Bulletin of the *Transilvania* University of Braşov
Series VII: Social Sciences • Law • Vol. 18(67) No. 1 – 2025
https://doi.org/10.31926/but.ssl.2025.18.67.1.25

ASPECTS REGARDING THE REGULATION OF THE ARTIFICIAL INTELLIGENCE AT THE EUROPEAN LEVEL

Adrian Cristian MOISE[1]

Abstract: *Starting from the definition of artificial intelligence, the article analyzes and presents the most important provisions in the field of artificial intelligence, such as the Regulation on artificial intelligence and the Framework Convention of the Council of Europe on artificial intelligence.*
Artificial intelligence can be considered as the most emerging field that can also be applied to the advancement of criminal sciences and justice system. Artificial intelligence uses effective algorithms in detecting risks in committing crimes and preventing illegal acts.
Algorithms based on artificial intelligence can detect an appreciable amount of data to discover risks and they are used to detect, prevent and even anticipate the commission of future crimes or some types of criminal behavior. How an AI system generates its results is often unknown to end users. This lack of understanding and transparency makes it difficult for users to anticipate the risks, damage or violations of their fundamental rights and freedoms that they may face.

Key words: *Artificial Intelligence, complex algorithms, Regulation on artificial intelligence, Council of Europe Framework Convention on Artificial Intelligence, the European Union.*

1. Introduction

In the field of criminal investigations of crimes committed in cyberspace, as well as physical space, artificial intelligence is used to identify the persons who committed the illegal acts and to find out the truth in the criminal process.

Artificial intelligence is the ability of a machine or program to perform human-like tasks, such as visual perception, person identification by voice and speech, cognitive thinking, decision-making, learning from experience, and solving complex problems at a higher speed and with a lower error rate than humans.

Artificial intelligence can be considered the most emerging field that can also be applied to progress in the field of forensic science and the justice system.

[1] *Spiru Haret* University of Bucharest, Faculty of Juridical, Economic and Administrative Sciences, Craiova, adriancristian.moise@gmail.com.

Artificial intelligence-based algorithms can detect a significant amount of data to uncover risks and are used to detect, prevent, and even anticipate future crimes or types of criminal behavior.

The term neural network is derived from the human brain, which is capable of learning from past experiences. An artificial neural network is like how the human brain works.

Neural networks have been used in many fields, such as visual scene interpretation, speech recognition, face recognition, fingerprint recognition, and iris recognition.

The field of criminal justice faces many challenges due to the huge amount of data, insignificant evidence, traditional forensic laboratories, and sometimes insufficient knowledge that can lead to the failure of a criminal investigation, or a serious miscarriage of justice.

Artificial intelligence is the weapon to fight these challenges involving machine learning and deep learning. Machine learning is a part of artificial intelligence that allows a machine or computer program to learn from historical activities or patterns to predict new output values using specific algorithms. Deep learning is a subfield of machine learning algorithms (Dupont, Stevens, Westermann, Joyce, 2018, pp. 16-17).

To understand how artificial intelligence can be used, we need to study the legal framework regarding the legal regulation of artificial intelligence at the international and European level.

2. The Legal Framework for Regulating Artificial Intelligence at The European Level

Artificial intelligence is made up of complex algorithms that are learnt from ever-expanding and changing data sets. How an AI system generates its results is often unknown to end users. This lack of understanding and transparency makes it difficult for users to anticipate the risks, harms or rights violations they may face.

All these circumstances have determined the need for regulation of artificial intelligence.

Government-issued command-and-control regulations, known as hard law, barely exist for AI, and following the model of other technologies, it is likely to be adopted gradually in a filter that will widen in the future. AI will be governed primarily by a non-legally binding instrument known as soft law, which consists of a variety of instruments that create autonomous expectations that are not directly enforceable by governments (Marchant, Gutierrez, 2023, pp. 380-384).

We believe that the most important issue relates to the application of soft law to artificial intelligence, in the sense that soft law is not necessarily applicable, as there are doubts about its effectiveness.

Artificial intelligence, through the algorithms used, generates a kind of normativity like law, which it lacks, because these algorithms are not law, which leads to the impossibility of challenging artificial intelligence in a court of law (Marchant, Gutierrez, 2023, p. 384).

The fact that artificial intelligence cannot be challenged in a court of law produces a major deficiency in the relationship between law, technology and democracy, an aspect

that will be considered in the analysis of the main regulations in the field of artificial intelligence at the European level.

At the European level, there are several artificial intelligence regulations, which appeared in 2024: The Regulation on Artificial Intelligence, which was adopted by the European Parliament and the Council of the European Union on 13 June 2024 and the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law.

