SARA Law **R**esearch **C**enter
International **J**ournal of **L**egal and **S**ocial **O**rder, https://www.ccdsara.ro/ijlso
ISSN 2821 – 4161 (Online), ISSN 2810-4188 (Print), ISSN-L 2810-4188
N°. 1 (2025), pp. 272-282

THE NEW SOCIAL REALITY: ARTIFICIAL INTELLIGENCE AND THE NECESSITY OF ALIGNING NATIONAL LEGISLATION WITH SOCIETAL EVOLUTION

R.N. LUNGEANU

Received 31.04.2025; accepted 24.06.2025
First online publication: 24.06.2025
DOI:https://doi.org/10.55516/ijlso.v5i1.258

Robert-Nicolae LUNGEANU
PhD student (in the field of Law) of Doctoral School of Social Sciences, University „Dunărea de Jos" Galați
E-mail: lungeanurobert@gmail.com
ORCID ID: https://orcid.org/0009-0004-5922-4313

Abstract

This paper aims to analyse the implications of the development and use of artificial intelligence from both legal and social perspectives, in a context where contemporary society is deeply shaped by digitalization. Beyond the undeniable benefits brought by this emerging technology, a critical reflection is required on how national legislation can—and must—adapt to new technological realities. The study raises a fundamental question: to what extent can technological evolution be pursued without compromising core human values? In this regard, the analysis emphasizes the imperative need for balanced regulation that ensures the protection of fundamental rights while also supporting responsible innovation.

Key words: *artificial intelligence, legal regulation, social transformation, fundamental rights.*

INTRODUCTION

In recent decades, technology has experienced unprecedented development, with artificial intelligence (AI) becoming a fundamental driver of this revolution. From autonomous devices performing complex tasks to algorithms influencing economic decisions, artificial intelligence is reshaping the foundations of the global economy and social relations. Although the concept of artificial intelligence is not new, it has only in recent decades emerged as a disruptive force in contemporary society.

Beginning with Alan Turing's seminal work (*Turing, 1950, pp. 430–460*), AI has evolved rapidly, impacting sectors such as automotive, healthcare, and finance. However, this technological advancement has not been matched by a corresponding evolution in legislation, which remains significantly behind emerging technologies.

While technological innovation progresses at a rapid pace, national legal frameworks have struggled to keep up, resulting in a critical legal challenge: how can we regulate technologies that fundamentally alter our way of life? How should legislation respond to the challenges posed by artificial intelligence? Moreover, how can fundamental rights be safeguarded in an era when algorithmic decisions increasingly influence individual futures? Despite the rapid development of AI, the question persists: is current legislation adequately prepared to address this new social reality?

The article „Legal Responsibility for Errors Caused by Artificial Intelligence (AI) in the Public Sector" (*Al-Dulaimi & Mohammed, 2025, pp. 1–11*) addresses this pressing issue, focusing on the attribution of legal responsibility for errors caused by AI systems within public institutions. Given the growing adoption of AI in public administration to enhance efficiency and service delivery, determining liability in the event of AI-related errors poses a complex challenge. Since AI systems may operate autonomously without direct human intervention, identifying whether liability rests with developers, public entities implementing AI, or end-users is a critical concern.

To clarify the legal understanding of artificial intelligence, the European Union Regulation 2024/1689 (*Official Journal L 239, 12.07.2024*) defines AI in Article 3 as „a machine-based system designed to operate with varying levels of autonomy and capable of exhibiting adaptability after deployment, which, pursuing explicit or implicit objectives, deduces from the input data how to generate outputs such as predictions, content, recommendations, or decisions that may influence physical or virtual environments." In essence, AI refers to systems designed to emulate human reasoning based on the data (experiences) they process.

In the 2000s, significant progress was made in developing algorithms capable of mimicking human language and cognition to interact effectively with their environments. Widely recognized examples of AI applications accessible to the public include Apple's Siri and Google's Alexa, culminating in the present-day prominence of systems like ChatGPT.

Danilo Doneda and Virgílio A. F. Almeida (*2016, pp. 60–63*), in their article "What is Algorithmic Governance?", examine the risks associated with algorithmic governance, including manipulation, social discrimination, and infringements of privacy and property rights, emphasizing the need for regulatory oversight.

Similarly, Magrani (*2017, pp. 1–17*), in „Internet Threats in a Technologically Regulated Society: A New Legal Challenge of the Information Revolution," analyzes how the pervasive interaction among devices, sensors, and users results in an exponential increase in data production, storage, and processing. While this connectivity offers benefits to consumers, it also poses risks to privacy and fundamental rights.

