consequence, they require a comprehensive understanding of human behavior, technological tools, applicable legal and organizational needs. As will be discussed in the subsequent sections, the legal approach, which aims primarily to protect the data subject, specifically the employee, imposes limitations on the implementation of certain practices that the industry seeks to adopt to enhance process efficiency, cost savings, and customer service improvements.

In recruitment and selection, psychological principles help in understanding candidate behavior and predicting job performance[4], while data science techniques enable the analysis of large applicant pools and the identification of the best matches through algorithms and predictive analytics. Organizational behavior insights ensure that selected candidates fit well with the company's culture and values. Law is intricately related to the recruitment process by establishing the legal framework within which hiring practices must operate. It ensures fairness and equality, prohibiting discrimination based on race, gender, age, or other protected characteristics. Employment laws regulate the use of personal data during recruitment, ensuring privacy and consent. Legal standards also dictate the terms of job postings, interview processes, and employment contracts, protecting both employers and potential employees.

Performance monitoring similarly integrates various disciplines. Data science and analytics are essential for processing performance metrics and providing actionable insights. Psychological theories aid in understanding employee motivation and engagement, crucial for designing effective performance management systems. Organizational behavior principles help in creating feedback mechanisms and development plans that align with the overall goals of the company. Law is crucial to the performance monitoring process as it ensures that employee evaluations are conducted fairly and ethically. Legal frameworks protect employee rights, mandating that performance data is collected and used without discrimination or bias. Privacy laws regulate how employee information is gathered, stored, and shared, ensuring confidentiality and informed consent. Labor laws also outline acceptable practices for performance reviews, feedback, and disciplinary actions, preventing unjust treatment and fostering a transparent work environment.

[4] J. M. Conte, F.J. Landy, *Work in the 21st Century. An introduction to Industrial and Organizational Psychology* Sixth Edition, Wiley, 2018, p. 169.

The transdisciplinary nature of recruitment and performance monitoring processes can create complexities in applying legal provisions due to the interplay of the diverse fields. This integration demands a nuanced understanding of various disciplines, making it challenging to ensure legal compliance uniformly. For instance, psychological assessments used in recruitment must be designed to avoid biases and adhere to anti-discrimination laws. However, integrating these assessments with data-driven tools like AI algorithms introduces additional layers of complexity. Ensuring that these algorithms are free from bias and do not inadvertently discriminate against protected groups requires continuous monitoring and legal oversight, which can be technically challenging and resource-intensive. Similarly, in performance monitoring, the use of advanced analytics and data science techniques must comply with privacy laws, ensuring that employee data is collected and processed transparently and with consent. Balancing the need for detailed performance insights with legal requirements for data protection can be difficult, especially as technologies evolve rapidly.

1. Some legal considerations regarding the use of AI in recruitment

The use of AI in recruitment has garnered significant academic attention, particularly concerning the legal implications. The literature also points to the necessity of interdisciplinary approaches, as legal scholars collaborate with data scientists and ethicists to develop comprehensive regulatory frameworks that address the multifaceted challenges posed by AI in recruitment. Moreover, the research papers underscore the importance of stringent legal oversight and the development of transparent, fair, and accountable AI systems to ensure that the benefits of AI in recruitment are realized without compromising legal and ethical standards.

Scholars such as Binns[5] and Leicht-Deobald et al.[6] emphasize the necessity for transparent AI systems to prevent discrimination and ensure fairness in hiring practices. These studies highlight the potential for AI to perpetuate biases if not properly monitored, raising significant legal challenges under employment discrimination laws. Barocas and Selbst[7] argue that the opacity of AI algorithms can obscure biased decision-making processes, making it difficult to identify and

[5] R. Binns, *Fairness in Machine Learning: Lessons from Political Philosophy*, Proceedings of the 2018 Conference on Fairness, Accountability, and Transparency, pp. 149-159. https://doi.org/10.1145/3287560.3287581.

[6] U. Leicht-Deobald, T. Busch, C. Schank, A. Weibel, S.D. Schafheitle, I. Wildhaber, G. Kasper, *The Challenges of Algorithm-Based HR Decision-Making for Personal Integrity*, Journal of Business Ethics, no. 160, 2019, pp. 377-392, https://doi.org/10.1007/s10551-019-04204-w.

[7] S. Barocas, A.D. Selbst, A. D., *Big Data's Disparate Impact*, California Law Review, no. 104**,** 2016, pp. 671-732, https://doi.org/10.15779/Z38BG31.

address discriminatory practices. Dastin[8] underscores the need for compliance with data protection regulations, particularly with regard to the General Data Protection Regulation (GDPR). Thus, the data subject has the right to be informed in a „concise, transparent, intelligible and easily accessible form, using clear and plain language" (Article 12 (1), about how his data is collected, processed, and used, including about „the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject" (Article 13 (2) f). Employees and candidates can request access to their personal data and obtain details about the logic behind AI-driven decisions that significantly affect them (Article 15 (1) h). They also have the right to rectify inaccuracies in their data (Article 16) and to object to automated decisions, demanding human intervention in certain cases (Article 18).

Further, Raghavan *et al.*[9] explore the impact of AI on privacy rights, emphasizing the importance of consent and transparency in data collection. Their research suggests that AI tools often collect extensive personal data, necessitating robust legal frameworks to protect candidates' privacy. The work of Kim[10] delves into the ethical and legal ramifications of using predictive analytics in recruitment, arguing that the predictive nature of AI can lead to preemptive discrimination against certain demographic groups, challenging existing anti-discrimination laws. Ajunwa, Crawford, and Schultz[11] discuss the implications of the Americans with Disabilities Act (ADA) in the context of AI, noting that automated systems must be designed to accommodate individuals with disabilities, ensuring accessibility and fairness. Additionally, scholars like Edwards and Veale[12] highlight the need for accountability in AI systems, suggesting that the lack of clear responsibility can complicate legal recourse for affected individuals.

Another aspect worth analyzing is the legal applicability in recruitment of the Article 22 of the GDPR, which states that „the data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly

[8] J. Dastin, *Amazon Scraps Secret AI Recruiting Tool That Showed Bias Against Women*, Reuters, 2018 [online] at https://www.reuters.com/article/us-amazon-com-jobs-automation-insight-idUSKCN1MK08G, accessed on 10.06.2024.

[9] M. Raghavan, S. Barocas, J. Kleinberg, K. Levy, *Mitigating Bias in Algorithmic Hiring: Evaluating Claims and Practices*. Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency, 2020, pp. 469-481, https://doi.org/10.1145/3287 560.3287587.

[10] P.T. Kim, *Data-Driven Discrimination at Work*, William & Mary Law Review, no. 58, 2017, pp. 857-936, https://scholarship.law.wm.edu/wmlr/vol58/iss3/5.

[11] I. Ajunwa, K. Crawford, J. Schultz, *Limitless Worker Surveillance*, California Law Review, no. 105, 2017, pp. 735-776. https://doi.org/10.15779/Z38BR8MF94.

[12] L. Edwards, M. Veale, *Slave to the Algorithm? Why a 'Right to an Explanation' is Probably Not the Remedy You Are Looking For*, Duke Law & Technology Review, no. 16, 2017, pp. 18-84, https://doi.org/10.2139/ssrn.2972855.

significantly affects him or her." In this context, we aim to examine how SCHUFA ECJ ruling[13] on automated processing, particularly in relation to a credit scoring system, could provide guidelines for data processing in the recruitment process.

SCHUFA, a private German company, provides its contractual partners with information on the creditworthiness of third parties, especially consumers. It creates a „score” predicting future behavior, like loan repayment, based on certain personal characteristics using mathematical and statistical methods. The scoring process assumes that by grouping individuals with similar characteristics, future behavior can be predicted. OQ was denied a loan by a third party due to negative information from SCHUFA. She requested SCHUFA to provide her personal data and to erase allegedly incorrect data. SCHUFA informed OQ of her score and generally described the scoring methods but, citing trade secrecy, refused to disclose specific elements and their weightings used in the calculation. SCHUFA maintained that it only provides information to its partners, who make the actual contractual decisions. OQ filed a complaint with HBDI, the competent supervisory authority, on October 18, 2018, requesting that SCHUFA grant her access to information and erase the incorrect data. On June 3, 2020, HBDI rejected her complaint, stating that it was not proven that SCHUFA failed to comply with Article 31 of the BDSG regarding its activities. OQ appealed this decision to the Verwaltungsgericht Wiesbaden (Administrative Court, Wiesbaden, Germany).

In response to Verwaltungsgericht Wiesbaden question, the ECJ ruled that „Article 22(1) of GDPR „must be interpreted as meaning that the automated establishment, by a credit information agency, of a probability value based on personal data relating to a person and concerning his or her ability to meet payment commitments in the future constitutes ‘automated individual decision-making’ within the meaning of that provision, where a third party, to which that probability value is transmitted, draws strongly on that probability value to establish, implement or terminate a contractual relationship with that person.”

In its reasoning, the ECJ clarified that for Article 22(1) to be applicable, three cumulative conditions must be met., Firstly, there must be a 'decision.' Secondly, that decision must be 'based solely on automated processing, including profiling’. Thirdly, that it must produce ‘legal effects concerning [the interested party]’ or ‘similarly significantly [affect] him or her’[14].

Regarding the concept of a decision, the Court clarified that this refers not only to acts that produce legal effects concerning the individual but also to acts that similarly significantly affect him or her. To support this interpretation, reference was made to recital 71 of the GDPR, which explicitly mentions the „automatic refusal of an online credit application or e-recruiting practices without any human intervention.” According to Advocate General Pikamäe, in the case under consideration, the decision process included several phases, such as

[13] ECJ, Judgment of 7 December 2023, Case C-634/21, SCHUFA Holding, ECLI:EU:C:2023:957.

[14] *Ibidem*, 43.

profiling, the establishment of the score, and the actual decision on the grant of credit[15].

Additionally, the Advocate General noted that the possibility of assigning certain powers to an external service provider does not seem to play a crucial role in the analysis regarding the application of the rules under Article 22(1). What is important is that the result of the analysis conducted by SCHUFA was almost automatically adopted by the credit institution. Thus, according to the referring court, even though human intervention was still possible at that stage of the decision-making process, the decision to enter into a contractual relationship with the data subject was practically determined by the score transmitted by credit agencies to such a considerable extent that the score heavily influenced the third-party controller's decision. Consequently, the score itself must be regarded as having the status of a ‘decision’ within the meaning of Article 22(1) of the GDPR.

Returning to the issue of recruitment, it is a common practice for companies to collaborate with external recruitment providers to leverage specialized expertise, access a broader talent pool, and streamline the hiring process. External contractors possess deep industry knowledge, extensive networks, and advanced tools for candidate sourcing and evaluation, which can result in higher quality hires and reduced time-to-fill positions. When external recruitment contractors use AI for candidate profiling, they use advanced algorithms to analyze vast amounts of data to predict candidate suitability for specific roles. This technology can analyze various factors, such as work history, education, skills, and even social media activity, to create comprehensive candidate profiles. As long as the GDPR provisions regarding data minimization, candidate notification, and the granting of legally recognized rights are adhered to, the use of algorithms cannot be considered inherently unlawful. The issue arises when the data subject, specifically the candidate, believes they have been harmed by how their profile was established, either through a discretionary action of the algorithmic analysis or by the omission of relevant information. In such instances, similar to the SCHUFA case, it must be determined whether the external consultant can be required to provide the candidate with information about the various elements considered in the calculation and their respective weightings.

Given that the matter concerns the conclusion or non-conclusion of an employment contract, it is evident that the outcome of the analysis produces "legal effects concerning him or her" or "similarly significantly affects him or her." The impact of the score determined by the recruitment firm through AI technology is more significant with the prominence of the recruitment firm. Although the company requesting the recruitment services could theoretically disregard the score provided by the recruiter, it will most likely be significantly influenced by it. As highlighted by the ECJ, it is the responsibility of national courts to determine,

[15] ECJ, Opinion Of Advocate General Pikamäe, delivered on 16 March 2023, Case C-634/21, SCHUFA Holding, ECLI:EU:C:2023:220.

in each case, the contextual framework and the extent of the recruitment firm's influence on the hiring company.

Consequently, recruitment contractors utilizing AI must ensure transparency in their data handling practices and provide candidates with the opportunity to understand and challenge decisions made by AI systems. To substantiate this right, candidates must be informed about how their data is being used, that the data will be processed not by the prospective employer but by a third party, including through the use of AI and that this process involves generating profiles and scores that will be transmitted to the prospective employer.

2. Legal risk related to the use of AI in monitoring the employee activity

The use of AI in monitoring employee activity involves sophisticated algorithms that analyze vast amounts of data to evaluate performance, productivity, and compliance with company policies. AI systems can track various aspects such as computer usage, communication patterns, and even biometric data to provide detailed insights into employee behavior. Monitoring methods are multiple and continuously developing. Some of the tools help employers monitor real-time activity. For example, Toggl and RescueTime use AI to automatically track the time employees spend on different tasks and applications, providing detailed productivity reports. Platforms such as Hubstaff and Teramind offer extensive features including screen capture, keystroke logging, and application usage tracking. Some other tools like ActivTrak use AI to analyze behavioral patterns, identifying trends and anomalies in employee performance. Devices like smartwatches and fitness trackers can monitor physical activity, stress levels, and overall well-being, providing employers with insights into employee health and productivity. Platforms like Microsoft Teams and Slack have integrated analytics that track communication patterns and collaboration metrics, helping managers understand team dynamics and efficiency. With the rise of remote work, tools like Time Doctor and Hubstaff offer features specifically designed to monitor remote employees, including GPS tracking, activity levels, and project management integration.

While enhancing the ability to monitor and improve employee productivity, these tools raise significant privacy and ethical considerations, as they constitute continuous monitoring. As noted in WP 29 Opinion on data protection at work, if there are no limits to the processing, and if it is not transparent, there is a high risk that the legitimate interest of employers in the improvement of efficiency and the protection of company assets turns into unjustifiable and intrusive monitoring"[16].

One recent example of exceeding the limits of an employer's right to monitor employee activity is the case of Amazon Logistique France, which received

[16] Article 29 Data Protection Working Party, Opinion 2/2017 on data processing at work, Adopted on 8 June 2017, p. 9.

a fine of 32 million euros from the French Supervisory Authority, the CNIL. Amazon France manages extensive warehouses in France, handling the reception, storage, and preparation of items for customer delivery. Employees in these warehouses are equipped with scanners to document the real-time performance of tasks such as shelving or packing items. Each scan generates data recorded and used to calculate indicators on the quality, productivity, and periods of inactivity of each employee. Following media reports on the company's practices, the French Supervisory Authority (SA) conducted multiple investigations and received several complaints from employees.

The analysis of data obtained from employees aimed to align with research in industrial practices. Access to such data allows managers to identify and address issues as they arise. Moreover, real-time performance monitoring provides immediate feedback, motivating employees to improve their productivity and efficiency. In „The Second Machine Age," MIT's Erik Brynjolfsson and Andrew McAfee[17] demonstrate that data-driven decision-making can lead to substantial productivity gains by enabling companies to adapt swiftly to changing conditions. The issue, therefore, is determining whether there are limits to such monitoring and, if so, what elements must be considered to establish those limits.

The CNIL did not question the need for ensuring a company's competitiveness, which justified Amazon's scanner system to manage its operations. Thus, the practice of electronically monitoring employees and using the obtained data for industrial purposes was validated. However, the French Supervisory Authority noted that the retention of all this data and the resulting statistical indicators was disproportionate. The system for measuring the speed at which items were scanned was found excessive. This system operated on the principle that items scanned very quickly increased the risk of error, leading to the establishment of an indicator to measure whether an item had been scanned in less than 1.25 seconds after the previous one. Consequently, employee behaviour was monitored every 1.25 seconds.

Such monitoring, which involved the use of scanners, differed from traditional activity monitoring methods due to its scale, exhaustiveness, and permanence, leading to very close and detailed scrutiny of employees' work. The permanent monitoring of employees, encompassing the entire spectrum of their activities throughout the workday, was considered abusive because it placed employees under continuous pressure. The Article 29 Working Party (WP29) noted as early as 2017 that monitoring communications and behavior pressures employees to conform to prevent the detection of perceived anomalies, similar to how intensive CCTV use has influenced citizen behavior in public spaces[18]. The CNIL further deemed it excessive to retain all data collected by the system and the resulting statistical indicators for all employees and temporary workers for 31 days.

[17] E. Brynjolfsson, A. McAfee, *The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies, 2014,* W.W. Norton & Company.

[18] Article 29 Data Protection Working Party, Opinion 2/2017 on data processing at work, Adopted on 8 June 2017.

Amazon France responded[19] that the use of warehouse management systems is a common practice in the industry, being necessary to ensure the safety, quality, and efficiency of operations, as well as to track inventory and process parcels in a timely manner and in accordance with customer expectations. The three indicators either signal a risk of error when an employee scans an item in less than 1.25 seconds after scanning a previous item (the "Stow Machine Gun" indicator), periods of scanner inactivity of ten minutes or more (the "idle time" indicator), or scanner interruptions between one and ten minutes (the "latency under ten minutes" indicator). It is proven[20] that, by integrating various functions such as inventory control, order fulfilment, and shipping logistics, warehouse management systems enhance operational efficiency and reduce errors. They provide real-time visibility into inventory levels, locations, and movement, enabling better decision-making and resource allocation. However, industrial practices, even if proven to be efficient, must pass the test of legality, including those related to data minimization (Art. 5(1)(c)) and lawful processing (Art. 6 of GDPR).

The considerations of the CNIL's decision can contribute to shaping industrial practices that avoid abuses, even when these practices are based on seemingly neutral technical aspects, such as the need for data analysis to optimize production. Thus, without denying the potential importance of providing assistance to an employee or reassigning them in real time within the industrial process, the CNIL ruled that this does not necessitate access to every detail of the employee's quality and productivity indicators collected over the last month using scanners. The supervisory authority expressed the opinion that, in addition to real-time data, a selection of aggregated data, on a weekly basis, for example, would be sufficient.

We are therefore at a juncture where a just balance must be found between the industry's tendency to generate safety and progress through the use of AI and the employees' right to perform their work in conditions that do not constitute continuous pressure on them. The trend of measuring employees' activity down to the smallest gesture could hinder the natural development of human personality and the specific axiological characteristics of human beings.

3. Employee involvement for a legitimate AI use

The employment contract is characterized by an inherent imbalance of power between the parties, with the employee performing their duties under the authority of the employer. According to Article 40(1)(a) and (d) of the Labor Code,

[19] Déclaration d'Amazon à propos de la décision de la CNIL, https://www.aboutamazon.fr/actualites/politiques-publiques/declaration-damazon-a-propos-de-la-decision-de-la-cnil.

[20] L. N. Tikwayo, T. N. D. Mathaba, *Applications of Industry 4.0 Technologies in Warehouse Management: A Systematic Literature Review*, Logistics 2023, no. 7, 24. https://doi.org/10.3390/ logistics7020024.

the employer is granted the right to determine the organization and functioning of the unit and to exercise control over how job responsibilities are fulfilled. Even prior to the formalization of an employment contract, employers possess the authority to conduct comprehensive analyses of prospective employees' personal data. This practice involves the use of automated data processing techniques, including profiling, either directly by the employer or through an authorized agent. The exercise of such powers is subject to stringent legal and ethical scrutiny, given the potential for significant intrusion into personal privacy. Throughout the tenure of the employment relationship, employers may implement various monitoring mechanisms to oversee employee performance and compliance with job responsibilities. The degree of intrusiveness associated with these monitoring activities can vary significantly. Key factors influencing this include the specific technological tools employed, the scope and nature of these instruments, and the extent of data processed. Advanced technologies such as artificial intelligence and video surveillance can offer detailed insights into employee activities, raising important considerations regarding data protection and privacy rights under applicable legal frameworks. Employers must balance the legitimate business interests in monitoring and maintaining workplace efficiency with the necessity of safeguarding employees' privacy and personal data. Compliance with data protection regulations, such as the GDPR, is imperative to ensure that monitoring practices do not disproportionately infringe on employees' rights.

Beyond the actions of employers, employees, through unions or employee representatives, must play a proactive role in promoting their own rights. For instance, Romanian law[21] stipulates that when electronic communication systems or video surveillance are used in the workplace for monitoring purposes, the processing of employees' personal data to achieve the legitimate interests pursued by the employer is permitted only if the following cumulative conditions are met. First, the employer's legitimate interests must be thoroughly justified and outweigh the interests, rights, or freedoms of the individuals concerned. Additionally, the employer must provide mandatory, complete, and explicit prior information to the employees. Before introducing monitoring systems, the employer must consult with the union or, where applicable, employee representatives. It is also necessary that other less intrusive means and methods to achieve the employer's intended purpose have previously proven ineffective. Lastly, the duration of personal data storage must be proportional to the purpose of the processing and not exceed 30 days, unless expressly regulated by law or justified by specific situations.

[21] Law no. 190/2018 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 with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), published in the Official Gazette no. 651 of 26 July 2018.

According to the Social Dialogue Law[22], consultation entails the exchange of opinions and information and the establishment of a dialogue between social partners (article 1, 2. b). This process ensures that both parties - employers and trade unions or employee representatives - can contribute to decision-making processes, particularly those affecting working conditions and employee rights. Therefore, unions or, where applicable, employee representatives are entitled to access the information and studies that formed the basis for implementing monitoring measures. They have the right to request further details and to articulate their stance on the introduction of such measures. This involvement ensures transparency and accountability in the decision-making process, allowing employees' interests to be considered and safeguarded. If individual employees and candidates might find it challenging to protect their rights[23], unions can play a crucial role in this regard. Through the consultation procedure and collective bargaining[24], unions can help establish a framework that ensures real protection of employees' rights, particularly concerning the use of AI in employment relationships. Unions can advocate and bargain for transparency, fairness, and accountability in AI-driven processes[25], ensuring that these technologies are used in ways that respect and uphold workers' rights. This collective approach is essential in balancing technological advancements with the need for equitable treatment in the workplace. In this regard, trade unions in several European countries have begun incorporating AI-related issues into collective bargaining agreements. For instance, under a recent agreement concluded by the government and the social partners in Spain, „digital platforms will have to make available to trade unions an algorithm, or any artificial intelligence of sorts, which may have an impact on such conditions – including individuals' access to, and maintenance of, employment and their profiling. This right to information is granted to everyone working through a platform [...] and thus the transparency requirement applies to all digital platforms equally"[26]. At European level, the European social partners agreed on a programme on European social dialogue which addresses the challenges of the extensive increase in the use of digital tools at the workplace and decided to „create the space for exchanging views on these trends and the relevance

[22] Law. no. 367/2022 on Social Dialogue, published in the Official Gazette no. 1238 of 26 December 2022.

[23] A. Aloisi, V. De Stefano, *Your Boss is an Algorithm. Artificial Intelligence, Platform Work and Labour*, Oxford Hart Publishing, 2022.