The first proposal to regulate artificial intelligence was made in 2018 at the level of the European Union Commission in the document entitled Artificial Intelligence for Europe, published on the 25th of April 2018. This legal document highlighted the role of artificial intelligence in anticipating threats to computer security. According to the same communication, artificial intelligence refers to systems that exhibit intelligent behavior by analyzing their environment and that act - with a certain degree of autonomy - to achieve specific objectives. Systems based on artificial intelligence are based on software, acting in the virtual world, such as, for example, voice assistants, image analysis software, search engines, voice and facial recognition systems, or artificial intelligence can be incorporated into hardware devices, such as, for example, advanced robots, autonomous vehicles, drones or applications for the Internet of Things.

On the 21st of April 2021, a proposal for a regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Artificial Intelligence Law) was adopted, where Article 3(1) of this proposal for a regulation defines the notion of artificial intelligence system, which represents "software that is developed using one or more of the techniques and approaches listed in Annex I and that, for a specific set of human-defined objectives, can generate outputs such as content, predictions, recommendations or decisions that influence the environments with which it interacts". Accordingly, the notion of an "AI system" would refer to a range of software-based technologies that includes "machine learning", "logic and knowledge-based" systems and "statistical" approaches.

On the 14th of June 2023, the European Parliament published the amendments adopted by this European Union institution regarding the proposal for a regulation on artificial intelligence. An important amendment is the one adopted in reason 1, which completes the purpose of this regulation, which is to "promote the uptake of human-centric and trustworthy artificial intelligence and to ensure a high level of protection of health, safety, fundamental rights, democracy and the rule of law and the environment against the harmful effects of artificial intelligence systems in the Union, while supporting innovation and improving the functioning of the internal market. This Regulation establishes a uniform legal framework, in particular for the development, placing on the market, putting into operation and use of artificial intelligence, in accordance with the values of the Union and ensures the free movement of goods and services based on AI across borders, thereby preventing Member States from imposing restrictions on the development, marketing and use of artificial intelligence systems, unless explicitly authorized by this regulation".

On the 9th of December 2023, the European Parliament and the Council of the European Union drafted a proposal for a regulation establishing harmonized rules on

artificial intelligence, known as the Artificial Intelligence Act. The aim of this draft regulation is to ensure that AI systems used in the European Union are safe and respect fundamental rights and the values of the European Union.

The Regulation on Artificial Intelligence was finally adopted by the European Parliament and the Council of the European Union on June 13, 2024. The purpose of this Regulation is to improve the functioning of the internal market by establishing a uniform legal framework, in particular for the development, placing on the market, deployment and use of artificial intelligence systems in the Union, in accordance with the values of the Union, to promote the uptake of trustworthy and human-based artificial intelligence, while ensuring a high level of protection of health, safety, fundamental rights enshrined in the Charter of Fundamental Rights of the European Union, including democracy, the rule of law and the environment, to protect against harmful effects of AI systems in the Union, and to support innovation.

The AI Regulation aims to: develop rules on high-impact general-purpose AI models that may cause systemic risks in the future, as well as on high-risk AI systems; create a revised governance system with some enforcement powers at EU level; allow law enforcement bodies to use remote biometric identification in public spaces, subject to safeguards; require operators to carry out an impact assessment on the fundamental rights of users before a high-risk AI system is placed on the market by its operators.

Recital 17 of the AI Regulation defines a 'remote biometric identification system' as "an AI system intended to identify natural persons without their active involvement, typically at a distance, by comparing a person's biometric data with biometric data contained in a reference database, regardless of the specific technology, processes or types of biometric data used. Remote biometric identification systems should typically be used to perceive multiple persons or their behavior simultaneously, with the aim of significantly facilitating the identification of natural persons without their active involvement".

We note that the AI Regulation does not include AI systems intended to be used for biometric verification, including authentication, the sole purpose of which is to confirm that a specific natural person is the person they claim to be and to confirm the identity of a natural person for the sole purpose of granting access to a service, unlocking a device or secure access to a premises. This exclusion is justified by the fact that such AI systems are likely to have a minor impact on the fundamental rights of natural persons compared to remote biometric identification systems that can be used to process biometric data of large numbers of individuals without their active involvement.

Recital 18 refers to an 'emotion recognition system' which is "an AI system designed to identify or infer the emotions or intentions of natural persons based on their biometric data". This refers to emotions or intentions such as happiness, sadness, anger, surprise, disgust, embarrassment, excitement, shame, contempt, satisfaction and amusement. Physical states such as pain or tiredness are not included, including, for example, systems used to detect the tiredness of professional pilots or drivers for the purpose of accident prevention.