An illustrative case is Microsoft's Tay chatbot, which was withdrawn within 24 hours of launch due to generating offensive content. Keith W. Miller, Marty J. Wolf și F.S. Grodzinsky (*2017, pp. 1–12*), in their commentary "Why We Should Have Seen This Coming: Comments on Microsoft's Tay 'Experiment' and Its Broader Implications," stress the ethical responsibilities of AI developers and the need for stricter development standards and regulatory frameworks.

Consequently, as AI systems increasingly influence critical aspects of individuals' lives—from recruitment processes to judicial rulings—it becomes imperative to adapt legal frameworks to protect fundamental rights while fostering responsible technological advancement.

I. EUROPEAN UNION LEGISLATION ON ARTIFICIAL INTELLIGENCE

Since the danger of using artificial intelligence for the personal interest of certain individuals, which could act against the common interest of society, has become tangible, the legislator at the EU level contributed by implementing in 2016 the General Data Protection Regulation, published in the Official Journal of the European Union L 119 of 04.05.2016, which came into force on 25.08.2018.

This regulation sets forth certain conditions under which any legal entity managing personal data is obliged to respect the right to privacy of natural persons, as well as to prohibit the dissemination of such data except in legal situations authorized by competent bodies.

The GDPR imposes strict standards regarding transparency in the collection, storage, and use of personal data processed by artificial intelligence for various legal entities, examples being Facebook, Google, and so forth.

According to Article 5 of EU Regulation 2016/679, the fundamental principles of the GDPR are legality, transparency, fairness, data minimization, data accuracy, limited storage, and primarily confidentiality.

To understand data minimization in the analysis of artificial intelligence, it means that the data collected must only be those useful for the specific purpose. The emergence of this principle has forced companies implementing AI to find a balance so that the data collected is used efficiently.

Artificial intelligence systems processing personal data must obtain the explicit, free, and informed consent of the user, especially when the data is used to personalize algorithms that provide recommendations to the interlocutor, in the

sense that search engines used by the user offer suggestions based on their online searches. Thus, users have been granted the right to understand how the data they provide on the internet at large is used. The most illustrative example is marketing, where AI systems target individuals. Under this same aegis, the user has the right to delete their data uploaded on the internet, including the right to be forgotten by algorithmic systems.

The significant impact of artificial intelligence through the institution of this regulation concerns behavioral analysis, facial recognition, and machine learning, which rely on processing large volumes of information. According to Article 22 of GDPR 2016/679, automated profiling that leads to automated decisions directly affecting the person is prohibited. Automated profiling involves the use of algorithms for example for selecting certain candidates.

In case of non-compliance with the GDPR, Article 83 of EU Regulation 2016/679 provides that legal entities processing personal data can be sanctioned with fines of up to 4% of the annual turnover. Sanctions are determined according to the severity of the breach of confidentiality in relation to the level of protection adopted to ensure an adequate security factor for the personal data in their possession.

For a proper regulation of social reality, the European Union adopted the Artificial Intelligence Regulation, namely EU Regulation 2024/1689. During April 2021, the European Commission proposed a legislative framework to include the use of artificial intelligence globally. The purpose of this regulation is to ensure that AI technologies developed and implemented at the European level are safe, transparent, and comply with ethical standards and the protection of fundamental rights of EU citizens.

Entered into force on 01.08.2024, it was intended to ensure the safety and protection of users by establishing clear rules to regulate the use of AI systems in order to prevent abuses and risks related to data privacy. At the same time, it encourages innovation, offering a clear pathway in which artificial intelligence and algorithms designed accordingly can develop and evolve.

EU Regulation 2024/1689 presents 4 risk categories for artificial intelligence systems:

• Minimal risks, which include most AI applications used daily, that do not involve significant risks;

• Limited risks, including AI systems that pose low risk but require regulation, such as systems used for entertainment, personalized recommendations, chatbots, etc.;

• In the high-risk category are AI systems that may significantly affect the rights and freedoms of individuals. These must comply with certain transparency standards and allow users to understand automated decisions;

• The last category is reserved for AI systems that may directly affect citizens' lives or public security systems. These must be subject to rigorous controls and continuous monitoring.

This technological revolution has brought with it an enormous challenge for legislation. While technology evolves rapidly, national and international legislations develop at a much slower pace, and existing rules are often outdated by new technological realities. From the development of the first computers to the emergence of autonomous algorithms, the rule of law has had to respond to the challenges brought by each technological leap.