[24] A. Aloisi, E. Gramano, *Artificial intelligence is watching you at work: Digital surveillance, employee monitoring, and regulatory issues in the EU context*, Comparative Labor Law & Policy Journal no. 41(1), 2019, pp. 95–122.

[25] V. De Stefano, *'Masters and servers': Collective labour rights and private government in the contemporary world of work,* International Journal of Comparative Labour Law and Industrial Relations no. 36(4), 2020, pp. 435–443.

[26] A. Aranguiz, *Spain's platform workers win algorithm transparency*, Social Europe, 2021, [Online] at https:// www.socialeurope.eu/spains-platform-workers-win-algorithm-transparency, accessed on 10.06.2024.

this has for social partners and collective bargaining at all appropriate levels across Europe"[27]. Moreover, in the matter of employment, the Article 88 of GDPR itself recognizes the role of collective bargaining, alongside that of the law to provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees' personal data in the employment context, in particular for the purposes of the recruitment, the performance of the contract of employment, including [...] management and planning and organization of work.

Conclusion

The utilization of AI in society, particularly within the realm of labour relations, presents not only a legal challenge but also a significant moral dilemma in the current stage of societal development. While technological advancements captivate by breaking barriers in critical life domains, they simultaneously compel us to identify and preserve those quintessential human attributes that should remain beyond the reach of non-human entities. In labour relations, sophisticated tools have already been implemented to deeply measure various aspects of human behaviour and performance. This includes both the profiling of job candidates and the ongoing, comprehensive monitoring of employees. Such practices place workers under continuous scrutiny, thereby eroding their privacy and encroaching upon their private behavioural and even physiological traits. To mitigate potential abuses, a synergistic approach is essential, involving legal frameworks, judicial oversight, supervisory authorities, unions, and professional organizations. The objective is not to resist technological progress but to shape the future in accordance with values that universally define human dignity and integrity. By addressing these challenges through a concerted effort, we can ensure that the integration of AI into the workplace enhances rather than diminishes the human experience, safeguarding fundamental rights while embracing technological innovation.

Referencess

Airoldi M., *Machine Habitus. Socilogia degli algoritmi*, Luiss University Press, 2024, p. 71.

Ajunwa I., Crawford K., Schultz J., *Limitless Worker Surveillance*, California Law Review, no. 105, 2017, pp. 735-776. https://doi.org/10.15779/Z38BR8MF94.

Aloisi A., De Stefano V., *Your Boss is an Algorithm. Artificial Intelligence, Platform Work and Labour*, Oxford Hart Publishing, 2022.

Aloisi A., Gramano E., *Artificial intelligence is watching you at work: Digital surveillance, employee monitoring, and regulatory issues in the EU context*, Comparative Labor Law & Policy Journal no. 41(1), 2019, pp. 95–122.

Aranguiz A., *Spain's platform workers win algorithm transparency*, Social Europe, 2021, [online]

Barocas S., Selbst, A. D., *Big Data's Disparate Impact*, California Law Review, no. 104, 2016, pp. 671-732, https://doi.org/10.15779/Z38BG31.

[27] European Social Dialogue, Work Programme 2022-2024, [Online] at https://www.businesseurope.eu/sites/buseur/files/media/reports_and_studies/2022-06-28_european_social_dialogue_programme_22-24_0.pdf, accessed on 10.06.2024.

Binns R., *Fairness in Machine Learning: Lessons from Political Philosophy*, Proceedings of the 2018 Conference on Fairness, Accountability, and Transparency, pp. 149-159. https://doi.org/10.1145/3287560.3287581.

Brynjolfsson E., McAfee A., *The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies, 2014,* W.W. Norton & Company.

Butera F., De Michelis G., *Intelligenza artificiale e lavoro, una rivoluzione governabile*, Marsilio Editori, 2024, p.25.

Conte J. M., Landy F.J., *Work in the 21st Century. An introduction to Industrial and Organizational Psychology* Sixth Edition, Wiley, 2018, p. 169.

Dastin J., *Amazon Scraps Secret AI Recruiting Tool That Showed Bias Against Women*, Reuters, 2018 [online]

Edwards L., Veale M., *Slave to the Algorithm? Why a 'Right to an Explanation' is Probably Not the Remedy You Are Looking For*, Duke Law & Technology Review, no. 16, 2017, pp. 18-84, https://doi.org/10.2139/ssrn.2972855.

European Social Dialogue, Work Programme 2022-2024, [online]

Kim P.T., *Data-Driven Discrimination at Work*, William & Mary Law Review, no. 58, 2017, pp. 857-936.

Leicht-Deobald U., Busch T., Schank C., Weibel A., Schafheitle S. D., Wildhaber I., Kasper G., *The Challenges of Algorithm-Based HR Decision-Making for Personal Integrity*, Journal of Business Ethics, no. 160, 2019, pp. 377-392, https://doi.org/10.1007/s10551-019-04204-w.

Raghavan M., Barocas S., Kleinberg J., Levy K., *Mitigating Bias in Algorithmic Hiring: Evaluating Claims and Practices.* Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency, 2020, pp. 469-481, https://doi.org/ 10.1145/3287560.3287587.

De Stefano V., ‘*Masters and servers’: Collective labour rights and private government in the contemporary world of work,* International Journal of Comparative Labour Law and Industrial Relations no. 36(4), 2020, pp. 435–443.

Tikwayo, L. N., Mathaba T. N. D., *Applications of Industry 4.0 Technologies in Warehouse Management: A Systematic Literature Review*, Logistics 2023, no. 7, 24. https://doi.org/10.3390/ logistics7020024.

Analele Ştiinţifice ale Universităţii „Alexandru Ioan Cuza” din Iaşi
TOM LXX, 2, Ştiinţe Juridice, 2024

DOI: 10.47743/jss-2024-70-2-6

Digitalizarea pieței imobiliare și a notariatului prin tehnologia *blockchain*

The Digitalization of the Real-estate Market and the Civil Law Notary Using *Blockchain* Technology

Răzvan ANTOHIE[1]

Rezumat: Ne pregătim cu toţii de revoluția tehnologică. Niciodată în istoria sa, omul nu a fost mai afectat de schimbările extrem de rapide care se întâmplă în jurul său. Dintre acestea, tehnologia blockchain pare a avea cel mai mare impact, fiind asemănată, nu de puține ori, cu efervescența pe care am cunoscut-o cu toții atunci când a apărut internetul. Însă spre deosebire de internet, blockchain ne afectează viețile mult mai vizibil. Nu ne oferă doar acces la informații, ci și posibilitatea de a realiza operațiuni care până acum durau mult mai mult, precum plăți, sau comenzi de produse, în doar 10 secunde, totul fiind, așa cum se spune, „la un click distanță”. Notariatul reprezintă una dintre cele mai vechi meserii juridice. Principiile sale sunt cele care au stat la baza dreptului roman însuși, iar aceste principii și nevoi sociale sunt cele care au asigurat existența meseriei secole la rândul. Însă ne punem firesc întrebarea: În noul context digital, își mai are loc notarul? Mai ales luând în considerare că necesitățile sociale la care acesta răspunde încep să fie preluate încetul cu încetul de Inteligența Artificială. Prezentarea de față își propune să răspundă la această întrebare. Putem oare „sări” notarul atunci când încheiem un contract de vânzare a unui bun imobil? Cu alte cuvinte, putem înlocui actul autentic notarial cu ceea ce astăzi este numit smart contract?

Cuvinte cheie: imobiliar, notar, autentificare, *blockchain*, *smart contract*

Abstract: We are all preparing for the technological revolution. Never in his existence has humanity been affected so quickly by the changes around him. The blockhain technology stands out and seems to have the biggest impact; not once has blockchain been compared with the impact that the internet has had on us since its’ beginning. But, unlike the internet, blockchain seems to affect out lives much more visible. Not only does this new technology offer us access to information, but also gives us the possibility to realize operations that, until now, took us much more time, like payments or online shopping. The civil law notary is one of the oldest professions in the world; it’s existence can be traced to roman law. But in this new digital world, one must wonder: does this bureaucratic civil servants have a

[1] Notar public drd., Facultatea de Drept, Universitatea „Alexandru Ioan Cuza” din Iași, e-mail:razvan_antohie@yahoo.com.

place? Especially when Artificial Inteligence seems to fulfil the social needs that have been the backbone of the notarial profession since its' founding. This article will try to answer the question if the civil law notary, as we know him, can be skipped when purchasing a real estate asset? In other words, can the notarial act be replaced with what is today known as a smart contract?

Keywords: real estate, notary, authentication. blockchain, smart contract

Introducere

Termenul general de „imobiliar" acoperă o varietate de activități: de la administrarea la tranzacționarea bunurilor imobile, promovarea lor, inclusiv la domeniul construcțiilor de imobile (rezidențial, industrial, urbanism, garanții imobiliare etc.). Prezenta lucrare se referă prin urmare la „imobiliare" în sens larg, acoperind toate activitățile menționate anterior.

Imobiliarele reprezintă stâlpul economiei mondiale. Într-un studiu elaborat de firma de consultanță Savills, valoarea totală a pieței imobiliare globale din 2022 era de 379.900 miliarde de dolari, în condițiile în care Produsul Intern Brut Mondial[2] a fost de 100.135 miliarde de dolari[3]. Această statistică relevă faptul că valoarea totală a activelor imobiliare din lume este de trei ori și jumătate mai mare decât PIB-ul global, adică decât tot ceea ce se produce în lume (bunuri și servicii). Dintre acestea, 75,7% reprezintă active imobiliare sub forma investițiilor rezidențiale, 13,37% reprezintă imobiliare de natură comercială, iar 1,87 reprezenta valoarea terenului agricol. Dintre acestea, cele mai valoroase imobile se aflau în China (26%)-căreia îi corespundea 17,72% din populația lumii, Statele Unite ale Americii (19%)-căreia îi corespundea 4,23% din populația lumii, urmate de Japonia, Germania, Marea Britanie și Franța. Africa și Orientul Mijlociu, cărora le corespund 19% din populația globului, dețineau doar 6% din valorile imobiliare globale. Ca și termen de comparație, în 2016, valoarea totală a pieței imobiliare era de 204,250 miliarde de dolari, iar PIB-ul era de 66,828 miliarde de dolari[4].

Cu titlu de exemplu, în Franța, PIB-ul național a fost în 2018 de 2.353 miliarde de euro[5]. 313,8 miliarde de euro și 285,5 miliarde de euro din această valoare era reprezentată de activități în domeniul imobiliar, respectiv activități în domeniul construcțiilor care, împreună reprezentau 15% din producția națională totală, evaluată la valoarea de 4.029 miliarde de euro[6]. O parte greu de neglijat din economia națională. În sectorul imobiliar din Franța lucrează aproximativ 242.000 angajați, iar în domeniul construcțiilor, 1,7 milioane de angajați. Există 660.000 firme în domeniul construcțiilor și 221.000 în domeniul imobiliar, din totalul de

[2] https://www.savills.com/impacts/market-trends/the-total-value-of-global-real-estate-property-remains-the-worlds-biggest-store-of-wealth.html.

[3] https://www.statista.com/statistics/268750/global-gross-domestic-product-gdp/.

[4] HSBC&Savills World Research, *Global Real Estate, Trend în the worlds' largest asset class,* 2017.

[5] https://www.insee.fr/fr/statistiques/4272575.

[6] https://www.insee.fr/fr/statistiques/4272575.

5.086.000 de firme active (17,5%). Sectorul imobiliar și al construcțiilor contribuie cu 18,4% din PIB, reprezentând cel mai mare contributor la bugetul de stat din Hexagon[7].

Pe scurt, imobiliarele reprezintă unul dintre cele mai importante domenii ale economiei, deoarece sunt cele mai mari creatoare de plus-valoare din lume. În plus, este un sector în care, în timp, valoarea bunurilor crește în mod constant (deoarece de fiecare dată când un imobil este construit, el poate genera numeroase activități economice ulterioare precum tranzacții, închirieri, renovări, investiții etc.)

Cu toate acestea, în ciuda faptului că în ultimele decenii a fost și domeniul imobiliar afectat de digitalizare, este totuși caracterizat de un anumit arhaism, generând o serie de fricțiuni pe diferite niveluri în ceea ce privește tranzacțiile, investițiile, accesul la proprietate, administrarea, piața imobiliară în general. Tehnologia *blockchain* și-a adus și ea aportul la aceste fenomene.

1. Piața imobiliară și *blockchain*

Imobiliare reprezintă un sector recunoscut pentru rezistența la schimbări. Motivele sunt următoarele:

1. Produsele în această piață sunt atât de variabile, diferite ca preț și caracteristici (suprafață, locație etc.) încât este imposibilă o standardizare a imobiliarelor, un element comun care să le lege;

2. Un imobil reprezintă un bun de o valoare foarte mare, prin urmare acestea nu sunt tranzacționate în mod regulat și frecvent pe piața liberă. Cu puține excepții, persoanele nu tranzacționează în mod curent imobile, prin urmare nu sunt educate în ceea ce privește piața imobiliară și practicile ei;

3. Mare parte din tranzacțiile imobiliare se desfășoară prin intermediari, în special agenții imobiliare. Acești intermediari au tot interesul ca piața să fie cât mai opacă, deoarece le este frică de faptul că, prin apariția tehnologiei, importanța meseriei lor s-ar putea diminua.

Piața imobiliară din ultimii ani a trecut prin trei mari etape. Acestea sunt explicate într-un raport al Oxford Business School, iar fiecare dintre etape poartă denumirea de PropTech[8]. Înainte de 1985, imobiliare reprezentau o lume tradițională. Informațiile erau distribuite pe suport hârtie (planuri, documente, contracte etc.) din momentul proiectării, în timpul construcției, a tranzacționării bunului construit și ulterior, pentru întreținerea acestora. Abia după acest an, sectorul imobiliar a început să asimileze noile tehnologii. Astfel, aceste trei etape sunt:

Apariția calculatorului în anii 1940 nu a afectat prea mult domeniul imobiliar. Abia după 1985, când pe piața a apărut primul PC (*Personal Computer*),

[7] Statistici separate nu există în România, deoarece acestea plasează sectorul construcțiilor împreună cu cel al industriei, prin urmare nu se poate face o departajare exactă.

[8] A. Baum, *PropTech 3.0; The future of Real Estate,* Said Business School, Oxford University, 2017. Denumirea vine de la alăturarea cuvintelor *Proprety* și *Technologies,* la fel cum este și cazul FinTech și ConTech.

care permitea utilizatorului să lucreze pe foi de calcul și tabele (precum Excel), și în imobiliare au început să apară schimbări. Această primă revoluție tehnologică a beneficiat și de entuziasmul generat de apariția actorilor pe piața *dotcom*[9], care au direcționat investiții masive în multe proiecte de genul *start-up* (care ulterior au dus la apariția bulei economice cauzate de Internet de la începutul anilor 2000, ce au avut ca și cauza supraevaluarea la bursă a companiilor din acest domeniu).

Următoarea etapă în evoluția imobiliară este reprezentată de criza anilor 2007-2008, deoarece jucătorii din piață au început să caute noi metode de a-și eficientiza, sau cel puțin conserva rentabilitatea portofoliului imobiliar, astfel că au început să caute noi metode pentru a reduce costurile. Apariția tehnologiilor de genul *Cloud Computing*[10], combinate cu internetul care avea o viteză de funcționare din ce în ce mai mare au dus la apariția unor instrumente digitale sofisticate și multe mai ieftine, atât în ceea ce privește elaborarea unui proiect de construcție, spre exemplu, prin programe informatice de genul *Building Information Modeling,* sau BIM, cât și în ceea ce privește inspecția etapelor desfășurării acestuia (prin gestiunea de la distanță a proiectului cu ajutorul tehnologie de tipul *cloud*).

Pe de altă parte, apariția *Smartphone* a permis ca informația din domeniul imobiliar să ajungă la toată lume, în orice moment, instant și gratuit. Au început să apară pe piață noi actori în domeniu, precum Airbnb și WeWork care sunt exponenții celei de-a doua etape de PropTech. Această etapă a permis digitalizarea numeroaselor aspecte din sector, mai ales în ceea ce privește accesul la informații, o refuncționalizare a etapelor unui proiect imobiliar precum și noi metode de a reduce costurile din domeniu.

Boom-ul provocat de PropTech 2.0 a început să își piardă din elan începând cu anii 2014-2015, însă interesul pentru piața imobiliară a rămas constant, lucru dovedit și de faptul că cei mai mari jucători pe piața financiară continuau să investească în companii de genul start-up din acest sector[11].

[9] Ne referim la primii mari actori pe piața internetului, precum Google, Yahoo!, eBay, Amazon etc.

[10] Utilizarea unui server aflat la distanță pentru a stoca și distribui informații.

[11] Există mai multe modalități de finanțare a companiilor de genul start-up în lumea Tech. Obiectivul inițial a acestor companii este de a cuceri cât mai mult din piața internațională, cât mai repede de la înființare, printr-o creștere rapidă, care de cele mai multe ori se întâmplă în pierdere. Înainte de a începe să producă profit, companiile start-up trebuie să își adapteze oferta la piață cât mai repede, pentru a-și conserva avansul câștigat până la acel moment (*tehnology and timing*). Pentru a face acest lucru, aceste companii au nevoie de finanțare. În general aceste finanțări vin de la persoane fizice sau fonduri de investiții care sunt dispuse să investească în companiile cu risc ridicat.

Există mai multe modalități consacrate de finanțare a start-up-urilor: *crowdfunding* (fonduri obținute prin intermediul platformelor de finanțare); finanțare de tipul *seed* (inverestiții între 100.000 și 300.000 de euro care vin de la familie sau de la prieteni); *business angels* (finanțarea oferită de antreprenori cu vechime antreprenorilor tineri, care în general variază între 300.000 și 3 milioane de euro); fonduri de investiții de serie A (care sunt dispuse să finanțeze proiectul cu sume între 1 și 5 milioane de euro); fonduri de investiții de serie B (care sunt dispuse să finanțeze proiectul cu sume între 2 și 10 milioane de euro);

Apariția etapei PropTech 3.0, care începe la sfârșitul anului 2015, este determinată de mai mulți factori: presiunea generalizată cu privire la normele sanitare și de protecția mediului, inclusiv în construcții, urbanizarea rapidă a statelor cu o populație foarte mare (China, India, țările din continentul african), inteligența artificială și mai ales apariția tehnologiei *blockchain*.

Cel mai probabil, în perioada care va urma, sectorul imobiliar va fi cel mai afectat de apariția *blockchain*: pe de o parte, pentru că acest sector a încercat mereu să evite progresul tehnologic, și să își mențină modul de ”viață” neschimbat, iar pe de altă parte pentru că acest sector este unul dintre cele mai puțin maleabile și efervescente sectoare ale economie. Cu toate acestea, *blockchain* are capacitatea de a afecta toate activitățile componente ale domeniului imobiliar precum construcțiile, modul de finanțare, tranzacțiile imobiliare, administrarea imobilelor etc.

Schimbările deja au început să se producă, iar principalele arii afectate sunt următoarele:

a) reducerea costurilor și a timpului de tranzacționare

Transparența este binevenită în orice domeniu. În sectorul imobiliar ea reprezintă însă o necesitate deoarece, deși de multe ori informațiile ajung la publicul larg, ele nu sunt informații utile, deoarece de multe ori ele ajung incomplete[12]. Prin comparație, Proptech 3.0 nu doar că aduce la utilizator informația, așa cum făcea PropTech 2.0, ci îi conferă și autenticitate (etapa anterioară în evoluția tehnologică a imobiliarelor oferea utilizatorului informația, fără însă a-i garanta veridicitatea). În plus, numărul mare de intermediari într-o tranzacție augmentează numărul de interacțiuni umane, aspect care duce la întârzieri, precum și la creșterea costurilor. *Blockchain* aduce cu sine o transparență totală a acestor tranzacții, scopul fiind de a reduce durata și costul lor. Totodată, această nouă tehnologie poate veni în sprijinul notarilor, care, cu ajutorul *smart contract*, ar putea încheia tranzacțiile mai rapid și cu costuri mai mici pentru ei.

b) facilitarea accesului la proprietate

Investiția în mai multe proprietăți nu este accesibilă celei mai mari părți ale populației, care de regulă deține în proprietate o locuință, care reprezintă locuința principală, și maxim încă un imobil cu titlu de investiție. Prin urmare, accesul la investițiile imobiliare este destul de limitat, întrucât presupune existența unor lichidități consistente care să fie direcționate în case, apartamente, terenuri etc. Investițiile în imobiliare sunt astfel accesibile unui segment restrâns din populație, iar lucrurile nu se îndreaptă spre o direcție bună întrucât, în ultima perioadă, și cheltuielile cu întreținerea locuinței unei familii sunt din ce în ce mai

fonduri de investiții de serie C (care sunt dispuse să finanțeze proiectul cu sume mai mari de 10 milioane de euro). În domeniul imobiliar, în general start-urile sunt finanțate de investitori din seria A, B sau C. A se vedea și N. Reiff, *Series A, B, C Funding: How it works*, 5 martie 2020, Investopedia.

[12] Cel mai elocvent exemplu este un anunț al unei agenții imobiliare, care se rezumă doar la a spune numărul de camere, descrieri care să conțină cuvântul ”lux”, ”zonă bună”, ”vecini liniștiți”, ”balcon mare”, fără însă a da date complete cu privire la oferta imobiliară.

mari. *Blockchain* însă poate schimba acest aspect din prisma faptului că poate facilita accesul la investițiile imobiliare pentru populația generală prin elemente precum cryptomonedele, *token*-urile etc.[13].

c) optimizarea administrării imobilelor

A fi proprietar sau a da în chirie imobile în calitate de locator poate fi o sarcină complexă și cronofagă. De asemenea, experiența închirierii unui imobil poate fi obositoare și dificilă, chiar înainte de a prelua în folosință bunul închiriat, încă din faza căutărilor. Prin urmare, este greu pentru multe persoane să își găsească un imobil pe care să îl închirieze în condiții decente, mai ales în zonele în care piața este volatilă sau prețurile sunt foarte mari. De asemenea, a administra un activ imobiliar reprezintă o muncă dificilă, atât pentru cel care are mai multe clădiri în proprietate, cât și în egală măsură pentru cel care are doar un apartament pe care trebuie să îl gestioneze. Tehnologia *blockchain* poate facilita administrarea imobilelor pentru instituții publice, particulari, locatori, chiriași sau mandatarii administratori de clădiri. Spre exemplu se poate facilita apariția unei piețe de chirii subsidiare, prin intermediul *token*-urilor; adunările generale ale asociațiilor de proprietari ar putea fi mult mai facile și ar avea cvorum mult mai mare; existența aplicațiilor care să faciliteze relația dintre proprietari și chiriași[14] etc.

d) transformarea sectorului imobiliar cu ajutorul tehnologiei

Problema mediului afectează și acest sector deoarece o clădire nu mai este doar o simplă construcție, ci reprezintă o prezență fizică cu impact asupra mediului în care se află pe termen lung, iar zonele adiacente unei clădiri sunt afectate din mai multe puncte de vedere: energetic, urbanistic, din punct de vedere al proprietăților învecinate, al transportului, al apei potabile și de subsol, al impactului social asupra populației, al arhitecturii zonei etc. Potrivit unui studiu

[13] Cu titlu de exemplu, în data de 25 iunie 2019, a avut loc prima tranzacție notarială din Franța în care prețul a fost plătit prin Bitcoin. Hotelul AnnA din zola Boulogne-Billancourt, lângă Paris, a fost cumpărat de Societatea Valorcim și Sapeb pentru suma de 6,5 milioane de euro, achitabilă în Bitcoin. Ulterior, societatea cumpărătoare a emis un număr de 1000 de token-uri, fiecare corespunzând unei acțiuni din societate, iar fiecare token fiind împărțit în 100.000 de subunități cu o valoare de vânzare de 6,5 euro fiecare. Astfel, orice persoană putea cumpăra o astfel de subunitate, devenind practic coproprietar pe firma care deținea hotelul. Cu alte cuvinte, un fel de bursă însă mai puțin reglementată.