Regarding emotion recognition systems, we highlight the role of the artificial neural networks, which can identify a person's stress or insincerity. Thus, together with a variety

of physiological characteristics, it is possible to identify situations of high stress and even detect a person's insincerity and simulated behaviour of the person, which conceals the truth, using artificial neural networks (Nirvan, Sonone, Saini, Sankhla, 2024, pp. 1-15).

Even during imaging investigations of the human brain, artificial intelligence algorithms based on artificial neural networks can analyze the activities that a suspect's brain undergoes to determine whether they are engaging in true or false behaviour (Alaa El-Din, 2022, pp. 18-21).

Furthermore, as regards the use of 'real-time' remote biometric identification systems in publicly accessible premises, the AI Regulation clarifies the objectives for cases where such use is strictly necessary for law enforcement purposes and where, as a result, law enforcement authorities should exceptionally be allowed to use such systems. The AI Regulation provides for additional safeguards and limits these exceptions to cases of victims of certain crimes, to the prevention of real, present or foreseeable threats, such as terrorist attacks, and to the search for persons suspected of having committed the most serious crimes.

We underline that the AI Regulation requires a fundamental rights impact assessment to be carried out before a high-risk AI system is placed on the market by its operators. The AI Regulation also provides for increased transparency regarding the use of high-risk AI systems.

We note that certain users of a high-risk AI system that are public entities will also be required to register in the European Union database for high-risk AI systems. In addition, the AI Regulation emphasizes the obligation for the users of an emotion recognition system to inform individuals when they are exposed to such a system.

In addition, the AI Regulation contains provisions that allow, under certain conditions and subject to specific safeguards, the testing of AI systems in real-world conditions. To reduce the administrative burden for smaller businesses, the AI Regulation includes a list of actions to be taken to support such operators and provides for some limited and clearly specified derogations.

The Artificial Intelligence Regulation was adopted by the European Parliament and the Council of the European Union on the 13th of June 2024 and entered into force on 1 August 2024, with most of the provisions of the regulation applying from 2 August 2026. Some provisions of the regulation will apply from 2nd of August 2025, and the classification rules for high-risk AI systems will apply from 2nd of August 2027.

Artificial Intelligence Regulation is the first comprehensive regulation on artificial intelligence to be adopted worldwide.

The second very important step in the field of artificial intelligence regulation at the European and international level was taken on the 17th May 2024, when the Council of Europe adopted the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law in Strasbourg during the annual ministerial meeting of the Committee of Ministers of the Council of Europe.

The Council of Europe adopted the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law; adopted at the international level, the latter aims to ensure respect for human rights, the rule of law and democratic legal standards in the use of artificial intelligence systems.

The Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law establishes transparency and control requirements adapted to specific contexts and risks, particularly the identification of content generated by the AI systems.

The Council of Europe Convention provides a common approach to ensure that AI systems are compatible with human rights, democracy and the rule of law, while enabling innovation and trust. The Convention covers AI systems that could interfere with human rights, democracy and the rule of law, following a differentiated and risk-based approach.

The Convention will be implemented in the EU through the AI Regulation, which generally contains fully harmonized rules for the placing on the market, putting into operation and use of AI systems, complemented by other relevant Union acquis, where appropriate.

The principles and obligations set out in the Convention will apply to activities throughout the life cycle of AI systems undertaken by public authorities or by private actors acting on their behalf. As for private sector actors, while they must address the risks and impacts of AI systems in a way that aligns with the objectives of the Convention, they have the option either to apply the obligations set out in the Convention directly or to implement appropriate alternative measures.

The Council of Europe Convention includes a number of key concepts from the EU AI Regulation, such as a risk-based approach, transparency along the value chain of AI systems and AI-generated content, detailed documentation obligations for AI systems identified as presenting a high risk, and risk management obligations, with the possibility of introducing bans for AI systems considered to pose a clear threat to fundamental rights.

The Council of Europe Convention also includes other key concepts of the AI Regulation, such as: the focus on human-centric AI, consistent with human rights, democracy and the rule of law; key principles for trustworthy AI, e.g. transparency, robustness, safety, governance and data protection; transparency for AI-generated content and in interactions with AI systems; strengthening documentation, accountability and remedies; supporting safe innovation through regulatory sandboxes; risk management and documentation obligations; oversight mechanisms for overseeing AI activities. The general obligations stipulated by the Convention aim at the protection of human rights and the integrity of democratic processes and respect for the rule of law.