The Romanian legislator is always concerned with defending national security (*Iancu E.A., 2021, pp. 633-642*), whereby through criminal legal norms, it sanctions illegal acts that can be committed using IT systems (*Iancu, E-A. & al., 2023, pp. 363-383*). The realization of the law will contribute to ensuring legal security (*Lorincz A.L., 2025, p. 2*), which will determine both the degree of trust in state authorities and the perception of the legal order in a state at a given time.

II. UNDERSTANDING AI LEGISLATION FROM A SOCIAL PERSPECTIVE

To understand how the aforementioned legislative regulations were shaped, one must first understand the underlying need that motivated them. This cause lies in the transformations of society resulting from the evolution of artificial intelligence. These changes are profound and manifest across a wide range of domains. Artificial intelligence impacts the economy, jobs, education, and even social values and behavior. These technological shifts affect social and cultural values, and their adaptation will shape the future.

In the labor market, many activities involving repetitive tasks have already been automated, and this trend will continue to intensify. Examples come from the fields of industry, logistics, and financial services. In this context, jobs involving mechanical activities will disappear, but new ones will be created, such as those related to managing and supervising AI systems.

As more jobs become automated, the demand for roles requiring skills that only the human brain can analyze will increase. Additionally, there will be growing demand for critical thinking, innovation, and managing teams and automated processes. Work will become more flexible and increasingly reliant on collaboration between humans and machines. Professionals will need to adapt their working methods to maximize the efficiency of collaboration with automated systems.

One state that has adapted and continuously encourages the use of artificial intelligence is Saudi Arabia. U. Pagallo, in his work *Vital, Sophia and Co.—The Search for the Legal Status of Robots* (*U. Pagallo, 2018, pp. 1-11*), explores the legal status of robots, highlighting the frequent confusion between

their legal agency and juridical personhood. The example is Sophia, the first AI-powered robot granted citizenship by Saudi Arabia in October 2017, and the implications of this decision in the context of regulating emerging technologies are discussed.

In education, the AI revolution has influenced both how we learn and what we learn. The educational process has become much more personalized. The definition of artificial intelligence is "the ability of a machine to imitate human functions such as reasoning, learning, planning, and creativity." AI systems can analyze each student's progress and adapt educational materials and teaching methods to meet individual needs.

Through AI, access to educational resources has become easier for populations in isolated or disadvantaged areas. Educational institutions currently use AI implemented in programs to automate administrative tasks such as scheduling and student registration, saving time and resources.

In financial services, AI has transformed and accelerated global economic growth by rapidly solving logistical and administrative problems and by creating algorithms that accurately project economic market development. Companies use AI to analyze customer behavior, personalize user experiences, and optimize marketing and sales.

However, if legislation continues to evolve in step with human creativity regarding algorithm development underlying AI, what is the fear surrounding this technology? It all stems from fear of the unknown. Humans are shaped by certain social patterns and values, but since these patterns and our development are limited, AI—which can develop algorithms and patterns at an infinite scale—remains alien.

The more adaptable AI programs become, the more unpredictable their actions are, bringing new risks. Specialized studies (*S. Kapoor, P. Henderson, and A. Narayanan 2024, pp. 1-13*) have shown that AI has significant potential to transform the legal profession, but current evidence does not support a complete redefinition of it. They identify three types of legal tasks where AI is increasingly present: information processing, tasks involving creativity, reasoning or judgment, and predictions about the future.

Thus, AI can be used to make decisions in essential areas such as hiring, recruitment, and credit granting. An algorithm used for employee selection can favor a particular ethnic or gender group depending on the historical data used for training it.

The *Code of Ethics* of the Association for Computing Machinery stipulates that professionals in the field, regardless of prior legal regulations, should develop "comprehensive and thorough assessments of information systems and their impacts, including risk analysis" (*Magrani, 2019, p. 5*).

AI algorithms have been used to predict the recidivism of offenders but have been criticized for amplifying racial discrimination. For example, colored

individuals have often been considered at higher risk of reoffending despite behaviors not differing significantly from other groups. These algorithm-based forms of discrimination can lead to systemic inequalities in various societal domains, negatively impacting already marginalized groups.

In terms of national security, AI can pose significant threats in several ways, from sophisticated cyberattacks to the use of autonomous technologies in armed conflicts. In an era where AI is becoming increasingly advanced and integrated into critical infrastructures, governments and security institutions must understand and adequately respond to the associated risks.