[14] Cu titlu de exemplu menționăm aplicația RentBerry. Care reprezintă o soluție în sistemul *blockchain* apărută în Statele Unite în anul 2015 și care este folosită pentru închirierile de lungă durată. Această aplicație facilitează relația dintre proprietar și chiriaș. Specific acestei aplicații este că un chiriaș poate apela, pentru plata garanției sau chiar pentru plata chirie, la *crowdfunding* din partea celorlalți utilizatori. Astfel, chiriașul achită numai 10% din garanție sau din chirie, iar pentru restul poate apela la finanțare din partea unor terți. Aceștia contribuie achiziționând *token*-uri specifice numite *Berry token,* pe care ulterior le pot folosi când închiriază un imobil prin intermediul aplicației pentru diferite facilități: *late checkout,* transport de la aeroport etc. Toate aceste operațiuni se petrec prin încheierea unui *smart contract* cu ajutorul tehnologiei *blockchain.* Pentru mai multe detalii https://rentberry.com.

realizat în 2019[15], industria construcțiilor este responsabilă de 40% din consumul de energie globală, iar edificarea de clădiri stă la baza a 50% din consumul de materii prime din lume. O clădire nu reprezintă un element fizic, ce stă neschimbat pe întreaga sa durată de existență, ci devine un element evolutiv ce trebuie să fie mereu în armonie cu mediul înconjurător; această armonizare se realizează prin efectuarea unor studii și verificări la fiecare clădire, cum ar fi evaluarea performanțelor energetice ale acesteia, a consumului și pierderilor de căldură și de apă, sau prin realizarea unei evidențe a stării clădirilor[16]. Diversitatea și complexitatea informațiilor care astfel sunt colectate necesită un flux al transferurilor de informații foarte rapid, precum și o modalitate eficientă de stocare a acestor informații în plan digital. Tehnologia *blockchain* este singura care poate oferi să „găzduiască" un volum așa de mare de informații.

Tehnologii precum *blockchain* sau inteligența artificială (AI) sunt în plin proces de dezvoltare, iar ceea ce trăim noi astăzi este doar începutul. Acestea vor bulversa economia; se estimează că, până în 2030, programele electronice vor efectua 80% din sarcinile repetitive și cronofage pe care le întreprind oamenii astăzi, multiplicând productivitatea de trei ori[17]. De asemenea, se estimează că inteligența artificială va avea un impact de 13.000 miliarde de dolari până în 2030[18].

Tehnologia *blockchain* poate de asemenea să fluidizeze mobilitatea urbană și rurală, să faciliteze oferirea de servicii, să contribuie la gestiunea corectă a deșeurilor, precum și la o distribuire mai eficientă a energiei. Potrivit raportului Forumului economic mondial[19] de la Davos, până în anul 2027 aproximativ 10% din PIB-ul mondial va fi stocat utilizând tehnologia de tip *blockchain.* Toate aceste tehnologii noi însă, se completează unele pe celelalte și au ca scop să ne facă viața mai ușoară, iar unul dintre domeniile în care acest lucru va fi vizibil cu siguranță că va fi domeniul imobiliar.

2. *Blockchain-smart* contract în domeniul notarial

Apariția tehnologiei *blockchain* a avut ca efect un proces de dematerializare a actelor, registrelor și procedurilor notariale (prin apariția consultațiilor la distanță, eficientizarea unor servicii publice, cum ar fi Oficiul de Cadastru și Publicitate Imobiliară, care nu mai lucrează cu notarii decât în sistem *on-line*,

[15] Bronckers J., Veuger J., Appelmans A., Cesar T., Brahmbhatt S., *Fibree Industry Report Blockchain Real Estate 2019,* 2019, organizația Fibree.

[16] Începând cu 1 ianuarie 2020, în Franța, fiecare clădire trebuie să dețină o carte tehnică în format electronic, care este inclusă într-o bază de date folosind tehnologia *blockchain*, și al are toată lumea are acces (*Loi 2018-1021 du 23 novembre 2008).*

[17] FuturaCorp, *Artificial Intelligence and the Freedom to be Human,* Raport IPSoft, ianuarie 2017.

[18] Jacques Bughin, Jeongmin Seong, James Manyika, Michael Chui, Raoul Joshi, *Notes from the A.I. frontier: modeling the impact of A.I. on the world economy-Discussion Paper,* editura McKinsey & Company, Chichago, septembrie 2018.

[19] Sursă online: https://www.weforum.org/agenda/2024/01/blockchain-change-world-finance-stablecoins-internet/

platforme digitale etc.), efect care, în mod inevitabil, îi obligă și pe notari să își adapteze activitatea la noile condiții. Astfel, fără a considera tehnologiile actuale ca fiind un element distructiv al circuitului actelor notariale, tehnologia *blockchain* a schimbat radical modul în care birourile notariale colaborează cu instituțiile statului, cu clienții, câteodată chiar și cu personalul propriu (având în vedere că există și situații în care angajații biroului notarial pot lucra de la distanță) fără însă a aduce atingere atribuțiunilor notarului, sau a identității acestuia; în fond, acesta rămâne un mandatar al puterii publice care are ca scop autentificarea actelor și convențiilor dintre părți. Notarilor nu trebuie să le fie frică de apariția tehnologiei *blockchain*, însă trebuie să fie în continuare vigilenți, și să folosească noile tehnologii pentru a-și ușura munca, nu pentru a o înlocui.

Sunt multe avantaje care au venit împreună cu *blockchain*, iar una dintre acestea este reprezentată de apariția în spațiul public din ce în ce mai des a conceptului de *smart contract.*

Smart contract reprezintă un program care, funcționând în sistemul *blockchain*, facilitează automatizarea unor sarcini care până acum erau făcute manual de un om. Cu toate acestea, ideea unui program care să execute în mod automat sarcinile pe care le are de făcut un om nu este o noutate; această idee a apărut în jurul secolului XVII, odată cu apariția curentului filosofic numit „mecanicism”[20]. Noutatea constă în asocierea acestui proces automat cu tehnologia *blockchain* (introducerea contractului în acest sistem se face prin emiterea unei adrese formulate în sistemul de numerație hexazecimal care declanșează toate informațiile dintr-un contract de tip *smart*) de către Nick Szabo[21] la mijlocul anilor 1990, care a pus în picioare un protocol permanent la care aveau acces toate persoanele, chiar dacă nu se cunoșteau dinainte, și care putea încheia acte și tranzacționa valori într-un sistem digital foarte sigur.

Cu toate acestea, contractele *smart* nu au nimic în comun cu Inteligența Artificială. Acestea nu sunt contracte *per se,* ci sunt programe informatice care automatizează anumite fapte sau acte, și care au o structură ”*If this...Then that...*”, respectiv o comandă declanșează o altă comandă, care la rândul ei declanșează o altă comandă etc.[22] Ele nu reprezintă un contract inteligent, doar au în componență un algoritm pe care programatorul l-a imaginat și creat, prin urmare nu lasă loc de interpretări, însă în egală măsură nu lasă loc nici de negocieri sau de schimbări imprevizibile. Scopul contractului *smart* este de a transpune în lumea digitală, și în rețeaua *blockchain* un contract care a fost anterior încheiat în „lumea reală”, respectiv a fost negociat de părți, iar forma sa finală a fost stabilită. Însă numai anumite etape ale procesului de încheiere a unui contract pot fi automatizate *smart,* precum remiterea unor documente, efectuarea unor plăți, înscrierea în cartea funciară a unui imobil etc.

[20] Tournier G., *Babel ou le vertige technique,* Editura Fayard, Paris, 1959, p. 104.

[21] Nicholas Szabo, n. 5 aprilie 1964, este un programator american cunoscut pentru studiile sale în domeniul contractelor și a valutelor digitale. Acesta a creat în 1998 prima monedă virtuală, BitGold, considerată precursoarea BitCoin-ului.

[22] Ferre-Andre S., Camouz S.Y et alii, *Notaire,* Editura Dalloz, Paris, 2020, p. 82.

Pentru a înțelege mai bine cum funcționează un *smart contract*, cel mai indicat este să dăm un exemplu, în cazul unei tranzacții imobiliare. Părțile interesate fie s-ar prezenta la notar, fie s-ar loga în sistem de videoconferință de la distanță, la data și ora programării. Notarul le identifică (tot electronic), le prezintă actul, se descrie bunul, prețul, condițiile vânzării și toate termenele contractului. Ulterior, consimțământul părților este luat prin semnătura electronică a fiecăreia. În momentul în care actul este semnat electronic, începe procesul *smart.* Contractul cu toate datele introduse în program intră în sistemul tehnologic de tip *blockchain.* În mod automat, în câteva secunde, contul bancar al cumpărătorului este debitat cu valoarea prețului, iar cel al creditorului este alimentat. Tot astfel, dreptul de proprietate al cumpărătorului este imediat înscris în Cartea Funciară a imobilului, pe rolul fiscal, la asociația de proprietari, la furnizorii de utilități etc. Nu ar fi cu nimic diferit față de cazurile în care fiecare dintre noi comandăm un produs pe internet. Și sistemele magazinelor on-line folosesc *blockchain* pentru operativitate. Astfel, când dăm o comandă, introducem datele de livrare și numărul cardului bancar iar comanda este preluată automat de programul electronic, și se declanșează un întreg proces de evenimente: contul nostru bancar este debitat, comanda este înregistrată, plasată și transmisă imediat la depozitul furnizorului care înștiințează imediat firma de curierat că trebuie să ridice un colet pentru un client și să îl livreze la adresa indicată.

Cu toate acestea, un contract de tip *smart* are avantajul că optimizează procesul de încheiere a unei convenții precum și cel de punere în executare a acesteia, dar mai ales optimizează plata efectuată în baza unui contract.

Există numeroase teorii fanteziste cu privire la *blockchain* și *smart contracts.* Fără însă a intra în discuții exagerate, se impune a răspunde la trei întrebări care să ne ajute să înțelegem fenomenul: procesul contractual digital este sigur? Procesul contractual digital este complet dematerializat? Procesul contractual digital se produce exclusiv automat, fără niciun fel de intermediar?

Fără niciun fel de dubiu că utilizarea tehnologie *blockchain* în general, și a celei de *smart* contract în mod particular, prezintă o siguranță mai mare pentru părți în cazul încheierii sau executării unui contract. Cu cât există mai multe persoane implicate sau cu cât sunt mai multe documente în fizic ce stau la baza contractului, cu atât riscul este mai mare. Documentele fizice pot fi pierdute, distruse, falsificate sau expediate unor alte persoane decât cele în drept să le știe. În toate aceste cazuri, automatizarea procesului de creare și emitere de documente, exclusiv în format digital, reprezintă un avantaj. Această tehnologie permite de asemenea și confirmarea datei în care un document a fost creat sau expediat. De asemenea, cu cât sunt mai mulți actori implicați, cu atât durata încheierii unui contract este din ce în ce mai mare. Comunicarea cu diferite instituții, chiar dacă se face prin poștă electronică, tot durează. În sistemul *blockchain*, toate aceste comunicări se fac instant, în timp real, astfel încât documentele certificate prin semnătură electronică sunt mereu suspendate în spațiul virtual, putând fi accesat în câteva secunde de orice parte interesată. Reducerea erorilor umane care ar putea apărea, a întârzierilor și a costurilor fac din *blockchain* și din *smart contract* o alternativă ieftină pentru încheierea unei convenții, cheltuielile fiind semnificativ mai mici.

Însă ne întrebăm, oare procesul contractual poate fi încheiat exclusiv prin sistem *smart* contract, respectiv fără intervenția nici măcar a notarului sau a unui alt intermediar? Cu alte cuvinte, un contract de o importanță mare, cum ar fi un contract de vânzare a unui bun imobil, poate fi încheiat exclusiv în formă dematerializată? Răspunsul se pare că este nu, deoarece există numeroase obstacole de ordin tehnologic și juridic care ar împiedica acest lucru[23]. Pe plan tehnologic, multe din etapele contractuale nu pot fi transpuse într-un algoritm. Câte din condițiile de validitate ale unui contract pot îmbrăca forma unui program electronic? Cum traducem în limbaj digital emiterea unei oferte și acceptarea ei? Cum verificăm capacitatea civilă a unei persoane? Cum ne asigurăm că încheierea contractul, care se face de la distanță, nu este făcută sub amenințarea unei terțe persoane care se află în încăperea în care se află și partea semnatară? Astfel, respectarea tuturor condițiilor de validitate ale unei convenții și îndeplinirea exigențelor legale sunt imposibile exclusiv în sistem on-line.

Și sarcina probei actului ar fi dificilă în sistem *blockchain* și *smart contract.* Majoritatea legislațiilor europene recunosc semnătura electronică calificată emisă de un furnizor acreditat ca fiind suficientă pentru a conferi forță probantă unui înscris. Însă se pune întrebarea: actele emise în *blockchain* sau sub forma unui contract *smart*, se încadrează în această categorie? Răspunsul este că nu. Acestea nu conțin niciun fel de semnătură electronică. Ba mai mult, noile tehnologii permit emiterea de astfel de documente de către o persoană care nu își dezvălui numele adevărat, ci poate purta un pseudonim.

De multe ori se zice că tehnologia *blockchain* și *smart contract* reprezintă un sistem fără niciun fel de intermediari și ne permite să visăm la o lume complet transparentă, iar serviciilor digitale bazate pe sisteme care presupun un intermediar, cum ar fi Uber, Bolt sau Airbnb să le fie amenințată existența. Teoretic vorbind, există într-adevăr posibilitatea ca aceste sisteme să nu dispună de niciun fel de intermediere. Totul să se desfășoare automat, fără vreo altă intervenție. Însă, având în vedere cele prezentate mai sus, acest lucru ar fi extrem de dăunător circuitului juridic. Programele electronice nu lasă loc de „poate". Cu ele nu se poate negocia. În momentul în care primesc comanda, o execută fără să stea pe gânduri. Or într-o lume extrem de volatilă precum cea a juridicului, această atitudine nu reprezintă un avantaj.

Există cu toate acestea și posibilitatea unui al treilea intermediar, care poartă denumirea de *Trusted third party (TTP). Blockchain*-urile pot fi de trei feluri: publice, hibride și private. Dacă în cazul celor publice, toate lumea are acces, nu există intermediari iar transparența este totală, în cazul celor hibrid sau private există o a treia parte, un TTP, care controlează și se asigură că programele conectate în *blockchain* funcționează corespunzător, nu apar erori, iar dacă sunt

[23] Sursă online: https://jeromegiustiblog.wordpress.com/2016/05/27/les-smart-contracts-sont-ils-des-contrats/

situații neprevăzute, acesta le poate remedia. Cu titlu de exemplu, în cazul unui contract prin care părțile negociază plata prețului în rate: în act se stipulează că neplata unei rate la timp atrage penalități, iar neplata a trei rate consecutive atrage rezoluțiunea contractului. În cazul unui *smart contract* pe *blockchain* public, în prima situație s-ar începe executarea silită imediat, iar în ce-a de a doua, contractul ar fi reziliat automat, dreptul de proprietate reînscris în cartea funciară și în toate celelalte registre din nou pe numele vânzătorului. În cazul unui *smart contract* în *blockchain* hibrid sau privat, întârzierea la plată ar trece prin filtrul unui intermediar (TTP) care, în funcție de situația de fapt, ar aprecia dacă se impune activarea pactului comisoriu sau nu. Aceasta deoarece în juridic sunt multe necunoscute: poate a intervenit un caz de forță majoră; poate conduita vânzătorului nu a permis cumpărătorului să mai achite ratele etc.

În principiu, documentele înscrise în *blockchain* nu pot fi falsificate. Schimbul acestor documente (acte de stare civilă, contracte, diplome etc.) se poate face cu respectarea tuturor condițiilor de securitate. Aceasta deoarece odată ce au fost încărcate în *blockchain*, ele nu mai pot fi modificate. Această tehnologie permite astfel conservarea acestor documente într-o arhivă electronică pentru o perioadă nelimitată de timp. Cu toate acestea, deși prin această tehnologie se garantează integritatea documentului, sub nicio formă *blockchain* nu garantează și autenticitatea lui, în sensul în care nu se garantează că el chiar a fost emis de persoana de care se pretinde că ar fi emis. Prin urmare, în caz de litigiu, un judecător nu va putea fi obligat să ia în considerare o astfel de înscriere în *blockchain* ca fiind o veritabilă probă.

Contractele de tip *smart* au avantajul că se pot încheia foarte repede, însă în domeniul juridic există o serie de clauze care nu pot fi prevăzute de un program electronic. Deși un astfel de contract elimină multe riscuri la care pot fi expuse părțile prin încheierea unui contract fizic, acesta deschide calea la apariția altor riscuri. Astfel, pentru ca un *smart* contract să poată fi folosit în circuitul juridic, există o serie de clauze care are trebuie lăsate la interpretarea unei astfel de a treia părți (TTP) și nu executate automat, din simplul motiv că nu pot face obiectul unui algoritm. Acestea sunt de regulă clauzele care reglementează imprevizibilul. Să nu uităm că *smart contract* nu au nicio legătură cu Inteligența Artificială, care ar putea da naștere la *intelligent contracts.* Ele nu pot efectua decât operațiunile pe care programatorul le-a prevăzut și le-a inclus în algoritm. Prin urmare, situațiile neprevăzute precum cele de forță majoră, nu pot fi incluse în astfel de contracte. Totodată, contractele *smart* sunt ireversibile, prin urmare nu putem discuta de rezoluțiunea acestora. Cu toate acestea, în cazul unui contract *smart* încheiat într-un *blockchain* privat, se poate prevedea clauza ca, în eventualitatea în care un al treilea intermediar (TTP) constată că este îndeplinită o condiție care să atragă forța majoră, acest lucru să declanșeze între părți, automat, încheierea unui nou *smart contract*, care să îl înlocuiască pe cel inițial. Cu alte cuvinte, s-ar prevedea o *suicide clause* pentru contractul inițial. În materie de clauze imprevizibile se pune problema însă ce se întâmplă cu acele situații în care nu un element exterior programului intervine în executarea contractului, ci chiar unul din interiorul acestuia, precum un atac cibernetic sau furtul de date.

Concluzie

Răspunsul la întrebarea dacă tehnologia *blockchain* este pregătită să fie folosită în sistemul notarial sau, mai exact, dacă sistemul notarial și sectorul imobiliar este pregătit pentru tehnologia *blockchain*, este extrem de subiectiv. În ultima perioadă avem senzația că tehnologia ne invadează viețile, și suntem din ce în ce mai sufocați de noile măsuri de digitalizare pe care guvernul, instituțiile statului, ba chiar Uniunea Europeană ni le impun. Cu toate acestea, poate că ar trebuie să reflectăm dacă într-adevăr tehnologia este un sprijin pentru oameni, sau a ajuns să îi controleze. Poate că, prin excesul acesta de tehnologie, rasa umană va ajunge să își piardă multe dintre caracteristicile sale definitorii, inclusiv cea de „ființă socială”. Rămâne ca timpul să clarifice acest aspect.

Referințe

Baum A., *PropTech 3.0; The future of Real Estate, Said Business School*, Oxford University, 2017.

Bronckers J., Veuger J., Appelmans A., Cesar T., Brahmbhatt S., *Fibree Industry Report Blockchain Real Estate 2019,* 2019, organizația Fibree.

Bughin J., Seong J., Manyika J., Chui M., Joshi R., *Notes from the A.I. frontier: modeling the impact of A.I. on the world economy-Discussion Paper,* Editura McKinsey & Company, Chichago, septembrie 2018.

Ferre-Andre S., Camouz J.-Y.*et alii*, *Notaire,* Editura Dalloz, Paris, 2020.

FuturaCorp, *Artificial Intelligence and the Freedom to be Human,* Raport IPSoft, ianuarie 2017.

Tournier G., Babel ou le vertige technique, Editura Fayard, Paris, 1959.

HSBC&Savills World Research, *Global Real Estate, Trend în the worlds' largest asset class,* 2017.

ANALELE ŞTIINŢIFICE ALE UNIVERSITĂŢII „ALEXANDRU IOAN CUZA" DIN IAŞI
TOM LXX, 2, ŞTIINŢE JURIDICE, 2024

DOI: 10.47743/jss-2024-70-2-7

Datele cu caracter personal: *res digitalis* în sfera actelor încheiate *inter vivos* și a actelor *mortis causa*

Personal Data: *res digitalis,* Object of Acts Concluded *inter vivos* and of Acts Concluded *mortis causa*

Crina-Maria STANCIU[1], Codrin-Alexandru ȘTEFĂNIU[2]

Rezumat: Această prezentare își propune să exploreze echilibrul complex dintre valorificarea potențialului AI pentru progresul societății și abordarea implicațiilor etice ale utilizării datelor. În zilele noastre, datele sunt adunate și se stochează informații despre utilizatori, procedeu care trebuie să respecte un set de legi foarte specifice. Acest lucru dă putere cercetătorilor din domeniul AI să-și antreneze modelele fără a le alimenta cu date decriptate de utilizator. Dar cine decide cum să folosească datele? În prezent, majoritatea companiilor care colectează informații de la clienţii lor trebuie să urmeze un set de directive ale Comisiei UE. Prin urmare, evoluția inteligenței artificiale nu ar însemna invadarea intimității personale. În această lucrare sperăm să creștem necesitatea tratării datelor ca obiect legal căruia i se vor aplica reguli reinterpretate, conform fluxului de dezvoltare a AI. Ne vom concentra mai mult asupra conținutului datelor și asupra momentului în care datele ar putea fi stocate și transferate ca urmare a creșterii valorii lor (valoare economică). Datele sunt un activ care poate fi tranzacționat. De asemenea, datele pot ajuta la crearea unei personalități a utilizatorilor (de aceea valoarea datelor poate crește). O altă întrebare la care vom încerca să răspundem se referă la conceptul de „moștenire digitală" și datele post-mortem. După ce o persoană moare, ce se va întâmpla cu forma sa digitală, cum ar fi banii digitali (bitcoin sau active câștigate într-un joc), cu contul de Facebook, contul Google etc.? Datele personale ale omului vor crea oameni artificiali care vor supraviețui morții naturale?