The novelty that the Convention brings in relation to the AI Regulation refers to the establishment of principles related to the activities in the life cycle of artificial intelligence systems that signatory states must implement about artificial intelligence systems in a manner appropriate to their domestic legal systems and the other obligations in this convention. These principles refer to the following: human dignity and individual autonomy, in relation to activities in the life cycle of artificial intelligence system; transparency and oversight regarding activities in the life cycle of artificial intelligence systems, including the identification of content generated by artificial intelligence systems; accountability and responsibility for the negative impact on human rights, democracy and the rule of law resulting from activities in the life cycle of artificial intelligence systems; equality and non-discrimination for signatory states to ensure that

activities within the life cycle of artificial intelligence systems respect equality, including gender equality, and the prohibition of discrimination, in accordance with applicable international and domestic law and for maintaining measures that overcome inequalities to achieve fair, just and equitable outcomes, in accordance with applicable domestic and international human rights obligations; privacy and personal data protection in the sense that the privacy rights of individuals and their personal data must be protected by signatory states, including through applicable domestic and international laws, standards and frameworks; reliability, signatory states being obliged to take measures to promote the reliability of artificial intelligence systems and trust in their results, which could include requirements related to appropriate quality and security throughout the life cycle of artificial intelligence systems; safe innovation, in the sense that each signatory state, each party, must allow the establishment of controlled environments for the development, experimentation and testing of artificial intelligence systems under the supervision of its competent authorities. In Article 14, entitled Remedies, the Council of Europe Convention establishes for the first time some redress or compensation, so that signatory states take some measures to ensure the availability of accessible and effective remedies for human rights violations resulting from activities during the life cycle of artificial intelligence systems.

Thus, Member States must take measures to ensure that relevant information regarding artificial intelligence systems that have the potential to significantly affect human rights, and their relevant use is verified and provided to bodies authorized to access that information, or to ensure that the aforementioned information is sufficient for the affected persons to challenge the imposed decision. The remedy also refers to some measures that Member States must take, in the sense of providing in their domestic law the effective possibility for the people concerned to lodge a complaint with the competent authorities.

We are of the opinion that the text of Article 14 of the Council of Europe Convention, which refers to remedies, should be rewritten by legislators as it does not provide Member States with all the information necessary to establish these remedies.

Thus, legislators should first define which artificial intelligence systems could affect human rights and secondly, legislators should establish a clear procedure by which relevant information on artificial intelligence systems that have the potential to significantly affect human rights can be verified by the competent authorities under the domestic law of each Member State.

Article 15 of the Council of Europe Convention establishes procedural safeguards, meaning that each Member State shall ensure that where an artificial intelligence system has a significant impact on the exercise of human rights, effective procedural safeguards, guarantees and rights are available to the persons affected by them, in accordance with applicable international and national law.

We believe that Article 15 of the Council of Europe Convention should also be rewritten and amended, as the legislators of the Council of Europe have not specifically detailed what these procedural safeguards consist of and how they can be applied in the domestic law of each Member State.

3. Conclusions

Even though several legal instruments have been adopted at European level in the field of artificial intelligence regulation, we believe that the use of artificial intelligence systems still endangers the respect of fundamental rights and freedoms, such as, for example, the right to non-discrimination, freedom of expression, human dignity, the protection of personal data and the right to privacy. We consider that the implications of artificial intelligence systems for fundamental rights protected by the Charter of Fundamental Rights of the European Union, as well as the safety risks for users of artificial intelligence, when artificial intelligence technologies are incorporated into products and services, raise certain concerns at present.

The two legal instruments in the field of artificial intelligence, the Regulation on Artificial Intelligence and the Council of Europe Framework Convention on Artificial Intelligence, which also have many common provisions, still do not currently contain sufficient provisions and procedural guarantees to protect the relationship between law, technology and democracy.

References

Alaa El-Din, E.A. (2022). Artificial Intelligence in Forensic Science: Invasion or Revolution? *Egyptian Society of Clinical Toxicology Journal*, Vol. 10, Issue 2, ISSN: 2356-6515 (print), ISSN 2356-6523 (Online), The Egyptian Society of Clinical Toxicology, Zagazig University.

Dupont, B., Stevens, Y., Westermann, H., Joyce, M. (2018). International Centre for Comparative Criminology – Université de Montréal. Canada Research Chair in Cybersecurity. *Artificial Intelligence in the Context of Crime and Criminal Justice*. A *Report for the Korean Institute of Criminology*.s Montreal, Canada.

Marchant, G., Gutierrez, C.I. (2023). Soft Law 2.0: An Agile and Effective Governance Approach for Artificial Intelligence. *Minnesota Journal of Law, Science & Technology*, Vol.2 4(2). Minneapolis, Minnesota.

Nirvan, A., Sonone, S.S., Saini, K., Sankhla, M.S. (2024). Introduction to Artificial Intelligence in Forensic Science. In Saini, K., Sonone, S.S., Sankhla, M.S., Kumar, N. (eds.), *Artificial Intelligence in Forensic Science. An Emerging Technology in Criminal Investigation Systems* (14 pages). Boca Raton, Florida: CRC Press, Taylor & Francis Group.