One of the greatest national security threats is the use of AI for sophisticated cyberattacks. Machine learning algorithms can analyze vulnerabilities in a state's critical infrastructures, including sensitive sectors such as energy, finance, transportation, and communications.

AI is also used to influence public perception and manipulate information for political, economic, or social purposes. In the context of national security, it can be used to:

a. Generate and disseminate misinformation or fake news on a large scale, using natural language processing and neural networks capable of producing highly convincing false messages and articles. These can be used to destabilize a government or influence elections based on fabricated narratives.

b. Deepfakes: AI technologies for creating fake videos and audio recordings can produce propaganda material nearly indistinguishable from reality. For example, a deepfake video of a political leader making incendiary statements can be used to incite violence or destabilize a country's government.

c. Facial recognition: AI facial recognition technologies allow tracking individuals in public and private spaces, raising major privacy and civil liberties concerns.

d. Behavioral surveillance: AI algorithms can analyze people's online behaviors to anticipate actions or modify them through excessive personalization of content and advertising. This can lead to manipulation of public opinion and social control.

At the level of social network manipulation, AI can be used to amplify certain messages or ideas, creating filter bubbles or echo chambers that isolate users in realities where they are exposed only to specific viewpoints. These techniques can influence public opinion, polarize societies, and amplify internal tensions.

One of the gravest dangers is the use of AI in warfare. It can be and is used to develop autonomous weapons acting independently without direct human intervention such as:

- Autonomous drones — capable of identifying and destroying targets without human input, potentially leading to faster and harder-to-control conflicts;
- Combat robots — used in wars, reducing human casualties but causing massive collateral damage and with the potential to commit abuses;
- Cyber weapons — cyberattacks can become a form of warfare on a global scale, destroying critical infrastructures without conventional military force.

The use of AI in armed conflicts also raises fundamental moral and ethical questions: who is responsible if an AI machine makes an error and kills civilians? Can an algorithm be held responsible for war crimes?

III. HOW THIS PHENOMENON IS PERCEIVED IN THE ROMANIAN STATE

Romania has begun to recognize the importance of artificial intelligence for its economic and social future and is investing in the development of this field. In 2021, the Romanian Ministry of Research, Innovation, and Digitalization presented a national AI plan that includes objectives such as promoting education in the field, supporting research, attracting investments, and developing an appropriate legislative framework.

Interest in AI is growing in the private sector, with Romanian companies seeking to adopt the technology to remain competitive in international markets. There is also an increasing number of investments in research and development, with venture capital and European funds supporting startups in this domain.

There are concerns related to personal data protection, especially as AI is used in surveillance solutions or in the analysis of online behavior. Technologies such as facial recognition or social media data analysis are viewed with apprehension due to the risk of abuse or invasion of privacy.

Despite these concerns, there is also growing interest in AI technologies, particularly in the educational sector and among younger generations. Increasing numbers of young Romanians are interested in pursuing courses and specializations in this area, and Romania hosts several universities and research centers that train specialists in the field.

Romanian universities, such as the Politehnica University of Bucharest, Babeș-Bolyai University of Cluj-Napoca, and the University of Iași, offer academic programs and bachelor's, master's, and doctoral courses in fields such as artificial intelligence, machine learning, and data analysis. Additionally, there is a growing number of hackathons, online courses, and conferences dedicated to AI, organized to promote development in this domain.

However, one of the main obstacles is the lack of a specialized workforce in AI and related technologies. Although many talented young people exist in Romania, some choose to work in international companies or emigrate to

countries offering greater career opportunities and more attractive salaries in the AI field. This represents a challenge for talent retention and the development of innovative solutions locally.

Regarding AI regulation, Romania aligns itself with European standards, particularly the General Data Protection Regulation (GDPR), which governs how citizens' personal data can be collected and processed. Moreover, Romania actively participates in discussions on AI regulations at the European level to ensure a legal framework that protects citizens' fundamental rights and prevents the abusive use of AI technologies.

CONCLUSION

In my view, artificial intelligence represents one of the most significant challenges and opportunities of our time. It is a technology that, due to the scale and speed of its development, has the potential to reshape the economic, social, and cultural structure of Romania and the entire world. On one hand, I am deeply aware of the benefits AI can bring: increased efficiency across various sectors, support for decision-making through advanced data analysis, automation of repetitive processes, and last but not least, the creation of innovative solutions in health, education, and public administration.