Cuvinte cheie: IA, *machine learning*, acte *inter vivos*, acte *mortis causa,* proprietate.

Abstract: This presentation aims to explore the intricate balance between harnessing the potential of AI for societal advancement and addressing the ethical implications of data utilization. Nowadays data centers where user information is stocked must follow a very specific set of laws. This empowers researchers in the field of AI to train their models without feeding them with decrypted user data. But who decides how to use the data? Currently most companies that gather information from their customers must follow a set

[1] Drd., Facultatea de Drept, Universitatea „Alexandru Ioan Cuza" din Iași, e-mail: crina.stanciu@uaic.ro.

[2] Inginer software, e-mail: codrinstefaniu36@gmail.com.

of directives from the EU Commission. Therefore, the evolution of the artificial intelligence would not mean the invasion of personal privacy. In this paper we hope to increase the necessity of treating data as legal object to which will apply reinterpreted rules, according to the flow of AI development. We will focus more on the content of data and to the moment when the data might be stored and transferred because of its increasing value (economic value). Data is an asset who can be traded. Also, data can help to create a personality of the users (this is why the value of data can increase). Another question we will try to answer concerns the concept of „digital estate" and postmortem data. After a person dies what will happen with its digital form like digital money (bitcoin or assets won in a game), with the Facebook account, Google account etc.? Data from people will make artificial people who will survive the natural death?

Keywords: AI, *machine learning*, acts *inter vivos*, acts *mortis causa*, property.

1. Introducere

În vederea încadrării datelor cu caracter personal în sfera bunurilor asupra cărora persoana dobândește dreptul de proprietate, vom desluși, înainte de toate sensul acestora, folosind art. 4 al General Data Protection Regulation (Regulamentul UE 2016/679 GDPR):

> *„«date cu caracter personal» înseamnă orice informații privind o persoană fizică identificată sau identificabilă ("persoana vizată"); o persoană fizică identificabilă este o persoană care poate fi identificată, direct sau indirect, în special prin referire la un element de identificare, cum ar fi un nume, un număr de identificare, date de localizare, un identificator online, sau la unul sau mai multe elemente specifice, proprii identității sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale."*[3].

Datele cu caracter personal decurg din principalele caracteristici ale persoanei. Prin difuzarea acestora pe calea internetului s-a ajuns la crearea unor noi tipuri de comerț. De această dată comerțul implică transferul de date personale, fapt care se traduce prin transferul de informații cu privire la persoane, transfer care operează, de cele mai multe ori, dintr-un capăt al lumii în celălalt.

O problemă aparte survine la momentul în care se analizează și se transferă colecțiile de date denumite și „big data". Astfel, într-o primă fază datele sunt adunate de către o organizație fie pe cale directă (fiind obținute direct de la persoanele vizate prin variate chestionare adresate în mediul on-line), fie pe cale indirectă (prin intermediul brokerilor de date personale) sau prin combinarea unor date deja dobândite. O a doua fază are în vedere analizarea datelor în vederea obținerii de cunoștințe, de informații (analiză realizată prin tehnici *machine learning*). În final, cunoștințele se vor aplica și va fi creat un algoritm care poate arăta probabilitatea unei persoane, de exemplu, de a cumpăra un anumit produs într-un anumit interval de timp. În cazul în care datele și algoritmul astfel creat ar

[3] Regulamentul UE 2016/679, JOUE L119, 4.05.2016.

fi vândute unei terțe persoane se adresează întrebarea cum anume sunt protejate acele date împotriva abuzurilor variatelor organizații[4].

De un real interes este Carta Drepturilor Fundamentale a Uniunii Europene în cadrul căreia dreptul la protecția datelor este reprezentat de articolul 8[5]. Acesta stabilește dreptul fiecărei persoane la protejarea datelor cu caracter personal. De asemenea procesarea acestor date trebuie realizată numai pentru scopuri bine delimitate, având drept fundament consimțământul persoanei vizate sau un alt temei legal. În plus, fiecare persoană are posibilitatea de a accesa propriile date colectate, precum și dreptul de a le modifica sau de a le corecta. Subliniem faptul că acest drept fundamental nu are în vedere doar datele personale care sunt în legătură cu sfera privată a persoanelor, ci stabilește o metodă de protecție a acestora oricând are loc procesarea datelor cu caracter personal[6].

În vederea realizării unei analize pertinente vom avea în vedere modul în care se coroborează și se auto influențează art. 7 și art. 8 ale Cartei Drepturilor Fundamentale a Uniunii Europene. Articolul 7 are în vedere dreptul persoanei de a-i fi respectate viața privată și viața de familie, casa și căile de comunicare[7].

Carta a fost prezentată prima dată de Parlamentul European, de Consiliu și de Comisie la data de 7 decembrie în anul 2000 la Nisa, producând efecte de la data de 1 decembrie 2009.

În articolele vizate observăm faptul că sintagma „viață privată" nu are un singur sens, ci o multitudine. Aceasta nu poate face obiectul unei reglementări singulare deoarece articolul astfel creat ar conduce la limitarea sferei de aplicare a ceea ce este „privat". Autori precum Samuel Warren și Louis Brandeis au văzut în viața privată „dreptul de a fi lăsat în pace"[8]. Cu alte cuvinte, viața privată a persoanei va fi analizată de o manieră *in extenso* în sfera juridică pentru a-i putea oferi aria de aplicare cea mai largă.

Conferința de Nord a Juriștilor din anul 1967, a întărit convingerea că o componentă a protecției datelor cu caracter personal este acest drept al persoanei de a fi lăsată în pace, cu o minimă ingerință din exterior. Cu alte cuvinte, dreptul

[4] M. Backhoum, B. C. Gallego, M. O. Mackenrodt, *et. alii*, *Personal Data in Competition, Consumer Protection and Intellectual Property Law. Toward a Holistic Approach?*, în *MPI Studies on intellectual Property and Competition Law 28*, Springer, Berlin, 2018, pp. 15-18, https://doi.org/ 10.1007/978-3-662-57646-5.

[5] Carta drepturilor fundamentale a Uniunii Europene, JOUE C303, 14.12.2007. [Online] la https://fra.europa.eu/ro/eu-charter/article/8-protectia-datelor-cu-caracter-personal, accesat la 02.2.2024.

[6] T. Naef, *Data Protection without Data Protectionism. The Right to Protection of Personal Data and Data Transfers in EU Law and International Trade Law, in loc. cit.*, Marc Bungenberg, Christoph Herrmann, Markus Krajewski, et. alii., *EYIEL Monographs-Studies in European and International Economic Law*, Vol. 28, Springer, 2021, p. 30, https://doi.org/10.1007/978-3-662-57646-5.

[7] Carta drepturilor fundamentale a Uniunii Europene, JOUE C303, 14.12.2007.

[8] S. D. Warren, L. D. Brandeis, *The Right to Privacy, in Harvard Law Review*, Vol. IV, decembrie 1890, [Online] la https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html, accesat 12.04.2024.

la protecția datelor cu caracter personal ajunge să includă și protecția împotriva atingerilor aduse familiei, vieții de acasă, aspectelor vieții cu privire la nume, identitate[9].

Evoluția tehnologică atacă această sferă a vieții private, fapt care poate fi observat mai ales în activitatea de supraveghere continuă realizată de colecționarii de date: colectează mari cantități de date ale persoanelor din e-mailurile private, locația telefonului, istoricul web, toate acestea fără consimțământul persoanei și fără un fundament legal.

Îmbinarea celor două articole amintite a condus către limitarea accesului statului în viața privată a persoanei, fără o justificare temeinică. Protecția datelor și regulile care o implică nu exclud procesarea datelor cu caracter personal, creând un temei juridic, limitând modurile în care datele cu caracter personal vor putea fi procesate. Un bun exemplu este articolul 9 GDPR care împiedică procesarea anumitor categorii specifice de date cu caracter personal în ceea ce privește originea etnică, rasa, opinia politică, religioasă, credințele filozofice, apartenența la o asociație de comerț, procesarea datelor genetice, în vederea identificării persoanei fizice, a datelor cu caracter medical sau acelea care au în vedere orientarea sexuală a persoanei, în aliniatul al doilea al articolului fiind prevăzute excepții.

Articolul 8 al Cartei Drepturilor Fundamentale a Uniunii Europene va fi coroborat cu art. 4 GDPR în vederea aflării conținutului acestui drept fundamental, al protecției datelor cu caracter personal. Deducem, astfel, faptul că datele precum adresa IP, date de identificare ale persoanelor fizice vor fi incluse în noțiunea de „date”. Mai mult decât atât, se afirmă faptul că informația referitoare la persoană este mult mai voluminoasă, mai complexă decât informațiile care au în vedere strict acea persoană. Toate aceste informații vor fi protejate împotriva procesării datelor, procesarea însemnând colectarea, înregistrarea, depozitarea, combinarea, transferul datelor dintr-un stat în altul.

Aliniatul al doilea al articolului 8 din Cartă, este de asemenea edificator în ceea ce privește conținutul protecției datelor, structurată fiind pe trei trepte de analiză: procesarea datelor trebuie să se facă de o manieră corectă, de bună-credință; procesarea datelor trebuie să aibă în vedere un scop bine determinat; procesarea datelor trebuie realizată cu consimțământul persoanei vizate sau să aibă un alt fundament legal[10].

Pentru ca procesarea datelor să poată fi realizată de o manieră corectă, de bună-credință, persoana vizată trebuie să cunoască existența datelor și a procesării. Cu alte cuvinte, procesarea datelor personale fără un fundament legal bine determinat va avea un caracter ilicit.

De asemenea, scopul procesării datelor cu caracter personal are în vedere așteptarea rezonabilă a subiectului vizat, precum și limitele existente și alipite

[9] T. Naef, *op. cit.,* pp. 32-33.

[10] T. Naef, *op. cit.,* p. 39.

procesului. Scopul este întotdeauna stabilit înainte de procesarea datelor cu caracter personal pentru o mai mare siguranță a raportului juridic astfel creat.

Fundamentul legal al procesării datelor cu caracter personal trebuie să poată fi identificat întotdeauna, iar consimțământul persoanei vizate la procesarea datelor va trebui acordat de o manieră liberă, serioasă, fără eroare, așa cum este solicitat și de art. 4 al GDPR.

Articolul 8 din Cartă acordă persoanei vizate alte două prerogative, respectiv dreptul de a avea acces la datele colectate și dreptul de a corecta datele procesate. În acest fel, subiectul de drept va putea observa modul în care îi sunt procesate datele, operațiunile stabilite, putând verifica corectitudinea datelor personale și dacă îi sunt respectate drepturile prevăzute de legislația în vigoare. Prin urmare, subiectul de drept dobândește un oarecare control asupra procedeului de procesare a propriilor date cu caracter personal.

Alte două articole din GDPR sunt strâns legate de aceste componente ale art. 8 din Cartă, respectiv art. 15 GDPR (care stabilește că subiectul de drept va primi un document cu informațiile referitoare la procesarea datelor, scopul procesării, precum și cu țările, subiectele de drept/operatorii care vor primi rezultatul acelei procesări) și art. 16 GDPR (care stabilește necesitatea rectificării oricăror date incorecte, de îndată, fără întârziere)[11].

În România, implementarea Directivei Uniunii Europene 95/46/EC cu privire la protecția datelor cu caracter personal a avut loc înainte ca țara să adere la Uniune, prin adoptarea Legii nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date[12]. Cu

[11] *Idem*, p. 41.

[12] În art. 3 al Legii nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date se specifică:

„În înţelesul prezentei legi, următorii termeni se definesc după cum urmează:

a) date cu caracter personal – orice informaţii referitoare la o persoană fizica identificata sau identificabila; o persoană identificabila este acea persoana care poate fi identificata, direct sau indirect, în mod particular prin referire la un număr de identificare ori la unul sau la mai mulţi factori specifici identităţii sale fizice, fiziologice, psihice, economice, culturale sau sociale;

b) prelucrarea datelor cu caracter personal – orice operaţiune sau set de operaţiuni care se efectuează asupra datelor cu caracter personal, prin mijloace automate sau neautomate, cum ar fi colectarea, înregistrarea, organizarea, stocarea, adaptarea ori modificarea, extragerea, consultarea, utilizarea, dezvaluirea către terţi prin transmitere, diseminare sau în orice alt mod, alaturarea ori combinarea, blocarea, ştergerea sau distrugerea;

c) stocarea – păstrarea pe orice fel de suport a datelor cu caracter personal culese;

d) sistem de evidenta a datelor cu caracter personal - orice structura organizată de date cu caracter personal, accesibila potrivit unor criterii determinate, indiferent dacă aceasta structura este organizată în mod centralizat ori descentralizat sau este repartizata după criterii functionale ori geografice;

e) operator – orice persoană fizica sau juridică, de drept privat ori de drept public, inclusiv autorităţile publice, instituţiile şi structurile teritoriale ale acestora, care stabileşte toate acestea, în anul 2004 s-a considerat că exista o lipsă în modul în care era supravegheată respectarea legii și modul în care era pusă în aplicare. De aceea, România a reacționat și a întărit modul de implementare a noii legi. În acest fel, legea a fost mai bine structurată și organizată, punctând faptul că subiectele de drept aveau dreptul a fi informate, dreptul la acces, dreptul ca datele personale să fie schimbate sau modificate, dreptul la ștergerea datelor, dreptul de a face plângeri la autoritatea privind protecția datelor sau de a se adresa instanțelor de judecată. Modificările GDPR nu au mai fost incluse în legislația din România, precum dreptul la portabilitate a datelor, dreptul la a fi uitat[13], dreptul la a fi notificat în caz de

scopul şi mijloacele de prelucrare a datelor cu caracter personal; dacă scopul şi mijloacele de prelucrare a datelor cu caracter personal sunt determinate printr-un act normativ sau în baza unui act normativ, operator este persoana fizica sau juridică, de drept public ori de drept privat, care este desemnată ca operator prin acel act normativ sau în baza acelui act normativ;".

[13] Art. 17 GDPR „(1) Persoana vizată are dreptul de a obține din partea operatorului ștergerea datelor cu caracter personal care o privesc, fără întârzieri nejustificate, iar operatorul are obligația de a șterge datele cu caracter personal fără întârzieri nejustificate în cazul în care se aplică unul dintre următoarele motive:

(a) datele cu caracter personal nu mai sunt necesare pentru îndeplinirea scopurilor pentru care au fost colectate sau prelucrate;

(b) persoana vizată își retrage consimțământul pe baza căruia are loc prelucrarea, în conformitate cu articolul 6 alineatul (1) litera (a) sau cu articolul 9 alineatul (2) litera (a), și nu există niciun alt temei juridic pentru prelucrare; (c) persoana vizată se opune prelucrării în temeiul articolului 21 alineatul (1) și nu există motive legitime care să prevaleze în ceea ce privește prelucrarea sau persoana vizată se opune prelucrării în temeiul articolului 21 alineatul (2);

(d) datele cu caracter personal au fost prelucrate ilegal;

(e) datele cu caracter personal trebuie șterse pentru respectarea unei obligații legale care revine operatorului în temeiul dreptului Uniunii sau al dreptului intern sub incidența căruia se află operatorul;

(f) datele cu caracter personal au fost colectate în legătură cu oferirea de servicii ale societății informaționale menționate la articolul 8 alineatul (1).

(2) În cazul în care operatorul a făcut publice datele cu caracter personal și este obligat, în temeiul alineatului (1), să le șteargă, operatorul, ținând seama de tehnologia disponibilă și de costul implementării, ia măsuri rezonabile, inclusiv măsuri tehnice, pentru a informa operatorii care prelucrează datele cu caracter personal că persoana vizată a solicitat ștergerea de către acești operatori a oricăror linkuri către datele respective sau a oricăror copii sau reproduceri ale acestor date cu caracter personal.

(3) (a) Alineatele (1) și (2a) nu se aplică în măsura în care prelucrarea este necesară:

(a) pentru exercitarea dreptului la liberă exprimare și la informare;

(b) pentru respectarea unei obligații legale care prevede prelucrarea în temeiul dreptului Uniunii sau al dreptului intern care se aplică operatorului sau pentru îndeplinirea unei sarcini executate în interes public sau în cadrul exercitării unei autorități oficiale cu care este învestit operatorul;

(c) din motive de interes public în domeniul sănătății publice, în conformitate cu articolul 9 alineatul (2) literele (h) și (i) și cu articolul 9 alineatul (3);

încălcare a modului de procesare a datelor cu caracter personal[14].

De un real interes este articolul 28 al legii care îi obligă pe profesioniști să redacteze coduri de conduită care să primească aprobarea Autorității pentru protecția datelor.

2. Datele cu caracter personal – *res digitalis*, obiect derivat al dreptului de proprietate? Datele cu caracter personal incluse la nivelul actelor încheiate *inter vivos*

Comportamentul persoanei în ceea ce privește bunurile pe care le deține este unul specific proprietarului, de stăpân, putând folosi, dispune și poseda bunul, iar acest comportament se extinde nu doar asupra a ceea ce este corporal, ci și a ceea ce este intangibil, necorporal. Cu alte cuvinte, lexemele „a avea" se extind și asupra ideilor persoanei, dar și a datelor cu caracter personal din sfera digitală.

Dreptul de proprietate este unul perpetuu, exclusiv, absolut, fiind, prin urmare, opozabil *erga omnes*, iar tipologia sa precum și conținutul îi sunt atribuite de către lege. Obiectul trebuie să fie bine determinat și adus la cunoștința publicului[15]. Pe cale de consecință, unul dintre doctrinarii elvețieni, Eckert, a considerat că datele cu caracter personal sunt bunuri necorporale care ar trebui incluse în categoria bunurilor digitale, *res digitalis*, deoarece îndeplinesc cerința de control al proprietarului întocmai ca bunurile corporale[16]. Avem, astfel, în vedere și Codul Civil al Elveției[17] care statuează că forțele naturii supuse controlului uman pot face obiectul dreptului de proprietate, iar condiția corporalității bunurilor ar trebui să primească o interpretare *lato sensu*. Cu toate acestea, au fost aduse două critici acestei opinii fundamentate pe articolului Codului elvețian[18].

(d) în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice, în conformitate cu articolul 89 alineatul (1), în măsura în care dreptul menționat la alineatul (1) este susceptibil să facă imposibilă sau să afecteze în mod grav realizarea obiectivelor prelucrării respective; sau

(e) pentru constatarea, exercitarea sau apărarea unui drept în instanță.".

[14] B. Custers, Alan M. Sears, F. Dechesne *et. alii, EU Personal Data Protection in Policy and Practice, in* S. van der Holf *et alii, Information Technology and Law Series vol. 29,* Ed. T.M.C. ASSER PRESS, Haga, 2019, pp. 153-173, https://doi.org/10.1007/978-94-6265-282-8.

[15] G. Boroi, C.A. Anghelescu, B. Nazat, *Curs de drept civil. Drepturile reale principale*, Ed. Hamangiu, București, 2013, pp. 16-17.

[16] Eckert, M., *Digitale Daten als Wirtschaftsgut: digitale Daten als Sache, 112 Schweizerische Juristen-Zeitung 245*, 2016, *apud*, M. Backhoum, B. C. Gallego, M. O. Mackenrodt, *et alii*, *op. cit.,* p. 260.

[17] Codul civil Elvețian în vigoare din data de 1.01.1912 art. 641: *„Proprietarul are dreptul de a dispune de bunul său, așa cum va dori, însă în limitele stabilite de lege. El sau ea are dreptul de a obține bunul de la oricine îl deține fără drept și de a-l proteja împotriva oricărei activități nedorite."*.

[18] M. Backhoum, B. C. Gallego, M. O. Mackenrodt *et alii*, *op. cit.,* pp. 258-261. https://doi.org/10.1007/978-3-662-57646-5.

Pe de o parte, obiectul dreptului de proprietate trebuie să fie bine particularizat, determinat, iar datele cu caracter personal nu îndeplinesc această cerință. Mai mult decât atât, s-a subliniat faptul că nu se poate cunoaște cu exactitate dacă datele avute în vedere sunt cele furnizate direct de persoană sau acelea transmise către toate celelalte subiecte de drept care au primit acces la date (cu alte cuvinte, nu se cunoaște dacă avem în vedere o copie a datelor cu caracter personal sau datele își regăsesc originea în sursa principală).

Publicitatea datelor cu caracter personal reprezintă o altă critică adusă includerii acestora în sfera dreptului de proprietate. De esența datelor cu caracter personal este confidențialitatea. Acestea sunt motivele pentru care considerăm că ar trebui creată o nouă categorie de drepturi de proprietate cu privire la mediul virtual, categorie care să fie inclusă în aria stabilită de legiuitori. Cu toate acestea, o bună soluție la acest moment este includerea bunurilor digitale și a drepturilor aferente în categoriile deja cunoscute pentru a le oferi efectele necesare: avem în vedere suportul care depozitează datele, dreptul fiind legat de acest suport fizic.

La momentul în care datele sunt tratate ca obiect al unui contract, acestea vor fi analizate, mai degrabă, prin prisma conținutului acestora. Nu există la acest moment o singură definiție care să înglobeze toate sensurile aferente datelor ca obiect al contractului. Pentru o mai mare stabilitate se consideră necesar a fi cercetat conținutul datelor pentru a putea stabili cu exactitate conținutul viitorului act juridic care se va încheia. Datele sunt informații codificate *machine-readable*. La nivelul actelor încheiate între vii datele sunt incluse în sfera obiectului actului sau sunt considerate bunuri cu valoare economică[19].

Informația percepută ca un bun se remarcă prin intermediul conținutului, codului sursă și dispozitivului pe care este aceasta stocată. Astfel, informația ca bun are o anumită semnificație, fiind redată prin simboluri (biții redați prin 0 și 1) și este stocată sub o formă tangibilă, fizică (se are în vedere dispozitivul sau aplicația care stochează informațiile necesare). La momentul în care se realizează transferul datelor pe calea unui contract, de la o parte la cealaltă, vom observa modul în care sunt concepute clauzele, acestea trebuind să cuprindă semnele necesare care să descrie datele sau conținutul acestora va trebui descris de o manieră clară. Astfel, clauzele cu privire la datele personale și la transferul acestora vor trebui să stabilească cu claritate conținutul acestora și, eventual, să indice dispozitivul pe care sunt stocate sau codul de acces la aplicația de stocare a datelor necesare. De un real interes ne apar aceste trei niveluri de analiză a datelor, după cum s-a putut observa, respectiv pe cale semantică, sintactică și fizică.

Contractul va avea, astfel, un conținut digital definit prin intermediul art. 2 paragraf 11 al Directivei 2011/83/EU: „„conținut digital" înseamnă date produse și livrate în formă digitală"[20]. Pentru a putea fi considerate bunuri, datele trebuie

[19] H. Zech, *Data as Tradeable Commodity, in loc. cit.*, A. de Franceschi, *European Contract Law and The Digital Single Market. The Implications of the Digital Revolution*, Ed. Intersentia, Cambridge, 2016, p. 53.

[20] Directiva 2011/83/EU. [Online] la https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri= CELEX:3201 1L0083, accesat 4.10.2024.

să aibă o anumită utilitate[21]. În plus, modul în care vor putea fi utilizate datele va aduce cu sine posibilitatea de a include datele în sfera proprietății. În ceea ce privește posesia datelor, ca bunuri necorporale, se vor avea în vedere modurile în care s-ar putea crea o anumită exclusivitatea în ceea ce privește utilizarea lor. Astfel, această exclusivitate va putea fi acordată prin intermediul dreptului de autor sau al brevetului de invenție. Cu alte cuvinte, soluția pentru a trata datele ca pe un obiect al actelor încheiate între vii se poate găsi în sfera proprietății intelectuale: brevetul limitează utilizarea informației, dar nu și accesul la aceasta, iar dreptul de autor reduce accesul la datele create în temeiul algoritmilor și calculelor[22]. Același drept de proprietate va acorda deținătorului posibilitatea de a distruge datele respective sau de a le transfera.

Actele juridice încheiate *inter vivos* pot avea în vedere modalitatea în care este oferit accesul la informațiile din datele create. Aceste contracte vor răspunde mai multor întrebări dintre care cele mai relevante apar ca fiind „Cine are acces la datele care fac obiectul contractului?", „Care sunt datele la care va avea acces partea contractuală vizată?", „Care este perioada de timp pentru care se acordă accesul la datele descrise prin contract?". Accesul la date va oferi părții contractante beneficiare posibilitatea de a copia datele, de a le cerceta conținutul sau de a le include pe un suport separat și a le transmite către terțe persoane bine determinate. De un real interes ne apar ca fiind contractele mai bine caracterizate, respectiv acelea care oferă accesul la date exclusiv anumitor persoane, cu condiția ca datele să nu fie distribuite, să fie păstrate secrete. În acest context ne întrebăm ce formă juridică sau ce concept ar putea fi alăturat datelor pentru ca acestea să poată fi „traduse" din punct de vedere juridic. Problema vizată este, în principal, rezolvată prin intermediul clauzei de confidențialitate deoarece datele vor putea fi percepute ca un secret de comerț, ocrotit de către diferitele companii. Cu toate acestea, o atare clauză nu oferă o exclusivitate în folosirea datelor și nu stabilește o protecție împotriva oricărui tip de utilizare a datelor de către terțele persoane[23].

Datele cu caracter personal pot face obiectul unui contract și să fie incluse în sfera know-how-ului care poate fi corotit de o manieră parțială prin intermediul clauzei de confidențialitate, dar și cu ajutorul dreptului de proprietate deoarece datele pot avea un conținut economic care să determine stabilirea unor prejudicii mai mari în caz de încălcare a regulilor stabilite prin contract. Cu alte cuvinte, unei clauze de confidențialitate îi va fi alipită o clauză penală bine determinată în raport cu impactul pe care l-ar avea divulgarea datelor. Nu uităm de mijloacele de ocrotire a datelor prin intermediul regulilor contractuale care stabilesc necesitate îndeplinirii obligațiilor de către părți și a respectării drepturilor aferente. Ceea ce dorim să arătăm este faptul că datele trebuie privite ca pe oricare alte bunuri deoarece, odată incluse în sfera contractuală, li se vor alipi anumite drepturi și li se vor aplica principiile efectelor specifice actului juridic. Pentru a le putea ocroti va fi putea fi utilizat inclusiv remediul executării în natură a obligațiilor deoarece

[21] H. Zech, *op. cit.*, p. 56.

[22] *Ibidem*, p. 57.

[23] H. Zech, *op. cit.*, p. 63.

acestea de pe urmă vor fi legate de utilizarea, de transferarea, de transformarea datelor.

Autorul Herbert Zech afirmă faptul că regulamentul aplicabil protecției datelor cu caracter personal ar putea fi transformat într-un act pentru protejarea dreptului de proprietate cu privire la aceste date[24]. Pe cale de consecință, aplicarea acestuia ar putea fi extinsă către sfera economică și către o uniformizare a regimului juridic al datelor în cadrul unui contract de sine stătător. Aplicarea regulilor contractuale cu privire la datele cu caracter personal va trebui să aibă în vedere și o oarecare limitare redată prin necesitatea de a ocroti persoana despre ale cărei date este vorba.

După cum se poate observa, datele cu caracter personal din cadrul actelor încheiate între vii vor putea fi ocrotite pe mai multe căi, prin alocarea unor reguli variate: regulile aplicabile dreptului de proprietate, regulile aplicabile contractului și regulile aplicabile în domeniul proprietății intelectuale.

În ceea ce privește modul în care vor putea fi transferate datele cu caracter personal vom avea în vedere Directiva 2011/83/EU privind drepturile consumatorilor care stabilește: „Conținut digital înseamnă acele date care sunt produse și livrate în formă digitală, cum sunt programele de calculator, aplicațiile, jocurile, muzica, înregistrările video sau textele, indiferent dacă sunt accesate prin descărcare sau prin flux continuu, de pe un suport material sau prin orice alte mijloace. Contractele de livrare a conținutului digital ar trebui incluse în sfera de aplicare a prezentei directive. Dacă un conținut digital este livrat pe un suport material, cum sunt CD- urile sau DVD-urile, acesta ar trebui considerat drept un bun, în sensul prezentei directive."[25]. Cu alte cuvinte, vor putea fi transferate atât datele care se află pe un suport tehnic, cât și acelea incluse în aplicații sau pe suporturi intangibile, stabilite prin intermediul Internetului. Se vorbește, astfel, despre conceptul de „Internet of Things" care presupune schimbul datelor cu ajutorul suportului conectat la Internet. Spre exemplu un senzor care să aibă în vedere datele referitoare la comportamentul persoanei cu privire la alimentele din frigider sau aplicațiile care culeg datele referitoare la alegerile vestimentare ale persoanei.

Datele cu caracter personal pot avea și rolul unei contraprestații la nivelul contractelor. Astfel, se poate solicita de aplicație o anumită cantitate de date personale din partea subiectului de drept pentru ca acesta să-i poată utiliza funcțiunile[26]. Principalul mod de ocrotire împotriva pierderii datelor este acela al stabilirii clare a conținutului datelor și oferirea consimțământului cu privire la transfer.

[24] *Ibidem*, p. 66.

[25] Directiva 2011/83/EU. [Online] la https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/ ?uri=CELEX:320 11L0083, accesat 4.10.2024.

[26] C. Twigg-Flesner, *Disruptive Technology – Disrupted Law? How The Digital Revolution affects (Contract) Law in loc. cit.,* A. de Franceschi, *European Contract Law and The Digital Single Market. The Implications of the Digital Revolution*, Ed. Intersentia, Cambridge, 2016, p. 40.

Referitor la contractele de vânzare a datelor cu caracter personal vom menționa faptul că acestea sunt valabile (nu sunt interzise prin GDPR) atâta vreme cât sunt respectate anumite standarde precum: stabilirea exactă a datelor care vor fi transmise; scopul transmiterii și fundamentul legal; modul în care au fost obținute datele cu caracter personal; perioada de timp în care va avea loc procesarea datelor și modul în care vor putea să fie exercitate drepturile astfel dobândite[27].

Alte tipuri de contracte care pot conține date cu caracter personal sunt acelea de tipul click-wrap. Astfel, datele cu caracter personal se vor regăsi la nivelul unor contracte de adeziune, partea care nu propune încheierea actului trebuind să apese butonul de acceptare a termenilor din căsuța apărută pe site-ul web accesat. În acest fel este obținut consimțământul celeilalte părți pentru transferul datelor[28].

Aspectele analizate nu au făcut decât să sublinieze diferitele forme juridice pe care datele cu caracter personal le pot lua la nivelul actelor încheiate între vii, precum și modul în care le putem ocroti: prin intermediul dreptului de proprietate, regulilor contractuale (principiul forței obligatorii a contractului jucând un rol esențial) sau proprietății intelectuale.

3. Datele cu caracter personal și protecția acestora după decesul persoanei

Întrebările pe care și le adresează subiecte de drept cel mai adesea sunt: „ce se va întâmpla cu datele și acei „coins” obținuți în jocul video?”; „cine va putea să citească mesajele de pe platforma Facebook când persoana va deceda?”; „ce se va întâmpla cu contul YouTube, cu moneda digitală Bitcoin obținută?”.

A fost creată o diferențiere a datelor cu caracter personal în funcție de originea și localizarea acestora. Mult mai ușor se stabilește situația datelor incluse pe un *memory stick,* acel obiect fiind inclus în moștenire și, prin urmare acordat, eredelui căruia i se cuvine. În cazul în care s-ar dori separarea datelor de carcasa care le include, împărțirea acestora între moștenitori ar fi una dificilă. Pentru datele transmise în mediul on-line, moștenirea digitală va căpăta o altă formă în funcție de modul în care se vor aplica sau nu regulile din materia dreptului de proprietate intelectuală. Astfel, în ceea ce privește avatarul creat de *de cujus,* videoclipurile, colajele de fotografii create și care respectă cerința originalității, vor putea face obiectul dreptului de autor, stabilindu-se, în acest fel, soarta acestora.

În ceea ce privește celelalte conturi create de *de cujus* se vor aplica regulile din materia obligațiilor civile și a contractelor. Totuși, unele companii, din dorința de a asigura o modalitate transparentă și sigură pentru transmiterea datelor

[27] B. Fiten, *What should one keep in mind whwn selling, purchasing or licensing personal data?.* [Online] la https://www.timelex.eu/en/blog/what-keep-in-mind-selling-purchasing-licensing-personal-data, accesat la 4.10.2024.

[28] R. Momberg, *Standard Terms and Transparency in Online Contracts, in loc. cit.,* A. de Franceschi, *European Contract Law and The Digital Single Market. The Implications of the Digital Revolution*, Ed. Intersentia, Cambridge, 2016, p. 192.

utilizatorilor după decesul acestora, au încercat stabilirea unor mecanisme proprii. Un bun exemplu este crearea contului inactiv de către Google, cont prin intermediul căruia se va stabili cine va putea primi acces la contul principal dacă clientul principal decedează, precum și informațiile care vor putea fi accesate ulterior. Facebook stabilește, de asemenea, instituția moștenitorului de contact care funcționează ca un *trust,* prin acordarea accesului la contul celui decedat unei persoane de încredere (persoana nu va putea să citească mesajele sau să schimbe postările)[29]. Astfel, persoana de încredere va administra datele primite în folosul unui beneficiar determinat de constituitorul transmițător.

4. Datele cu caracter personal și procesarea acestora. Modul în care sunt create și procesate datele care vor fi incluse în cadrul actelor juridice

Dacă în contextul actelor încheiate între vii, precum și în acela al moștenirii digitale, datele cu caracter personal sunt văzute din perspectiva dreptului de proprietate, transmiterea lor implicând reguli juridice și contractuale bine stabilite, într-un cadru tehnologic, acestea capătă o cu totul altă valoare. În era digitală actuală datele nu reprezintă doar o resursă personală, ci și un element esențial în dezvoltarea unor tehnologii avansate precum inteligența artificială

În era digitală actuală, caracterizată de progrese rapide în inteligența artificială (AI), preprocesarea eficientă și etică a datelor este esențială pentru dezvoltarea modelelor de învățare automată (ML). Modelele AI precum GPT-4 se bazează pe seturi de date pentru a putea reproduce într-un mod cât mai nuanțat limbajul natural, uman. Preprocesarea datelor implică un set complex de pași tehnici pentru a transforma datele brute (sub formă de text, imagini sau videoclipuri) în date utilizabile pentru instruirea modelului.

Utilizarea datelor în instruirea modelelor lingvistice (ML) este unul dintre aspectele principale ale inteligenței artificiale (AI) și ale procesării limbajului natural (PLN). Modele lingvistice precum GPT-4 sau Gemini sunt instruite pe seturi vaste de date care includ texte din diverse surse, inclusiv cărți, articole, site-uri web și rețele sociale. Această instruire, bazată pe datele de intrare primite, le permite modelelor de inteligență artificială să genereze texte, imagini sau videoclipuri să îndeplinească o gamă largă de sarcini lingvistice sau matematice. Totuși, procesul de colectare și de pregătire a datelor reprezintă o provocare întrucât atât calitatea datelor, cât și veridicitatea acestora, nu poate fi garantată.

Calitatea și diversitatea datelor utilizate pentru instruirea modelelor lingvistice sunt esențiale pentru performanța acestora. Astfel, dacă un model AI este instruit cu un set amplu de date, respectivul model va putea să învețe nuanțele limbajului, să înțeleagă contextul și să genereze texte coerente și relevante pentru utilizatori. Datele de instruire pentru modelele lingvistice includ, de obicei, o gamă largă de genuri, stiluri și subiecte pentru a se asigura că modelul poate gestiona diverse construcții și contexte lingvistice. Această diversitate ajută modelul să se

[29] M. Backhoum, B. C. Gallego, M. O. Mackenrodt *et alii, op. cit.,* pp. 262-266.

adapteze mai rapid la datele noi și care nu au mai fost procesate anterior, făcându-l mai complex și mai robust.

Datele de intrare folosite pentru instruirea modelelor lingvistice de AI provin din diverse surse, precum: extrase de pe pagini web: colecții de date textuale de pe site-uri web, bloguri și forumuri care oferă o gamă largă de utilizare a limbajului contemporan și colocvial, literatură și publicații: cărți, articole științifice și alte materiale publicate care oferă texte bine structurate și de înaltă calitate, contribuie la înțelegerea de către model a limbajului formal și tehnic; rețele sociale: postări și interacțiuni de pe platforme precum Twitter, Facebook și Reddit oferă perspective asupra limbajului informal și asupra subiectelor de actualitate; date tranzacționale: înregistrări de servicii pentru clienți, dialoguri și alte forme de comunicare tranzacțională, pot ajuta modelul de inteligență artificială să reproducă secvențe de dialog din situații practice.

Fiecare sursă contribuie la înțelegerea de către model a limbajului, a culturii și a interacțiunii umane, permițându-i să genereze răspunsuri coerente și relevante pentru contextul în care a fost folosit acesta.

Preprocesarea datelor este, de asemenea, un pas esențial în antrenarea modelelor lingvistice. Acest proces asigură formatarea adecvată a datelor pentru a putea fi utilizate de către algoritmii de învățare automată, maximizând astfel eficiența și performanța modelelor. Preprocesarea implică mai multe etape critice, fiecare având rolul său specific în pregătirea datelor pentru modelare.

În primul rând, curățarea datelor implică eliminarea „zgomotului". Acesta este reprezentat de informațiile irelevante care pot afecta negativ performanța modelului. Astfel, există mai mulți pași pentru a elimina "zgomotul" din datele folosite: eliminarea etichetelor HTML și a tag-urilor: datele extrase de pe web conțin adesea markup HTML, care trebuie eliminat pentru a evita confuziile în modelul lingvistic; îndepărtarea caracterelor speciale: caracteristicile precum simbolurile și caracterele speciale care nu adaugă valoare semantică textului sunt eliminate; gestionarea spațiilor excesive: spațiile multiple sunt reduse la un singur spațiu pentru a standardiza textul; filtrarea liniilor goale: eliminarea liniilor goale și a altor forme de zgomot care pot distorsiona reprezentarea datelor.

În al doilea rând, se poate folosi procesul de „normalizare". Acesta presupune transformarea textului într-un format consistent, facilitând astfel procesarea ulterioară. Acest proces include: conversia la litere mici („lowercasing"): toate caracterele sunt convertite la litere mici pentru a reduce variația cauzată de utilizarea inconsistentă a literelor mari și mici; standardizarea ortografică: ortografia variabilă a cuvintelor este standardizată pentru a evita confuziile (de exemplu, pentru modelele instruite în limba engleza, „color" vs. „colour").

În al treilea rând, pentru a putea pregăti datele ce urmează să servească drept „training data" pentru modelul de AI se folosește procedura de „tokenization" ce reprezintă procesul de descompunere a textului în unități mai mici numite token-uri. Token-urile pot fi cuvinte, sub-cuvinte sau caractere, în funcție de metoda de tokenizare utilizată:

a. tokenizare pe cuvinte: textul este împărțit în cuvinte individuale. Această metodă este simplă, dar poate duce la probleme cu cuvintele necunoscute (out-of-vocabulary, OOV).

b. tokenizare pe subcuvinte: tehnici precum Byte-Pair Encoding (BPE) și Sentence Piece sunt utilizate pentru a împărți cuvintele în subunități mai mici. Aceasta ajută la gestionarea cuvintelor necunoscute și reduce dimensiunea vocabularului, îmbunătățind astfel eficiența modelului.

Metoda Byte-Pair Encoding (BPE): BPE pornește cu un vocabular inițial de caractere și iterează prin combinarea celor mai frecvente perechi de caractere într-o nouă unitate, până când se atinge dimensiunea dorită a vocabularului.

Metoda Sentence Piece: o metodă de tokenizare care nu presupune separatoare explicite între cuvinte, facilitând astfel procesarea textelor în diverse limbi.

De asemenea, o altă metodă de o pregătire a datelor de intrare constă în filtrarea și selecția caracteristicilor.

- filtrarea „n-gramelor”: în funcție de necesitățile modelului de inteligență artificială antrenată, se pot genera și filtra „n-grame” (secvențe de „n” cuvinte) pentru a capta contextul local.

- selecția caracteristicilor: tehnici statistice pot fi utilizate pentru a selecta caracteristicile relevante ce trebuie antrenate, îmbunătățind, astfel, eficiența modelului.

A cincea abordare folosită în domeniul inteligenței artificiale pentru pregătirea datelor de intrare este reducerea dimensiunilor. Aceasta se poate face fie prin TF-IDF, fie prin metoda „embedding”.

TF-IDF (Term Frequency-Inverse Document Frequency): această tehnică transformă textul în reprezentări vectoriale ponderate, reflectând importanța unui cuvânt în documentul ce servește ca parte a datelor de intrare.

Embedding-uri: utilizarea embedding-urilor de cuvinte (de exemplu, Word2Vec, GloVe) pentru a transforma cuvintele în vectori denși care capturează relațiile semantice dintre cuvinte.

O ultimă metodă este regularizarea prin „oversampling” și „undersampling”. Pentru a aborda posibilul dezechilibru dintre diferite categorii de date din setul de date de intrare, se pot aplica tehnici de oversampling și undersampling.

Prin aplicarea acestor tehnici de preprocesare se asigură că datele sunt optimizate pentru antrenarea modelelor lingvistice, îmbunătățind, astfel, acuratețea și eficiența acestora.

Adăugarea de zgomot în datele folosite pentru instruirea unui model AI poate ajuta la îmbunătățirea complexității modelului. Tehnici precum augmentarea datelor, instruirea adversarială și introducerea intenționată a zgomotului pot produce variații controlate în datele de intrare, ajutând modelele să învețe să ignore variațiile minore și să se concentreze pe aspectele cele mai relevante.

Pentru modelele lingvistice, augmentarea datelor ar putea implica tehnici precum înlocuirea unor cuvinte cu sinonimele lor, traducerea inversă sau adăugarea de mici erori tipografice. Aceste metode pot simula dialogul cu un utilizator uman și pot îmbunătăți capacitatea modelului de a înțelege și de a genera text în condiții diverse.

Din perspectiva instruirii adversiale, aceasta implică adăugarea intenționată de exemple neobișnuite în setul de date de instruire. Pentru modelele lingvistice, aceasta ar putea însemna construirea de propoziții care sunt corecte din punct de vedere gramatical, dar greșite din punct de vedere semantic, ajutând modelul să învețe să se concentreze pe conținutul semnificativ.

Adăugarea de zgomot direct în datele de intrare (de exemplu, omiterea cuvintelor, schimbarea cuvintelor sau introducerea de cuvinte aleatorii) poate îmbunătăți capacitatea modelului lingvistic de a genera răspunsuri. Principala problemă la această metodă este faptul că trebuie ca nivelul de zgomot să nu depășească un anumit prag astfel încât să se îmbunătățească capacitatea modelului de a distinge sensul datelor primite fără a afecta semnificativ capacitatea acestuia de a învăța din ele.

Din perspectivă juridică, un important aspect este păstrarea confidențialității. Pentru a ne asigura confidențialitatea datelor ne putem folosi de doua metode: confidențialitatea diferențială și învățarea federată.

Confidențialitatea diferențială introduce zgomot în date în timpul procesului de instruire pentru a împiedica modelul să memoreze detalii specifice despre orice cumul de date individual. Prin aceasta tehnică este asigurat faptul că modelul instruit nu dezvăluie în mod neintenționat informații private.

Învățarea federată constă în instruirea modelelor de inteligență artificială pe mai multe dispozitive descentralizate sau servere, unde setul de date locale rămâne pe dispozitivele respective, dar odată ce procesul de instruire al modelului ia sfârșit, versiunea stabilă a sa este partajată, fără a mai avea acces la datele de intrare folosite anterior, reducând astfel riscul de expunere a unor date confidențiale.

Concluzii

Intersecția dintre inteligența artificială, datele și etică prezintă o provocare amplă pentru societatea modernă. Recunoscând datele ca obiect juridic cu valoare economică și personală semnificativă, putem naviga în mod responsabil în complexitatea moștenirii digitale, confidențialității și dezvoltării AI. Calea de urmat necesită un efort concertat din partea legislatorilor, inginerilor software și a societății în general pentru a se asigura că viitorul digital este atât inovator, cât și bazat pe aspecte etice.

Încurajarea dezvoltării etice a AI implică încurajarea unei culturi a practicilor etice în cercetarea și implementarea AI. Aceasta include prioritizarea echității, transparenței și consimțământului utilizatorului. Îmbunătățirea securității datelor implică implementarea unor măsuri avansate de protecție împotriva încălcării datelor și a accesului neautorizat la informațiile confidențiale. Încurajând un mediu de transparență, responsabilitate și îmbunătățire continuă, putem valorifica capacitățile inteligenței artificiale pentru a aduce beneficii societății.

Referințe

Abadi M., Chu A., Goodfellow I., McMahan H. B., Mironov I., Talwar K., Zhang L. (2016). Deep Learning with Differential Privacy.