On the other hand, I believe these advances should not be viewed solely through the lens of technological enthusiasm. They inevitably raise ethical, social, and legal questions. Personally, I feel a real concern about the impact AI may have on the labor market, especially for professional categories vulnerable to automation. Additionally, I believe the risks related to data privacy and the use of technology for surveillance or manipulation cannot be ignored, especially in an increasingly tense geopolitical context.

For this reason, I consider that Romania urgently needs a coherent and responsible national strategy for the development of artificial intelligence—a strategy that combines the promotion of innovation with clear regulation focused on protecting citizens and upholding democratic values. I also believe education must play a central role in this transition: not only by training specialists in the field but also by fostering a critical and ethical understanding of the technology among the general population.

Given these considerations, I take a balanced position between optimism about the progress AI can bring and the realism of recognizing its associated risks. The future of this technology—and how it will influence Romanian society—largely depends on our collective ability to understand, regulate, and use it wisely. Through a responsible and equity-oriented approach, I am convinced that artificial intelligence can become a genuine tool for sustainable development and social progress.

BIBLIOGRAFIE

1. 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) [Official Journal of the European Union, 04.05.2016];

2. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonized rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139, and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797, and (EU) 2020/1828 (Artificial Intelligence Regulation) [Official Journal of the European Union, 12.07.2024];

3. Al-Dulaimi,A.O.M. and Mohammed, M.A.-A.W. (2025), *"Legal responsibility for errors caused by artificial intelligence (AI) in the public sector*", International Journal of Law and Management, Vol. ahead-of-print No. ahead-of-print. DOI: https://doi.org/10.1108/ijlma-08-2024-0295

4. A. Tuing (1 octombrie 1950) „Mașini de calcul și inteligența” („Computing Machinery and Intelligence”) publicat în Mind DOI: https://doi.org/10.1093/mind/LIX.236.433

5. Doneda, D., & Almeida, V. A. F. (2016). What Is Algorithm Governance? *IEEE Internet Computing*, *20*(4), 60–63. DOI: https://doi.org/10.1109/MIC.2016.79

6. Iancu Elena-Ana, Enache Tușa, Nicolaie Iancu, Eduard Simion, Adrian-Cristian Moise (2023), Preventing computer crime by knowing the legal regulations that ensure the protection of computer systems în Tribuna Juridică, Nr.3./2023 WOS:001090715000003, https://doi.org/10.24818/TBJ/2023/13/3.03

7. Iancu, E.-A. (2021). *Regulation of offences against public security in the criminal Code of Romania*. International Journal of Legal and Social Order, 1(1). https://doi.org/10.55516/ijlso.v1i1.45

8. Lorincz, A.-L. (2025*). Review of some criminal judgments that do not resolve the substance of the case - procedural mean to ensure the legal order.* International Journal of Legal and Social Order, 5(1). https://doi.org/10.55516/ijlso.v5i1.248;

9. Magrani, E. (2017). Threats of the Internet of Things in a techo regulated society A New Legal Challenge of the Information Revolution. publicat în 2017 în *The ORBIT Journal*, vol. 1, nr. 1, paginile 1–17 *ORBIT Journal*, *1*(1). https://doi.org/10.29297/orbit.v1i1.17

10. Magrani, E. (2019). *New perspectives on ethics and the laws of artificial intelligence. Internet Policy Review*, 8(3). DOI: https://doi.org/10.14763/2019.3.1420

11. Miller, K. W., Wolf, M. J., & Grodzinsky, F. S. (2017). Why We Should Have Seen That Coming: Comments on Microsoft's tay "Experiment," and Wider Implications. *ORBIT Journal*, *1*(2). https://doi.org/10.29297/orbit.v1i2.49

12. Pagallo, U. (2018). Vital, Sophia, and Co.—The Quest for the Legal Personhood of Robots. *Information*, vol. 9, nr. 9. https://doi.org/10.3390/info9090230

13. Parlamentul European, „Ce este inteligența artificială și cum este utilizată?" data publicării 22.09.2020, actualizat la data de 21.06.2023, https://www.europarl.europa.eu/topics/ro/article/20200827STO85804/ce-este-inteligenta-artificiala-si-cum-este-utilizata

14. Sayash Kapoor, Peter Henderson, Arvind Narayanan (2024 Promises and pitfalls of artificial intelligence for legal applications, https://doi.org/10.48550/arXiv.2402.01656

15. Strategia Națională privind inteligența artificială" cod SIPOCA 704 implementat de Autoritatea pentru Digitalizarea României 2024–2027 (SN-IA) aprobată prin Hotărârea Guvernului nr. 832/2024, publicată în Monitorul Oficial nr. 730 din 25 iulie 2024.