Backhoum M., B. C. Gallego, M. O. Mackenrodt *et alii*, *Personal Data in Competition, Consumer Protection and Intellectual Property Law. Toward a Holistic Approach?, in MPI Studies on Tellectual Property and Competition Law 28*, Springer, Berlin, 2018, https://doi.org/10.1007/978-3-662-57646-5.

Boroi G., C.A. Anghelescu, B. Nazat, *Curs de drept civil. Drepturile reale principale*, Ed. Hamangiu, București, 2013, pp. 16-17.

Chawla N. V., Bowyer K. W., Hall L. O., Kegelmeyer W. P. (2002). SMOTE: Synthetic Minority Over-sampling Technique.

Custers B., Alan M. Sears, F. Dechesne *et alii, EU Personal Data Protection in Policy and Practice, in* S. van der Holf, *et. alii., Information Technology and Law Series, vol. 29,* Ed. T.M.C. ASSER PRESS, Haga, 2019, pp. 153-173. https://doi.org/10.1007/978-94-6265-282-8.

Fadaee M., Bisazza A., Monz C. (2017). Data Augmentation for Low-Resource Neural Machine Translation.

Franceschi A. de, *European Contract Law and The Digital Single Market. The Implications of the Digital Revolution*, Ed. Intersentia, Cambridge, 2016.

Kudo T., Richardson J. (2018). SentencePiece: A Simple and Language Independent Subword Tokenizer and Detokenizer for Neural Text Processing.

McMahan B., Moore E., Ramage D., Hampson S., Arcas B. A. (2017). Communication-efficient Learning of Deep Networks from Decentralized Data.

Mikolov T., Chen K., Corrado G., Dean J. (2013). Efficient Estimation of Word Representations in Vector Space.

Miyato T., Dai A. M., Goodfellow I. (2017). Adversarial Training Methods for Semi-Supervised Text Classification.

Momberg R., *Standard Terms and Transparency in Online Contracts, in loc. cit.,* A. de Franceschi, *European Contract Law and The Digital Single Market. The Implications of the Digital Revolution*, Ed. Intersentia, Cambridge, 2016.

Naef T., *Data Protection without Data Protectionism. The Right to Protection of Personal Data and Data Transfers in EU Law and International Trade Law, in loc. cit.,* Marc Bungenberg, Christoph Herrmann, Markus Krajewski, et. alii., *EYIELMonographs-StudiesinEuropeanandInternationalEconomicLaw*, Vol. 28, Springer, 2021, p. 30. https://doi.org/10.1007/978-3-662-57646-5.

Radford A., Wu J., Child R., Luan D., Amodei D., Sutskever I. (2019). Language Models are Unsupervised Multitask Learners.

Rajaraman A., Ullman J. D. (2011). Mining of Massive Datasets.

Sennrich, R., Haddow, B., & Birch, A. (2016). Neural Machine Translation of Rare Words with Subword Units.

Twigg-Flesner C., *Disruptive Technology – Disrupted Law? How The Digital Revolution affects (Contract) Law in loc. cit.,* A. de Franceschi, *European Contract Law and The Digital Single Market. The Implications of the Digital Revolution*, Ed. Intersentia, Cambridge, 2016.

Warren S.D., L. D. Brandeis, *The Right to Privacy, in Harvard Law Review*, Vol. IV, decembrie 1890, [Online]

Zech H., *Data as Tradeable Commodity, in loc. cit.,* A. de Franceschi, *European Contract Law and The Digital Single Market. The Implications of the Digital Revolution*, Ed. Intersentia, Cambridge, 2016.

Analele Ştiinţifice ale Universităţii „Alexandru Ioan Cuza" din Iaşi
TOM LXX, 2, Ştiinţe Juridice, 2024

DOI: 10.47743/jss-2024-70-2-8

The European Battle for Data in Tax Administration: Balancing Innovation and Compliance

Laura-Elena IONAȘCU (POSTOLACHE)[1]

Abstract: The development of Blockchain technology in recent years has underscored the need for legislative harmonisation through the creation of specific regulations at the level of the European Union. This technology has opened new doors to tax fraud and tax evasion activities in the tax field. As a response, the battle for data took the form of Council Directive (EU) 2023/2226 amending Directive 2011/16/EU on administrative cooperation in the field of taxation. The cost of ensuring transparency in this area falls on Crypto-Assets service providers, who are now required to collect and report more data to Member States. Through the fiscal cooperation mechanism, the tax authorities access to users' data is extensive, legitimised only by the interest to assure proper taxation and the security of the European Union`s internal market. In this context, this study aims to outline an overview of the data collected for tax purposes within the Blockchain sector and the obligations of the involved parties.

Keywords: data, Blockchain, crypto, tax administration, DAC8, Crypto-Asset Service Provider, Crypto-Asset Operator, reporting obligations, administrative cooperation.

Introduction

In recent years, the accelerated development of technology and the Internet has both simplified and complicated our lives through the mechanism of data processing. Since a few years ago, in the legal literature[2], it was reported that access to data has become easier and more convenient than ever. Additionally, it has created a new boundless market of data, once the efficiency of data transfer and exchange has increased. At present, data is everywhere and everything, and in our perspective, it might be considered the ”new gold” of our society.

In the taxation realm, data can be gathered from various sources, including public authorities and institutions, financial institutions, such as banks, as well as from private entities and individuals, through personal transactions, earnings, and expenditures. For tax administration, tax data processing can enhance the

[1] PhD Student, „Alexandru Ioan Cuza" University of Iași, Law Faculty, e-mail: laurapostolache@outlook.com.

[2] C.T. Ungureanu, *Personal data protection in international contracts*, in Analele Științifice ale Universității „Alexandru Ioan Cuza" Iași, tomul LXIII, Științe Juridice, 2017, nr. II, pp. 135-154.

effectiveness and promptitude of tax collection. Supplementary, it might play a significant role in the proper identification of fraudulent activities. Reflecting on the crucial role of data and the new challenges raised by the technology blockchain, it is essential to identify new legal approaches to regulate the evolving taxation field.

The present paper aims to examine the response of the EU legislator on the question of accessibility and transparency of data for tax authorities and the fiscal impact of it on the actors of blockchain[3]. First, we will delve into a brief exploration of the meaning of the term ”data” in the EU legislation and its nuances in different contexts. Also, we will try to determine the significance of data collection and processing, seeking to understand their role in the realm of taxation. Subsequently, we will analyse in depth the parties affected by the new regulations in crypto-markets and we will evaluate the rights and the obligations related to data reporting imposed on them. Furthermore, our goal is to critically scrutinise the compliance of the new provisions with human rights as protected by the EU Charter of Fundamental Rights.

I. A journey of a thousand miles begins with a single... data[4]

The fundamental role of data in shaping our future was highlighted by the European Commission in 2020 when it promoted a strategy on data for the European Union[5]. In its perspective ”Data is the lifeblood of economic development: it is the basis for many new products and services, driving productivity and resource efficiency gains across all sectors of the economy, allowing for more personalised products and services and enabling better policy making and upgrading government services.”[6]

The new dimensions of data collection and utilisation in our society have emphasised the necessity to increase the attention granted to this law area, in order to develop fair and transparent regulations. At the European Union level, this situation has led firstly, to the elaboration of a Regulation aimed at protecting personal data, known as Regulation (EU) 2016/679 of the European Parliament and of the Council 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

[3] In this context, we aim to analyse the approach of the European Union on this subject matter. Therefore, we will not delve into the analysis of the provisions of our national legislation. The present study addresses a theoretical perspective of the use and exchange of data by tax authorities in the European Union, in the context of the new technologies of blockchain.

[4] Reference to the well-known quote of Lao Tzu: “A journey of a thousand miles begins with a single step.”

[5] European Commission, *A European strategy for data,* Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the regions, COM/2020/66 final, 19 February 2020.

[6] *Idem*, p. 2.

95/46/EC (General Data Protection Regulation)[7]. This was the first step of prominent protection of this right, aligned with Article 8 of the European Union Charter of Fundamental Rights[8], titled ”Protection of personal data”.

The European Union has prioritised this right in every regulation with impact in this area, adopting new legal instruments to enhance the protection granted. The most important ones are the Regulation (EU) 2018/1807 of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European Union, the Regulation (EU) 2019/881 of the European Parliament and of the Council on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) 526/2013 (Cybersecurity Act), and the Directive (EU) 2019/1024 of the European Parliament and of the Council on open data and the re-use of public sector information.

Recently, the emergence of blockchain and its tokens has imposed a new and more active approach. For our present study, we will examine the dispositions of Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets.

To do this, we should respond firstly to the question: what is this element known as “data”? The term ”data” is defined in the dictionary as ”information, especially facts or numbers, collected to be examined and considered and used to help decision-making, or information in an electronic form that can be stored and used by a computer”[9]. In the European legal framework, we identify a comprehensive definition of this term in the provisions of Article 2 of the Regulation (EU) 2022/868 of the European Parliament and of the Council on European data governance. In this context, the term ”data” is defined as ”any digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audiovisual recording;”[10]. Surprisingly or not, this provision restrains the general meaning only to "digital" elements, excluding the physically written data.

On the other hand, as we already said, the European legislator has given particular attention to a specific category of data, respectively, the “personal data”[11]. Although there is no definition of data in general, in the Regulation (EU) 2016/679, the expression “personal data” is defined as “any information relating to an identified or identifiable natural person (data subject)”. Also, this regulation emphasises a clarification on the phrase "identifiable natural person” considered as “one who can be identified, directly or indirectly, in particular by reference to an

[7] OJ, L series, no. 119, 4 May 2016.

[8] OJ, C series, no. 326, 26 October 2012.

[9] Definition of data from the Cambridge Advanced Learner's Dictionary & Thesaurus, Cambridge University Press, accessed online at the link: https://dictionary.cambridge.org/dictionary/english/data.

[10] Article 2, paragraph 1 of the Regulation (EU) 2022/868.

[11] C.T. Ungureanu, *Legal remedies for personal data protection in European Union,* in „Logos, Universality, Mentality, Education, Novelty”. Section: Law 6.2, 2018, pp. 26-47.

identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".

In tax regulations, we would rather encounter the term "information" than "data", but the meaning is the same. Tax authorities gather data about taxpayers within the procedures they carry out, the ultimate goal being to increase the efficiency of the administration and to limit fraud activities. To achieve this objective, at the European level, the mutual exchange of data is regulated as a form of administrative cooperation in fiscal matters, through the Council Directive 2011/16/EU on administrative cooperation in the field of taxation and repealing Directive 77/799/EEC[12].

The Directive's text is unspecific regarding the definition of the term "information" and does not provide a specific list of the data considered. However, the provisions of Article 1 furnish some guidance on this matter, stating that it includes "information that is foreseeably relevant to the administration". The broad interpretation of this term is intentionally chosen and also expected in this context since eventually, any definition could narrow the scope of the regulation application in ways that would be detrimental to the national interests of the Member States in fiscal matters.

Despite this manifest general nature of the regulation, the Directive indicates several ways in which the targeted information can be transferred, highlighting the ”exchange of information on request”, the ”automatic exchange”, and also a form of ”spontaneous exchange”[13]. These provisions offer a more comprehensible approach to the data concerned, stating, for example, that the "automatic exchange" concerns "all information that is available concerning residents of that other Member State, on (...) specific categories of income and capital".

In consequence, the term "information", in the context of this Directive, encompasses both personal data and non-personal data. The result is a cumulative application of provisions from the two fields of data protection, respectively Regulation 2016/679 and Regulation 2018/1807. In this situation, according to Article 2 of Regulation 2018/1807: "In the case of a data set composed of both personal and non-personal data, this Regulation applies to the non-personal data part of the data set. Where personal and non-personal data in a data set are inextricably linked, this Regulation shall not prejudice the application of Regulation (EU) 2016/679".

II. Blockchain, a new realm to be conquered by tax regulations?

In response to the power and the control of the state in the economic sphere, humans began to seek a new payment system that could operate

[12] OJ, L series, no. 064, 11 March 2011.

[13] Article 3 of the Council Directive 2011/16/EU.

independently of government supervision[14]. The impact of money devaluation and the economic crisis that began at the end of 2007, along with the general decrease of public trust in financial institutions[15] have transformed this desire into a necessity.

The cryptocurrency system is based on distributed ledger technology. To secure the transactions and to ensure the transparency of the process, the contracts are recorded and verified across a large number of interconnected nodes, a fact that could abolish the interaction with other central authorities[16].

In consequence, we can say that the blockchain is built under the idea of a „new world" that is free from state control and intervention, where users are treated as „gods" in their actions. The main attractions include the decentralisation and autonomy of this system, as well as the advantages of conducting transactions using smart contracts and the inherent confidentiality of the system.

Given the relatively recent introduction of blockchain technology into our society, regulations at the European level emerged with some delay. The member states attempted to manage the legal aspects of the new technology in their own manner, applying the legal frameworks available already in their legislations[17] or developing various approaches in each member state.

The situation was changed once adopted Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937[18]. Since the advancement of these technologies represented a real trend back then at the European level, this regulation, known also as MiCA has clarified the legal definitions of the terms concerned and also the dimensions of the impact and effects of these technologies on our society.

The complexity and the ramifications of this act in this field offer us a glimpse of the laborious work of the EU legislator. It's important to note that the regulation proposal[19] was initiated in 2020, as a part of the Digital Finance package. However, the current version has faced extensive discussions and multiple

[14] O. Dragomir, *Criptomonedele şi tehnologiile aferente acestora*, in Revista Română de Drept al Afacerilor, no. 3, 2021, online access at. https://sintact.ro/#/publication/151022852?keyword=cripto&cm=SREST

[15] D. M. Ilucă, *Regulating Bitcoin. Legal aspects regarding the use of Bitcoin,* in "Alexandru Ioan Cuza" University Annals, Tome LXIII, Legal sciences series, supplement, no. II, Iași, 2017, p. 312.

[16] V. Benson, B. Adamyk, A. Chinnaswamy, O. Adamyk, *Harmonising cryptocurrency regulation in Europe: opportunities for preventing illicit transactions,* in European Journal of Law and Economics, no. 57, 2024, p. 38, online access at: https://doi.org/10.1007/s10657-024-09797-w.

[17] *Ibidem.*

[18] OJ, L series, no. 150, 9 June 2023.

[19] Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937, COM/2020/593 final, Brussels, 24 September 2020.

amendments, illustrating a nuanced understanding of the subject matter. At this time, the legal framework is a comprehensive one, including the representation of the actors in this market and emphasising on their rights and obligations.

From the perspective of the present study, we should consider the main definitions of this topic, respectively ”crypto-asset” and „crypto-asset service provider”. From a practical point of view, the elaboration of specific definitions has encountered many impediments caused by the various interpretations of these terms in Member States, often being interchangeable and creating legal uncertainty[20].

However, the European legislator decided on a final interpretation of this syntagma; according to its meaning, a ”crypto-asset” is seen as “a digital representation of a value or of a right that is able to be transferred and stored electronically using distributed ledger technology or similar technology”. A new element was the definition of the ”crypto-asset service provider” (CASP) which is defined as “a legal person or other undertaking whose occupation or business is the provision of one or more crypto-asset services to clients on a professional basis, and that is allowed to provide crypto-asset services in accordance with Article 59”.

As regards the crypto-asset service providers, according to this definition, they are not limited to only legal persons; any other entity that provides a crypto-asset service with character of continuity and pursuing a professional objective will be qualified as a CASP. Also, MiCA has imposed new obligations for licence requirements for CASPs to coordinate their statute in the Member States and secure these transactions on the internal market[21]. However, this regulation does not imply obligations in the taxation field for them.

Therefore, from a tax perspective, this new technological conquest and the income generated in this way should represent the object of taxation. To achieve this goal, tax authorities required access to the transaction and income data of the persons involved in the crypto trade. Challenges arose due to the cross-border nature of the trading process and the anonymous characteristic of the participants[22]. When the trading activities take place within the same country, tax authorities can more easily access the data involved, compared to the situation when the provider and the client are located in different jurisdictions.

[20] V. Benson, B. Adamyk, A. Chinnaswamy, O. Adamyk, *op.cit.*, p. 39.

[21] O. Dragomir, *Propunerea de Regulament privind pieţele criptoactivelor şi de modificare a Directivei (UE) 2019/1937*, in Revista Română de Drept al Afacerilor, no. 3, 2022, online acces at: https://sintact.ro/#/publication/151025536?keyword=cripto&cm=SREST.

[22] To become a part of the ”chain” and to participate in the peer-to-peer network, it is not necessary to register. The procedure implies simply the download of the software, a method that grants access to everybody to participate, regardless of the loci of the neophyte. Moreover, the system does not request any identification data; in consequence, the participants can choose a pseudonym. More information about the mechanism of the blockchain in T. van der Linden, T. Shirazi, *Markets in crypto-assets regulation: Does it provide legal certainty and increase adoption of crypto-assets?*, in Financial Innovation, 9(1): 22. https://doi.org/10.1186/s40854-022-00432-8

Moreover, under the terms of the Directive 2011/26/EU, the majority of crypto-assets are exempt from the reporting requirements stipulated by the Directive due to their non-conformance with the criteria associated with funds held in depository accounts or their classification as financial assets. Furthermore, entities operating within the crypto market, such as crypto-asset service providers and operators, have fallen outside the scope of the definition of a financial institution under Directive 2011/16/EU[23].

In this context, without access to this type of data for tax authorities, the taxpayers could easily commit tax evasion[24]. Being unable to seek the transactions realised, manifested usually as speculative trading or payment of goods and services in cryptocurrencies[25], the authorities (the absent creditor[26]) stay unaware of the participants in the crypto realm. Also, this state of affairs could easily offer new dimensions to money laundering and several other crimes[27].

In consequence, a straightforward and feasible solution was to create a regulation that imposed cooperation among Member States on the exchange of specific information on crypto trading. In addition, to obtain access to this data, it was necessary to implement a new set of obligations for the crypto-assets service providers. According to this objective they had become an intermediary and a connection between clients (seen as a subject of taxation) and tax authorities.

III. A new milestone for tax data: DAC 8

With the aim to create a more fair and transparent market, on 17 October 2023, it was adopted the Council Directive (EU) 2023/2226 amending Directive 2011/16/EU on administrative cooperation in the field of taxation[28]. From the historical legislative perspective, this act represented the seventh amendment to the Administrative Cooperation Directive, a fact that has attracted the appellation „DAC 8".

Considering the almost simultaneous adoption of the two normative acts, their terms are coordinated to avoid excessive administrative burdens for CASPs[29]. However, DAC8 covers a more diversified range of subjects that are requested to offer data to tax authorities, compared to MiCA.

Regarding the reporting obligation, the directive established in Annex III, Section IV, the crypto-assets whose trading must be reported by the service provider. For this purpose, they are covered by the term "Reportable Crypto-Asset" which means "any Crypto-Asset other than a Central Bank Digital Currency,

[23] Statement of reasons for the Directive 2023/2226, point 10.

[24] A. Brodzka, *" The future of automatic tax information exchange in EU countries*", in US-China Law Review, vol. 12, 2005, pp. 352-363.

[25] D. M. Ilucă, *op. cit.* p. 317.

[26] I.M. Costea, "*Taxing forms in the digital environment",* SHS Web of Conferences, no. 177, Legal perspectives on the Internet, COPEJI 6.0., 2023, p. 6

[27] V. Benson, B. Adamyk, A. Chinnaswamy, O. Adamyk, *op. cit.*, p. 39.

[28] OJ, L series, no. 2023/2226, 24 October 2023.

[29] Statement of reasons for the Directive 2023/2226, point 7.

Electronic Money, or any Crypto-Asset for which the Reporting Crypto-Asset Service Provider has adequately determined that it cannot be used for payment or investment purposes”. We notice that this definition is a general one, the Council of the European Union preferring to expressly exclude elements that have some similarities with cryptocurrency (regarding their digital nature), leaving also room for other new technologies that could be developed in the following years.

On a legal basis, the approaches proposed in this new regulation follow the line established by the Organisation for Economic Co-operation and Development in its guidelines, entitled the “Crypto-Asset Reporting Framework" (CARF)[30], as well as the requirements imposed by the amendments to its Common Reporting Standard[31].

“The Battle for Tax Data'' is therefore set in the digital environment between three main characters: the Member States, the Reportable Crypto-Asset Service Providers, and the relevant taxpayers/clients. But how does this regulation affect their behaviour, and what is their final goal?

Between the clarifications brought by the new amendments, the Directive currently comprises some new definitions of its terms in the strict interpretation of this act. In this background, the term “client” has another form than in the MiCA, the scope being a harmonised interpretation of the three mentioned subjects' special characteristics. In the context of this Directive, it refers to ”any intermediary or relevant taxpayer that receives services, including assistance, advice, counsel or guidance, from an intermediary subject to legal professional privilege in relation to a reportable cross-border arrangement.”

On the other hand, the term “Reporting Crypto-Asset Service Provider” means ”any Crypto-Asset Service Provider and any Crypto-Asset Operator that conducts one or more Crypto-Asset Services effectuating Exchange Transactions for or on behalf of a Reportable User”. The difference between a Crypto-Asset Service Provider and a Crypto-Asset Operator is given by the MICA, an act that establishes the background for the first term. In this context, a “Crypto-Asset Service Provider” will be identified in accordance with the dispositions of Article 3(1), point (15), of Regulation (EU) 2023/1114[32]. Meanwhile, a “Crypto-Asset Operator” is any other provider of Crypto-Asset Services not regulated under this act, respectively, it covers the entities located in jurisdictions outside of the

[30] OECD, *Crypto-Asset Reporting Framework and Amendments to the Common Reporting Standard*, Paris, 2022,https://www.oecd.org/tax/exchange-of-tax-information/crypto-asset-reporting-framework-and-amendments-tothe-common-reporting-standard.htm.

[31] Statement of reasons for the Directive 2023/2226, point 9, grants express references to the interpretations offered by the legal framework proposed by OECD.

[32] According to the MICA, (15) a ‘crypto-asset service provider’ represents ”a legal person or other undertaking whose occupation or business is the provision of one or more crypto-asset services to clients on a professional basis, and that is allowed to provide crypto-asset services in accordance with Article 59”.

European Union borders. Also, a CAO will be any other entity that provides crypto services but is regulated under other acts than MICA.

The ”Reportable user” remains always a Crypto-Asset User[33], who is also a Reportable Person[34] resident in a Member State. In this case, to correctly identify it, the two definitions have to be corroborated, resulting that the reportable user being understood as a client/consumer of a Reporting Crypto-Asset Service Provider involved in Reportable Transactions being either an individual, an Entity, or an estate resident in a Member State, apart from the Excluded Persons.

Regarding the ”excluded persons”, this category is expressly determined in the same annex, and it refers to: ”(a) an Entity the stock of which is regularly traded on one or more established securities markets; (b) any Entity that is a Related Entity of an Entity described in point (a); (c) a Governmental Entity; (d) an International Organisation; (e) a Central Bank; or (f) a Financial Institution other than an Investment Entity”. This enumeration encompasses especially the entities which are already strongly regulated in the field of exchange of information for tax purposes.

Nonetheless, it provides the general definition for a “Controlling Persons”, which according to this text represents the natural persons who exercise control over an Entity.

IV. An overview of the new obligations for RCASPs and Member States

DAC 8 extends the cooperation between Member States on fiscal matters, offering the possibility of exchanging data received from RCASPs. For this purpose, a new article was added, which specifies the ”scope and the conditions of

[33] According to the Directive, a Crypto-Asset User represents ”an ”individual or Entity that is a customer of a Reporting Crypto-Asset Service Provider for the purpose of carrying out Reportable Transactions. An individual or Entity, other than a Financial Institution or a Reporting Crypto-Asset Service Provider, acting as a Crypto-Asset User for the benefit or account of another individual or Entity as agent, custodian, nominee, signatory, investment advisor, or intermediary, is not treated as a Crypto-Asset User, and such other individual or Entity is treated as the Crypto-Asset User. Where a Reporting Crypto-Asset Service Provider provides a service effectuating Reportable Retail Payment Transactions for or on behalf of a merchant, the Reporting Crypto-Asset Service Provider shall also treat the customer that is the counterparty to the merchant for such Reportable Retail Payment Transactions as the Crypto-Asset User with respect to such Reportable Retail Payment Transaction, provided that the Reporting Crypto-Asset Service Provider is required to verify the identity of such customer by virtue of the Reportable Retail Payment Transaction pursuant to domestic anti-money laundering rules”.

[34] In this context, “Reportable Person” means” a Member State Person other than an Excluded Person.” Special attention should be accorded to the term “Member State Person” which refers not solely to ”an Entity or individual that is resident in any Member State under the tax laws of that Member State”, but also could be represented by ”an estate of a decedent that was a resident of any Member State”.

mandatory automatic exchange of information reported by RCASP". The newly added Article 8ad set in paragraph 3 the data concerned by this mechanism. Each Member State shall exchange this information within a term of "nine months following the end of the calendar year to which the reporting requirements applicable to Reporting Crypto-Asset Service Providers relate"[35]. Starting from 1 January 2026, the information shall be communicated for the relevant calendar year or other appropriate reporting period[36].

The directive also institutes new legislative obligations for the Member States. They are required to take new and appropriate measures in order to accomplish the registration of the RCASP and to ensure their compliance with the reporting obligations.

The RCASPs, on the other hand, should comply with a new set of obligations in this field. The directive established mainly for CASPs and CAOs a responsibility which has two components: a due diligence obligation manifested in their procedures of collecting data, and also an obligation to attain a predetermined result regarding the communication of the relevant data to tax authorities.

First, we will examine the obligation to collect the data from Reportable Users. To establish if a Crypto Asset User is a Reportable User, the RCASP should obtain a "self-certification" from him, to determine his fiscal residency[37]. Moreover, it includes an obligation of due diligence, because the RCASPs should verify the "reasonableness" of this certification, to assure, based on his information and any other relevant information it could access, the validity of it[38]. In the same way, it has to determine and verify the Controlling Persons of the Entity Crypto-Asset User.

Second, it has to inform the tax authorities of the data trading realised through their means. For the Crypto-Asset Operators (CAOs) not regulated under MiCA, the obligation is considered satisfied if they inform the tax authorities of the Member State where it is a resident for tax purposes[39]. In its absence, it could inform the Member State where it is incorporated and has to file tax returns regarding its income[40]. Lastly, it could be the Member State from where it is managed, or where it has its regular place of business[41]. For CASPs, the report is requested in front of the competent authority of the Member State of registration (where they have obtained its MiCA authorisation)[42].

Among the mandatory information to be communicated by CASPs are listed the name and the address, any TIN issued to it, and the Member States in

[35] Article 1, paragraph 6, point 6 of the Council Directive (EU) 2023/2226.

[36] *Ibidem.*

[37] Annex III, Section III, point A of the Council Directive (EU) 2023/2226.

[38] *Ibidem.*

[39] M. Bernt, *DAC8: Commentary on the European Union's New Crypto Tax Reporting Regime,* in European Taxation, 2023, p. 383.

[40] *Ibidem.*

[41] *Ibidem.*

[42] D. Post, C. Cipollini, *The DAC8 Proposal and the Future of Crypto-Asset Reporting: Some Preliminary Thoughts* in Kluwer International Tax Blog, 09 February 2023, p. 2.

which Reportable Users are residents[43]. In case of non-compliance, RCASPs will receive a reminder from the Member State of a single registration. Acquiring two reminders, but not before the expiration of 60 days, attracts sanctions for the operator, which will be prohibited from performing reportable transactions, and also penalties according to the legislation of each Member State[44].

Secondly, it involves an obligation for Member States to exchange information in this field to surpass the difficulties raised by the international characteristic of this trading within the European Union. In this phase, the designated national authority of the Member State which receives the data is compelled to communicate the information about the users to the Member States for their tax residency, to be verified.

V. The costs for fair taxation in the Blockchain realm

Nowadays, the presence of technology, digitalization, and the Internet in our lives is indisputable. We have analysed the involved parties regarding the new regulation on administrative cooperation in tax matters related to cryptocurrency. We have also noted new obligations in their responsibilities, which play a role in regulating and creating a safer and fairer blockchain network. This leads us to the question: Could collecting, using, and processing data in the tax field be harmful in some ways?

In this context, it would be a legitimate question if the RCASPs` obligation to report the transaction could represent to some extent an attempt to others' rights protected by the European acquis.

Firstly, the collecting and the exchange of data could raise difficulties and may be seen as an infringement of the right to the protection of personal data, protected under Article 8[45] of the Charter of Fundamental Rights. The European Data Protection Supervisor (EDPS) has presented a point of view on the new regulation, considering that the new rules comply with the GDPR[46].

In this respect, the text of the Directive establishes a maximum period in which the obtained data can be kept, namely five years[47]. At the same time, to avoid

[43] *Ibidem.*

[44] Annex III, Section V, paragraph A, point 2 of the Directive EU 2023/2226.

[45] The legal text, entitled ”Protection of personal data” states that ”1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority”.

[46] The European Data Protection Supervisor (EDPS), Opinion 6/2020 on a proposal for an amendment of Council Directive 2011/16/EU relating to administrative cooperation in the field of taxation, 28 October 2020, https://www.edps.europa.eu/data-protection/our-work/publications/opinions/edps-opinion-proposal-amendment-council-directive_en

[47] Article 1, paragraph 11, point 3 of the Council Directive (EU) 2023/2226.

the use of data for other purposes than those expressly provided for, new rules have been established for this scope.

The Member States are supposed to deal with this data under the obligation of official secrecy, offering in this way more guarantees of its protection. Also, in order to assure the safety of the automatic exchange between Member States, by 31 December 2026, the Commission is tasked with the responsibility of creating and providing a secure central register that contains information about how Member States are collaborating administratively in the area of taxation[48].

Moreover, according to the DAC8, the Member States could use the data ”for the assessment, administration, and enforcement of the national law of Member States concerning the taxes referred to in Article 2 (a.n. of the Directive 2011/16/EU[49]) as well as VAT, other indirect taxes, customs duties, and anti-money laundering and countering the financing of terrorism”. In fact, the provisions in discussion set a broad framework for the use of data gathered, to ensure not only an improved collection of taxes, but also to encourage and support the fight against tax fraud and tax evasion.

Furthermore, it offers Member States the possibility to disseminate the data to a Third Member State. If the Second Member State considers that the information would be useful in taxation scope to another State, it could communicate this data accordingly with the procedure determined under the Directive 2011/16/EU[50]. First Member State could oppose the communication of the information, by a response in this matter within 15 calendar days.

On the other hand, DAC 8 addresses specific discussions for the private sector and the administrative burdens it faces, for RCASPs to comply with the due diligence and reporting obligations it sets[51].

For small businesses, the resources necessary to obtain the requested data and to transfer it to the tax authorities could represent an obstacle ahead to the freedom to conduct a business. For instance, this right is protected under article 16 of the European Chart of Human Rights which specifies that ”The freedom to conduct a business in accordance with Union law and national laws and practices is recognised.”

Regarding this aspect, it is important to emphasise that the above mentioned articles are not an absolute right. In accordance with the article 52 of the Charter of Fundamental Rights, protection of personal data and the freedom to conduct a business could be the subject to some limitations[52].

[48] M. Bernt, *op. cit.*, p. 383.

[49] Article 2 paragraph 1 of the Directive 2011/16/EU provides that ”This Directive shall apply to all taxes of any kind levied by, or on behalf of, a Member State or the Member State’s territorial or administrative subdivisions, including the local authorities”. The text also contains some exceptions from this rule, in the paragraphs 2-4.

[50] Article 1, paragraph 7, point c) of the Council Directive (EU) 2023/2226.

[51] I.M. Costea, *op. cit.* p. 8.

[52] K.S. Must, *Taxpayers’ right to privacy and freedom to conduct business in light of DAC-6*, Master’s Thesis in International Business Taxation, School of Law, Tilburg

In this case, the evaluation of these fundamental rights should be realised through the comparison with the opposite principles raised in this field. In this spectrum, the principle of fair taxation and the freedom to access services are a priority, in order to ensure a competitive and fair internal market.

Is it a real battle? Our conclusions

Data is the new fuel of society that sets both the private and public environment in motion. In the fiscal field, the tax authorities rely on data to ensure taxpayers' compliance with their obligations and to maintain uniform taxation, combating fraud and tax evasion. On the other hand, taxpayers seek to minimise their tax burden, using various methods at their disposal[53]. In this context, the Blockchain technology, most commonly associated with Bitcoin, smart contracts, NFTs, and other cryptocurrencies, was initially perceived as an environment external to state sovereignty. However, the taxation of blockchain activities has proven to be inevitable.

Along with the increase in the number of people engaged in this new decentralised and anonymous system, the problem of collecting data on the transactions has attracted an important interest from both Member States, in particular, and the European Union institutions.

The conflict between the two opposing interests, namely the collection of data by state authorities for tax purposes and the preservation of their confidentiality, desired by blockchain users, has manifested itself, especially in recent years, with the emergence of new regulations in this matter. The „victims" of this conflict turned out to be the Crypto-Asset Service Providers, obliged by the new regulations to assure a greater transparency of the environment, in terms of transactions. This goal has to be accomplished by communicating the data of the participants in the operations to the tax authorities by digital means. As it was stated before, "to avoid corruption, the key then is to design incentive structures in such a way that the agent acts in the interest reducing the opportunities for corruption, and strengthening the mechanisms for monitoring and punishment"[54].

Although the new administrative tasks may represent some limitations of the right to conduct a business, they are viewed as necessary for the internal market. The rights of intermediaries have been sidelined in favour of establishing a uniform competitive environment and enduring efficient taxation of taxpayers. In this context, the digitalisation of the tax system brings new obligations for the providers of services and goods and also for the intermediaries, a situation that was qualified as "acceptable" for combating tax fraud. This path has already been

University, 2020, p. 19.

[53] M.Kačaljak, "*Paying taxes in the Digital Age*", in Bratislava Law Review, vol. 4, no. 2, 2020, pp. 21-30.

[54] O.O. Fagbohun, O. Obiyemi, "*Development of an Informal Sector and Tenement Taxes Monitoring and Compliance Enforcement Using Intelligent Based Electronic Policing System*", in Advances in Research, vol. 13, no. 1, 2018, pp. 1-16.

explored in previous years, an appropriate example in this case being the project of São Paulo Tax Invoice (Nota Fiscal Paulista) initiated by the Government of the State of São Paulo, in Brazil[55].

Cooperation between Member States in this field has also been recognized in the legal literature[56] as "a method adopted by states in a globalised system for the sustainability of the taxation field, playing an important role in facilitating the correct assessment of fiscal obligations and tax recovery and taxes, at the same time helping the taxpayer by respecting his rights".

We agree that a uniform set of rules on data in fiscal matters could represent a better approach to handling tax evasion and tax fraud. Also, for its subjects, it offers a specific procedure to deal with tax authorities, avoiding a multitude of legislative state mechanisms. Otherwise, in the absence of harmonisation at the level of the European Union, the tax authorities would still have tracked the incomes made through Blockchain. In this case, every Member State would establish for CARSPs their own rules, which may vary in terms of interpretation and obligations, increasing their administrative burden. Moreover, the legislative differences in this specific matter between Member States would transform the internal market into chaos, affecting the services offered by RCASPs.

From a user's perspective, their data collecting for tax purposes is a common procedure. Thus, the introduction of closer supervision in the Blockchain field is not a surprise, despite the decentralised nature of this system.

The data exchange system between Member States, as regulated by the amendments to Directive 2011/16/EU should not pose any threat to taxpayers' data. In any case, their simple engagement on the Internet, within this system, implies an automatic distribution of data concerning them. In this context, the main role of the service providers is to inform users about the transfer of their data to tax authorities. At the same time, we observe additional obligations for them. The obligation to communicate user data to the authorities of the Member States is a result obligation, sanctioned even with the prevention of the activity by the respective RCASP. At the same time, we note the existence of a due diligence obligation regarding the responsibility to collect data from users. Under these conditions, the anonymity provided by Blockchain is eroded, at least within these procedures.

[55] N. Oller De Mello, M.L.A. Fernandez, V.A. Zapparoli Castro Melo, E.M. Dias, C.F. Fontana, *"New technologies for Nota Fiscal Paulista (São Paulo Tax Invoice): Automation of the tax documents issue process in the retail of the state of São Paulo – Brazil*, in Wseas transactions on systems and control, issue 12, Volume 5, 2010.

[56] A.N. Dragordan, *Suveranitatea fiscală națională versus cooperarea fiscală interstatală**, in Revista Română de Drept al Afacerilor, no. 9, 2015, online access at https://sintact.ro/#/publication/151009845?keyword=cooperare%20administrativa%20fiscal &cm=SREST.

On the other hand, we have doubts about whether tax authorities will be able to analyse all the data they receive under Directive 2011/16/EU[57]. At least for the moment, the Member States do not have enough resources from an administrative point of view to fully achieve the intended purpose of data collection.

The continuous technological advancements in the sphere of the Internet, artificial intelligence and the transfer of certain legal relations to the blockchain sphere represent indeed the future of our society. It's inevitable that there will be opposition and dissatisfaction with certain regulations that initially seem to restrict users' rights. However, the regulation of legal relations is a necessity in this field as well. Only in this way can the European Union` internal market remain a safe and competitive place where the rights of all people are protected.

References

Benson, V., Adamyk, B., Chinnaswamy, A., Adamyk, O, *Harmonising cryptocurrency regulation in Europe: opportunities for preventing illicit transactions,* in European Journal of Law and Economics, no. 57, 2024.

Bernt, M., *DAC8: Commentary on the European Union's New Crypto Tax Reporting Regime,* in European Taxation, 2023.

Brodzka, A., *"The future of automatic tax information exchange in EU countries*", in US-China Law Review, 2005.

Costea, I.M., "*Taxing forms in the digital environment*", SHS Web of Conferences, no. 177, Legal perspectives on the Internet, COPEJI 6.0., 2023.

Dragomir, O., *Criptomonedele şi tehnologiile aferente acestora*, in Revista Română de Drept al Afacerilor, no. 3, 2021.

Dragomir, O., *Propunerea de Regulament privind pieţele criptoactivelor şi de modificare a Directivei (UE) 2019/1937,* in Revista Română de Drept al Afacerilor, no. 3, 2022.

Dragordan, A.N., *Suveranitatea fiscală naţională versus cooperarea fiscală interstatală**, in Revista Română de Drept al Afacerilor, no. 9, 2015.

European Commission, *A European strategy for data,* Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the regions, COM/2020/66 final, 19 February 2020.

Fagbohun, O.O., Obiyemi, O. "*Development of an Informal Sector and Tenement Taxes Monitoring and Compliance Enforcement Using Intelligent Based Electronic Policing System*", in Advances in Research, vol. 13, no. 1, 2018.

Falzon M., Curmi, M., *DAC 8: Reporting and Exchange of Information on Crypto-Assets,* on Zampa Debattista blog, 2024.

Ilucă, D. M., *Regulating Bitcoin. Legal aspects regarding the use of Bitcoin,* in "Alexandru Ioan Cuza" University Annals, Tome LXIII, Legal sciences series, supplement, no. II, 2017.

Kačaljak, M., "*Paying taxes in the Digital Age*", in Bratislava Law Review, vol. 4, no. 2, 2020.

Linden, T. van der, Shirazi, T., *Markets in crypto-assets regulation: Does it provide legal certainty and increase adoption of crypto-assets?*, in Financial Innovation, series 9(1), no. 22, 2023.

[57] M. Falzon, M. Curmi, *DAC 8: Reporting and Exchange of Information on Crypto-Assets,* on Zampa Debattista blog, 2024, online access at https://zampadebattista.com/insights/dac-8-reporting-and-exchange-of-information-on-crypto-assets/.

Must, K.S., *Taxpayers' right to privacy and freedom to conduct business in light of DAC-6*, Master's Thesis in International Business Taxation, School of Law, Tilburg University, 2020.

Oller De Mello, N., Fernandez, M.L.A, Zapparoli Castro Melo, V.A., Dias, E.M, Fontana, C.F., „*New technologies for Nota Fiscal Paulista (São Paulo Tax Invoice): Automation of the tax documents issue process in the retail of the state of São Paulo – Brazil*, in Wseas transactions on systems and control, issue 12, Volume 5, 2010.

Post, D., Cipollini, C., *The DAC8 Proposal and the Future of Crypto-Asset Reporting: Some Preliminary Thoughts* in Kluwer International Tax Blog, 2023.

Ungureanu, C.T., "*Legal remedies for personal data protection in European Union.", in Logos, Universality, Mentality, Education, Novelty. Section: Law*, issue 6, no. 2, 2018.

Ungureanu, C.T., *Personal data protection in international contracts*, in "Alexandru Ioan Cuza" University Annals, Tome LXIII, Legal sciences series, no. II, 2017.

Analele Ştiinţifice ale Universităţii „Alexandru Ioan Cuza” din Iaşi
TOM LXX, 2, Ştiinţe Juridice, 2024

DOI: 10.47743/jss-2024-70-2-9

General Considerations and Perspectives on New Artificial Intelligence (AI) Systems. Influence of AI Systems in the Area of Criminal Liability for Breaches of Integrity Rules in Public Office

Carmen Lorena VLĂDUȚ[1]

Abstract: Artificial intelligence systems are being used in various areas such as e-commerce, e-government and e-advertising, mainly because of their efficiency and ability to provide fast access to services. However, AI uses a massive amount of data, raising concerns about the privacy and control of this data held by large corporations or government entities. Although there are some risks associated with AI, such as discrimination in AI algorithms and over-reliance on technology, there are also many benefits to be gained from using these systems: automating administrative processes, providing assistance and support to citizens, data analysis and personalised decision-making etc. To maximise benefits and minimise risks, responsible control and management of AI data and systems is required. The integration of artificial intelligence in e-government and in the detection of breaches of the integrity of public functions may prove useful, but it must be accompanied by measures to ensure respect for human rights, data protection, discrimination and the avoidance of violations.

Keywords: artificial intelligence, public integrity, e-government, data control, AI risks, AI benefits, justice, integrity breaches, accountability, transparency, ethics.

I. Introduction

Artificial intelligence systems have an impact on various aspects of life and we can say that we are living in the age of *e-world*, from *e-business*, *e-commerce* to *e-government* and *e-advertising*. The continuous development of AI technologies and their application in more and more areas will influence the way we interact and function in the digital world.

Thanks to their ability to process and analyse large amount of information in real time, AI systems can provide solutions and recommendations in a variety of areas, with the main benefits being: operational efficiency and cost reduction. For example:

- In *e-commerce*, AI systems can recommend customised products to customers, based on their choices, resulting in an enjoyable shopping experience

[1] PhD student in Criminal Law, „Alexandru Ioan Cuza” University of Iași

and an increase in the number of potential customers who become customers of the retailer.

- In *e-government*, AI systems provide citizens with easy access to public services and improve the efficiency of public administration by automating repetitive and routine administrative processes for which public service employees are responsible. Thus, by relieving public sector employees of these repetitive processes, they will be able to perform highly complex tasks.

We can say without a doubt that the use of AI systems to manage data and make decisions based on the information used represents progress and development in all areas of *e-life*.

In terms of complex data analysis, AI systems have the ability to efficiently and accurately analyse large and diverse amount of available data, and to identify trends or patterns that are more difficult for humans to identify. The algorithms used can anticipate future outcomes or make certain predictions, helping to make effective decisions in certain contexts and in different domains.

The European Parliament, in its resolution of 20th January 2021 on artificial intelligence, underlines the importance of investing in human skills, including digital skills, in order to adapt to scientific advances involving AI-based solutions for people working in regulated professions, including activities related to the exercise of state authority, such as the administration of justice[2].

II. AI systems in *e-government*

Is AI-government more, or different, than the *e-government*? Since the inception of the Internet, scholars and practitioners have advocated the use of the Internet in government. Commonly known as *e-government*, the concept materialized over several decades and we have seen various manifestations of that in different times and in different countries. In the early stages of the Internet revolution, scholars recognized that the transformational success of *e-business* has a role to play in government and identified some exciting features of *e-government*. It was clarified that *e-government* involves using technology to benefit citizens[3].

The implementation of AI systems should not be considered an end in itself, but as a tool for the benefit of people, with the ultimate aim of increasing their quality of life, their capabilities and safety[4].

[2] See, European Parliament resolution of 20th January 2021 on artificial intelligence: questions of interpretation and application of international law in so far as the European Union is affected in the areas of civil and military uses and of state authority outside the scope of criminal justice (2020/2013 (INI), material available online at: https://www.europarl.europa.eu/doceo/document/TA-9-2021-0009_RO.html, consulted on 06.02.2024.

[3] See, Naqvi, Al. "AI-GOVERNMENT VERSUS E-GOVERNMENT: HOW TO VERNMENT WITH AI?" *Handbook of Artificial Intelligence and Robotic Process Automation: Policy and Government Applications*, edited by Al Naqvi and J. Mark Munoz, Anthem Press, 2020, pp. 97–108.

[4] See, European Parliament resolution of 6 October 2021 on artificial intelligence in

In the European Parliament resolution of 20th January 2021 on artificial intelligence, it[5] was considered necessary to adopt a common European legal framework on the definition of "AI system", being defined as *a system that is either software-based or embedded in hardware devices, and that displays behaviour simulating intelligence by, inter alia, collecting and processing data, analysing and interpreting its environment, and by taking action, with some degree of autonomy, to achieve specific goals.*

In the public sector, the use of AI has led to an efficient and productive public administration by freeing staff from routine tasks and eliminating human error in these processes, through automated document processing, correspondence management, event and meeting planning, and human resource management.

In the context of the European Union, one of the key pillars of the European legislative framework to promote the digitalization of public administration is the Digital Europe Strategy[6], launched by the European Commission in February 2020, which aims to set targets leading to the digitalization of Europe by 2030.

Digitisation and the use of AI systems are efficient both for the staff involved in the work of the public system and for citizens, as they primarily assist and support citizens by providing direct access to public services, making information of public interest available to them, offering assistance in filling in online applications and forms or answering questions.

The use of AI enables public administration to provide citizens with individual, personalised services, according to their needs, providing benefits to both citizens and administration, such as: a good user experience when interacting with the public administration, thanks to an efficient service that adapts to the needs and preferences of the citizen; increasing the level of trust and satisfaction of citizens by providing personalized, simple and safe services; the efficiency of the public services, by providing citizens with secure and fast resources, that deliver what they need through the appropriate use of resources; improving interaction and communication with citizens, by providing them with useful information according to their needs, which leads to a state of understanding and collaboration with public administration.

AI is increasingly being used in the justice sector, to enable more rational, lawful and timely decisions. The use of AI in the fight against crime and cybercrime

criminal law and its use by police and judicial authorities in criminal proceedings (2020/2016 (INI), material available online at: https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_RO.html, consulted on 06.02.2024.

[5] See, *European Parliament Resolution of 20 January 2021 on Artificial Intelligence, work cited.*

[6] See, R. Pérez-Morote, C. Pontones-Rosa, Montserrat Núñez-Chicharro, *The effects of e-government evaluation, trust and the digital divide in the levels of e-government use in European countries, Technological Forecasting and Social Change*, Volume 154, 2020,119973, ISSN 0040-1625.

could offer a wide range of possibilities and opportunities, and the principle that what is illegal offline is illegal online should continue to apply[7].

It is therefore expected that the use of AI will speed up judicial proceedings, where it will contribute to improving the process of analysing and collecting data and protecting victims, which could lead to an optimisation of the judicial process. The development of AI systems in the justice system is being studied, but the impact of the use of such technology, the use of algorithms that guarantee the fundamental principles of justice, such as a fair trial and the avoidance of discrimination or inequities, must certainly be assessed.

AI-based applications can offer great opportunities in the area of law enforcement, in particular to improve the working methods of law enforcement agencies and judicial authorities and to fight more effectively certain types of crime, in particular financial crime, money laundering and terrorist financing, online sexual abuse and exploitation of children, and certain types of cybercrime, thus contributing to the safety and security of EU citizens, but at the same time can pose significant risks to the fundamental rights of individuals; whereas any broad application of AI for mass surveillance purposes would be disproportionate[8].

However, the precautionary principle should be applied in the evaluation and use of AI technologies in the justice system, in order to minimise risks and potential negative consequences. It is important to recognise that the use of AI should not replace the involvement of humans at crucial moments, such as sentencing or decision-making. Instead, it should serve as a complementary tool, designed to support and enhance human activity, while respecting the rights and dignity of the individuals.

Thus, the benefits of integrating AI into public administration services are reflected in the efficiency and accessibility of public services, in user satisfaction, but also in the good management of human resources and the elimination of human error in non-complex, repetitive activities.

III. AI Data Control

The behaviour of AI systems is driven by the control of data by large technology corporations and public institutions.

With regard to public administration and *e-government*, public institutions have control over the AI systems used in this area due to their access to personal and non-personal data about citizens. As for large technology corporations, they have control over a large amount of information due to the data they collect through their online platforms and services.

It is essential that both public institutions and technology companies exercise responsible and ethical control over data and ensure that user's personal

[7] See, European Parliament Resolution of 20th January 2021 on Artificial Intelligence (...), *work cited.*

[8] See, European Parliament Resolution of 6th October 2021 on Artificial Intelligence in Criminal Law, *work cited.*

data is protected. In doing so, they will consider issues such as: technology corporations and public institutions should be transparent and accountable in how they manage data and how they implement AI systems; the protection of user's personal data and the implementation of data security and protection measures, as well as compliance with data protection regulations and standards, such as the General Data Protection Regulation; the evaluation of the AI algorithms used to ensure that they do not create discriminatory situations or result in unfair decisions; public consultation and participation of civil society in the process of development and implementation of AI systems, in order to take into account the interests of citizens and ensure that the benefits and risks of AI systems are properly assessed.

Regardless of the *'e'* domain, it is important to ensure that the control over data and AI is done responsibly and ethically, so that the benefits of AI are distributed fairly and user's personal data is protected. To achieve this, all stakeholders, namely governments, technology corporations, civil society and other interested parties, need to work together.

IV. Risks and hazards associated with AI systems

Anchored in the wider digital revolution, artificial intelligence (AI) is poised to transform the economy, society, geopolitics, and the global political orders we know today. The AI revolution's impact inextricably combines very substantive opportunities (e.g., AI for Good) and serious societal risks (e.g., unemployment, bias, privacy, safety). The prospect to shape AI development towards capturing these opportunities and minimizing the risks will depend on national-level policy, industry practices, and international coordination and collaboration. However, a global governance approach must consider the unique dynamics and challenges present in AI development[9].

The European Parliament was one of the first institutions to make recommendations on the regulation of artificial intelligence (AI), focusing in particular on issues of ethics, liability and intellectual property rights. These recommendations were an important step in paving the way for the European Union (EU) to become a world leader in the development and regulation of AI.

We need to recognise that along with the benefits of AI, there are certain risks that we need to be aware of:

1. bias and discrimination, which can occur when AI algorithms are trained on data that contains bias, or when they learn or amplify bias from training data.

Bias refers to the situation where AI algorithms can make unfair decisions due to inaccurate information they receive, which can lead to discriminatory or unfair treatment.

[9] See, Miailhe, Nicholas, and Yolanda Lannquist. "Global governance of artificial intelligence." *Handbook of Artificial Intelligence and Robotic Process Automation: Policy and Government Applications*, edited by Al Naqvi and J. Mark Munoz, Anthem Press, 2020, pp. 23-30.

In recruitment, AI systems can reproduce biases based on gender, age and ethnicity, affecting the fairness of the selection process.

In the justice system, AI algorithms can be biased in relation to procedural events, which could lead to violations of procedural rights.

In terms of discrimination, AI algorithms can result in unfair or unequal treatment based on race, gender, sexual orientation or other grounds.

To avoid these situations, AI algorithms must use diverse and balanced data in the training process, and the performance of the algorithms should be constantly evaluated in order to correct biases and develop algorithms that are not affected by discrimination and bias.

2. data confidentiality, namely the risks associated with it: unauthorized access, data leakage and unauthorised use of data.

The protection of individuals with regard to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union (the „Charter") and Article 16(1) of the Treaty on the Functioning of the European Union (the „TFEU") provide that every individual has the right to the protection of personal data concerning him or her[10].

AI systems can also use personal data to create detailed profiles of users, which can then be used to take decisions about them or predict their behaviour in ways that may affect their privacy and autonomy.

To avoid data privacy hazards in the use of AI, it is important that appropriate data security and protection measures are in place, including encryption, user access controls, informed and transparent user consent to the use of their data, and compliance with data protection regulations and standards, such as the General Data Protection Regulation (GDPR) in the European Union.

3. dependence on technology, a risk that society accepts with resignation, because in everyday life the human ability to make decisions or manage certain activities without technological support creates this vulnerability.

While we know that no technological system is immune to failure and error, reliance on AI systems makes people even more vulnerable, in addition to losing individual independence and autonomy with a life organised by technology.

Overall, it is important to find a balance between the use of technology and the development of human capabilities, in order to achieve our goals without compromising our critical thinking and ability to make independent decisions.

However, the European Union institutions recommend that Member States carefully assess the risks associated with the use of artificial intelligence (AI)-based technologies, in particular in relation to the automation of activities related to the exercise of state authority, such as the administration of justice. The assessment of these risks should be an integral part of the process of implementing AI technologies in these critical areas, which must take into account the need for

[10] See Regulation (EU) 2016/679 of the European Parliament and of the Council of 27th 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 (JO L 119, 4.5.2016, p. 1.)

safeguards, such as supervision by a qualified professional and strict rules of professional ethics.

V. Are we ready to accept the dangers posed by AI?

No matter how much we reflect on this question, the fact that AI systems offer us so many benefits in all areas: health, government, education, business etc., leading to efficiency, accuracy and accessibility of services and progress of society, we accept the potential risks, which we have a duty to ensure we minimise through the measures we take when using them.

The growing influence of AI in society has also led to the development of AI systems in the fight against corruption[11].

AI has been used to automatically predict corruption risks, based on data from news media[12], police archives[13], and financial reports[14]. Tweetbots can also highlight suspicious cases of MP's claiming expenses and encourage their followers to investigate further[15]. Algorithmic systems are already regularly used in the context of anti-money laundering, where they are employed to analyse large datasets of financial transactions in order to detect irregularities. They can flag certain transactions for further investigation or even restrict transactions before they take place[16]. However, AI can also have negative effects, which are often

[11] See, Aarvik, P. 2019. *Artificial Intelligence a promising anticorruption tool in development settings.* No. 2019:1. U4 Anti-Corruption Resource Center. *apud.* Köbis, N. C. et al. *The corruption risks of artificial intelligence.* Transparency International, 2022, material available online at: http://www.jstor.org/stable/resrep43028, Accessed 8 Feb. 2024.

[12] See, López-Iturriaga, F. J., Sanz, I. P. 2018. Predicting public corruption with neural networks: An analysis of Spanish provinces. Social Indicators Research, 140(3), 975 998, apud. Köbis, N. C. *et al. work cited.*

[13] See, Flachaire, S., Mocetti, P., Montalbano, A., Muscarnera, L. 2020. Predicting corruption crimes with machine learning. A study for the Italian municipalities, http://www.diss.uniroma1.it/sites/default/files/allegati/DiSSE_deBlasioetal_wp16_2020.pdf *apud.* Köbis, N. C. *et al. Ibidem.*

[14] See, Lavigne, S., Clifton, B., & Tseng, F. 2017. Predicting financial crimes: Augmenting the predictive policing arsenal. Preprint at https://arxiv.org/abs/1704.07826, *apud.* Köbis, N. C. *et al. Ibidem.*

[15] See, Forjan, J., Köbis, N. C., Starke, C. 2022. Using artificial intelligence to fight corruption: Expert interviews on the potentials and limitations of existing approaches. In A. Mattoni (Ed.), Digital Media and Anticorruption. 2006. Odilla, F. 2021. Bots against corruption: Exploring benefits and limitations of AI-based anti-corruption technology. International Seminar Artificial Intelligence: Democracy and Social Impacts, https://www.academia.edu/download/67395812/FO_AI_Bots_Against_Corruption_2May2021.pdf *apud.* Köbis, N. C., et al. *Ibidem.*

[16] See, Breslow, S., Hagstroem, M., Mikkelsen, D., Robu, K. 2017. The new frontier in anti money laundering.

https://www.mckinsey.de/~/media/McKinsey/Business%20Functions/Risk/Our%20Insights/The%20new%20frontier%20in%20anti%20money%20laundering/The-new-frontier-in-anti-money-laundering.pdf apud. Köbis, N. C. *et al. Ibidem.*

seemingly unintended. The implementation of AI systems in both the private and public sectors can lead to undesirable outcomes as a result of biased input data, faulty algorithms or irresponsible implementation[17]. For instance, certain facial detection software has been shown to perform poorly on people of colour, because it was not sufficiently trained with various training data sets[18].

The benefits of Artificial Intelligence (AI) systems in various aspects of "*e-life*" are considerable and deserve to be recognised, and with responsible and ethical management of AI technology, awareness of the risks and hazards associated with its use, and appropriate measures to manage it responsibly, *e-life* offers us enormous potential for improving the quality of life and advancing society.

VI. The influence of AI systems in the area of criminal liability for breaches of integrity rules in public office

The topic of the author's doctoral thesis is *Criminal liability for breaches of integrity rules in the exercise of public office and dignitaries*, i.e. for committing offences related to conflict of interest, corruption and service offences under the Romanian Criminal Code, offences assimilated to corruption offences under special laws, offences directly related to corruption offences, and an important aspect of the research could be how artificial intelligence systems could influence or intervene in the prevention, detection and investigation of these crimes, as well as in the monitoring of integrity in the public sector.

Previously, we mentioned that AI can be integrated into the justice system, of course with some due diligence so that the fundamental rights of the people involved are not affected by possible system errors, but we believe that it can also be implemented in the detection of the integrity of public functions, through the development of specialised software. Such software can use AI algorithms to analyse and monitor activities in the public sector and identify potential cases of corruption, fraud or abuse.

Artificial intelligence (AI) in the service of the law holds out the promise of a legal system that is more accessible, effective, efficient and just, where artificially intelligent systems, widely accessible and equipped with perfect knowledge of the law and of all jurisprudence, ensure high-quality legal representation and access to justice not just for the wealthiest among us but also for the most destitute and most vulnerable[19].

[17] See, Christian, B. (2020) *The Alignment Problem: Machine Learning and Human Values.* W. W. Norton & Company; Starke, C., Baleis, J., Keller, B., Marcinkowski, F. *No date. Fairness perceptions of algorithmic decision-making: A systematic review of the empirical literature. Big Data and Society.* https://arxiv.org/abs/2103.12016 apud. Köbis, N. C. *et al. Ibidem.*

[18] See, I. Buolamwini, T. Gebru (2018) *Gender shades: Intersectional accuracy disparities in commercial gender classification.* In S. A. Friedler & C. Wilson (Eds.), Proceedings of the 1st Conference on Fairness, Accountability and Transparency (Vol. 81, pp. 77-91). PMLR apud. Köbis, N. C. *et al. Ibidem.*

[19] See, N. Economou, B. Hedin. "Legal systems at a crossroads: justice in the age of

It should be noted that in criminal matters we do not have rules that cover the concept of integrity for criminal acts committed in the exercise of public functions, and the legislator has not provided for a specific penalty for failure to comply with the criminal rules on integrity in the exercise of public functions and dignities.

The term "integrity" in public office is sometimes used as an antonym to corruption, but integrity is not only about the absence of corruption, but also about personal dignity, communication and transparency in public decision-making, so as not to raise suspicions that private interests are taking precedence over the public interest.

The National Anti-Corruption Strategy 2021-2025 passed by Romanian Government defines integrity as the obligation of representatives of public institutions and authorities to declare any personal interests that may conflict with the objective exercise of their duties and to take all necessary measures to avoid such situations[20].

Public integrity implies the cumulative fulfilment of three conditions: the incorruptibility of the decision, irrespective of its beneficiary; respect for the principles of transparency and competitiveness; and good administration in terms of economy, effectiveness and efficiency[21].

In order to be held liable for criminal offences arising from breaches of integrity rules, there are preliminary steps that lead to this result if the conditions for criminal liability are met.

To this end, we believe that AI can be used to detect signs of breaches of integrity rules in the exercise of public functions, such as:

- financial anomalies resulting from significant discrepancies between the allocated budget and the execution of the budget;
- situations where persons holding public office or public dignitaries are involved in decisions or contracts that may be in conflict with their personal or financial interests, may raise suspicions about their integrity and impartiality; situations of discrimination in the decision-making process or in the provision of public services; inappropriate access to / or use of confidential or sensitive information for personal purposes or for the benefit of others; favouring certain companies or persons in the award of public contracts or licences; undue external influence on administrative or political decisions; irregularities in the recruitment and promotion process as a result of unclear or inconsistent procedures in this area;

artificial intelligence." *Handbook of Artificial Intelligence and Robotic Process Automation: Policy and Government Applications*, Anthem Press, 2020, pp. 119–28.

[20] Information that we have formulated in the chapter entitled *Criminal rules on integrity in the exercise of public functions and dignities*, from the research paper with the same name, in progress.

[21] See, *Guidelines on Whistleblower Protection (Ghidul privind protecţia avertizorilor de integritate),* Romanian Transparency Association, Bucharest, 2005, page 9, the text was consulted on 07.02.2024 at: https://www.transparency.org.ro/publicatii/ghiduri/GprotectieAvertizori.pdf.

and lack of transparency and accountability due to missing or inconsistent internal reporting and control systems.

These are just a few examples of indications of possible breaches of integrity in public office. It is important that these matters are properly investigated and dealt with to ensure that the principles of ethics, transparency and accountability in the exercise of public functions are respected and that legal procedures are followed where there is a suspicion of criminal offences in the exercise of public functions.

The algorithms of AI systems used to detect integrity rules violations could be trained to analyse large amount of data to identify suspicious activity by:

1. *analysing data*, in the sense that AI algorithms can analyse large amount of information to identify patterns and anomalies that may indicate suspicious activity in the performance of public functions, such as: monitoring financial flows, analysing public contracts and monitoring the behaviour of public servants.

2. *identifying patterns* or signals that may indicate corruption or fraud in administrative processes or decisions made in the exercise of public office. Algorithms can identify unusual discrepancies or inconsistencies in the way public resources are managed or in the way decisions are made within public institutions.

AI algorithms can identify discrepancies or inconsistencies in public resource management or decision-making, by analysing financial and accounting data to indicate possible fraud or abuse in the management of public financial resources. This can include detecting unusual transactions, unjustified expenditure or discrepancies between the budget and budget execution.

The algorithms can also monitor public contracts and government procurement, to identify potential cases of favouritism, corruption or abuse in the procurement process or in the execution of contracts. This can include analysing contract terms and conditions, comparing prices and identifying significant discrepancies.

The AI system can analyse administrative decisions taken by public institutions to identify potential cases of discrimination, bias or non-compliance with rules and procedures. This may include identifying discrepancies in the way different similar cases are handled, or analysing factors that influence administrative decisions.

AI algorithms can also monitor data flows and communications within public institutions, to identify potential cases of misuse or abuse of sensitive or confidential information.

By identifying and reporting these discrepancies or inconsistencies, AI algorithms can help improve transparency, accountability and integrity in the management of public resources and in public sector decision-making. This can lead to greater trust and credibility in public institutions and better protection of citizen’s interests and rights.

3. *monitoring*, in real time, *the conduct* in the performance of duties, to identify misconduct or behaviour that does not comply with ethical and legal

norms. This may include monitoring online activities, conversations or interactions with people outside the public institution.

By criminalising the offence of conflict of interest, the legislator's aim was to protect the social relations relating to the proper performance of the public official's activity, which requires the correct conduct of the person performing an activity within a public authority, public institution etc.; the social relations relating to the correctness of public officials in the performance of their duties also require them to refrain from taking any decision that could bring them, directly or indirectly, or a third party, a certain material advantage[22], with the exception of favouring relatives or persons with whom they have had business relations. Noting that the old and the new Romanian Penal Code similarly criminalize the conflict of interests, the previous doctrine emphasized that legislator also intended to protect the social relations related to the defence of the legal interests of natural or legal persons against the unlawful interests of public officials[23].

Where there is a suspicion that such an offence has been committed, investigative bodies may conduct monitoring using AI systems, while respecting the fundamental rights of individuals, including the right to privacy and confidentiality, and subject to safeguards to ensure that the AI system is used in a proportionate and necessary manner for the purpose of the investigation and that the data collected are handled appropriately and in accordance with ethical and legal principles.

4. *analysis of documents and internal communications of public institutions* using natural language processing algorithms to search for clues or indicators of suspicious or illegal conduct.

The ultimate aim of integrity is the rigorous respect of all legal frameworks within which public authorities must operate, in order to provide the widest and most predictable space for the full exercise of citizen’s fundamental rights[24]. Thus, the implementation of artificial intelligence in the detection of integrity in the exercise of public functions can contribute to increasing transparency, accountability and integrity in the public sector.

However, it is important to ensure that these systems are used in accordance with ethical and legal principles, and that adequate oversight and control mechanisms are in place, to prevent abuse or violation of individual rights, as well as expert oversight, to check for errors in the algorithms used by the system.

What is clear about the impact of artificial intelligence systems on criminal liability for breaches of public integrity is that the integration of such systems would play an important role in flagging potentially incriminating situations in

[22] See, T. Toader, *Drept penal. Partea specială, (Criminal Law, Special Part),* 7th Edition, Bucharest, Hamangiu Publishing House, 2012, p. 281.

[23] See, I. Măgureanu, „Conflictul de interese”, (*Conflict of Interests*), *Revista de Drept Penal (Journal of Criminal Law)* 2007, No. 2, p. 126.

[24] See, E.S. Tănăsescu, *Integrity in the exercise of functions as a guarantee of fundamental rights (Integritatea în exercitarea funcțiilor ca garanție a drepturilor fundamentale,) Judicial Courier, (Curierul Judiciar)* No. 2, 2018, p. 91.

relation to public integrity, a tool for preventing and combating corruption and other breaches of the law in the public sector, and could also lead to criminal liability for offences in relation to public integrity and beyond.

AI will not be able to replace investigative bodies or courts in providing legal solutions; the role of these systems is to generate information and indices to facilitate the investigative process and to help identify cases that require further attention from the relevant authorities.

VII. Conclusions

The use of artificial intelligence to detect breaches of integrity norms in public office is a promising approach to promoting transparency, ethics and accountability in the public sector. By analysing data and identifying anomalies or misconduct, AI systems can help prevent and combat corruption, conflicts of interest and other breaches of ethical and legal rules.

However, it is important to take into account the respect of fundamental rights of individuals and the protection of personal data in the monitoring process. The responsible use of AI technology must be accompanied by adequate safeguards, to respect the principles of confidentiality, transparency and impartiality.

The implementation of AI systems for this purpose should be part of a robust legal and institutional framework, that ensures respect for individual rights and promotes ethical and transparent governance. Through the proper management of these technologies, we can contribute to strengthening integrity and accountability in the exercise of public functions and the rule of law.

References:

Guide on protection of whistleblower, Romanian Association for Transparency, Bucharest, 2005.

Măgureanu I., *Conflictul de interese*, Revista de Drept Penal, 2007, no. 2.

Naqvi, Al. *AI-government versus e-government: how to government with AI?”.* Handbook of Artificial Intelligence and Robotic Process Automation: Policy and Government Applications, edited by Al Naqvi and J. Mark Munoz, Anthem Press, 2020.

Miailhe N., Lannquist Y., *Global governance of artificial intelligence.* Handbook of Artificial Intelligence and Robotic Process Automation: Policy and Government Applications, Anthem Press, 2020.

Economou N., Hedin B., *Legal systems at a crossroads: justice in the age of artificial intelligence.* Handbook of Artificial Intelligence and Robotic Process Automation: Policy and Government Applications, edited by Al Naqvi and J. Mark Munoz, Anthem Press, 2020.

Köbis N.C., et al. *The corruption risks of artificial intelligence.* Transparency International, 2022.

Pérez-Morote R., Pontones-Rosa C., Núñez-Chicharro M.T., *The effects of e-government evaluation, trust and the digital divide in the levels of e-government use in European countries*, Technological Forecasting and Social Change, Volume 154, 2020,119973, ISSN 0040-1625.

Toader T., *Drept penal. Partea specială*, Bucharest, Hamangiu Publishing House, 2012.