EUROPEAN UNION ARTIFICIAL INTELLIGENC LAW – A LEGAL FRAMEWORK FOR THE FUTURE

Mariana-Alina ZISU
ORCID [ID]: 0000-0003-2778-3749
E-mail: stefanoaia.mariana@yahoo.com
Affiliation: Legal adviser PhD Candidate
Member of the Methodological and Professional Guidance Commission of the "College of Legal Advisers Suceava" Association
Member of the Methodological and Professional Guidance Commission of the Federation Order of Legal Advisers from Romania

Abstract: In the context of the accelerated development of artificial intelligence (AI) technologies, the European Union has recognised the need for a clear legal framework that guarantees safety, transparency and respect for citizens' fundamental rights. This is how the Artificial Intelligence Act (AI Act) was born, the world's first comprehensive set of regulations in this area. Adopted in 2024, the law aims to position the EU as a global leader in the responsible governance of AI.

The Artificial Intelligence Act (AI Act) is the world's first comprehensive legal framework for regulating artificial intelligence. Adopted by the European Union in 2024, the law aims to ensure that AI systems used in the EU are safe, respect citizens' fundamental rights and stimulate innovation.

Keywords: technology; artificial intelligence; regulation; law.

Introduction

Artificial Intelligence (AI) is one of the most disruptive technologies of the 21st century, with a transformative potential for all sectors of society – from health, justice and education, to defence, industry and governance. Against the backdrop of this accelerated expansion, the European Union has recognised the need to establish a unified, predictable and focused regulatory framework that ensures both

the stimulation of innovation and the protection of citizens' fundamental rights. Thus, in 2024, the Regulation on Artificial Intelligence (informally called the "AI Law") was adopted, the first legal instrument of a general and binding nature at international level that transversally regulates the use of AI.

The legal basis of this regulation is Article 114 of the Treaty on the Functioning of the European Union (TFEU), which allows the adoption of measures for the harmonisation of the internal market. This choice reflects both economic reasons (avoiding fragmentation of the European digital market) and legal considerations – creating a common standard of compliance for all actors developing, providing or using artificial intelligence systems in the Union. At the same time, the regulation invokes the Charter of Fundamental Rights of the European Union, in specific Articles 1 (human dignity), 7 (privacy), 8 (protection of personal data) and 21 (non-discrimination), as ethical and legal foundations for limiting dangerous uses of AI.

A defining feature of the regulation is its risk-based approach, inspired by regulatory legislative models (such as medical devices or toys). Thus, AI systems are classified according to the risk they pose to the rights and safety of individuals: from unacceptable risk (prohibited) to high risk (strictly regulated), limited risk (transparency obligations) and minimal risk (not affected). This legal structure is coherent with the principle of proportionality in EU law and provides a flexible but firm framework for legislative intervention.

The EU AI Law is therefore not limited to a simple technological regulation, but a category of political and legal declaration of principle: artificial intelligence must be safe, transparent, controllable and compatible with the rule of law. In a world where AI regulation is either lax (the American model) or authoritarian (the Chinese model), the European Union proposes a balanced normative vision, becoming a legal laboratory for the global future of technological governance.

1. Legal basis and guiding principles of the European Union Law on Artificial Intelligence

The adoption of the Artificial Intelligence Regulation (AI Act) by the European Union in 2024 marks a defining moment for the law of emerging technologies. This regulatory framework is based not only on economic and technological reasons, but also on fundamental legal principles of the European order: the protection of fundamental rights, proportionality, transparency, accountability and legal certainty. At the heart of this regulation are two major components: the primary legal basis, represented by the Treaty on the Functioning of the European Union (TFEU), and a series of guiding principles drawn from both positive law and the ethics of technology regulation.

1.1. Legal basis: Article 114 TFEU

The AI Regulation is adopted on the basis of Article 114 TFEU, which empowers the European Parliament and the Council to adopt "measures for the approximation of the laws, regulations and administrative provisions of the Member States which have as their object the establishment and functioning of the internal market" (Treaty on the Functioning of the European Union). The choice of this basis is significant, as it positions the law as an instrument of legislative harmonisation, intended to prevent regulatory fragmentation and to create a uniform framework for all economic actors providing AI systems on the EU market.

This legal option has been criticised by some authors for ignoring the deeply constitutional and fundamental dimension of AI, in particular in relation to human rights (Veale & Borgesius, 2021). However, the case law of the Court of Justice of the European Union (CJEU) has confirmed that Art. 114 can also be used for regulations that have non-commercial objectives, as long as they indirectly contribute to the proper functioning of the internal market (CJEU, Case C-376/98 - German Tobacco Advertising, para. 84-86). Thus, although the law explicitly aims to protect fundamental values, it is nevertheless formally coherent with the architecture of the Treaties.

1.2. Guiding principles of regulation
a) Risk-based approach

The central principle of the regulation is to assess and classify AI systems according to the risk they pose to the health, safety and fundamental rights of individuals. This regulatory model is inspired by other areas of EU law, such as product safety (Compare with Regulation (EU) 2017/745 on medical devices), but also includes an ethical and social dimension. The law distinguishes four levels of risk:

- Unacceptable risk – systems completely prohibited;
- High risk – systems strictly regulated, such as those used in education, employment, law enforcement;
- Limited risk – transparency obligations for users (e.g. chatbots);
- Minimal risk – systems excluded from regulation.

This approach reflects the principle of proportionality, enshrined in Art. 5(4) TEU, according to which Union action must not go beyond what is necessary to achieve the objectives of the Treaties.

b) Respect for fundamental rights

Another cardinal principle is the protection of fundamental rights, in particular against the automation of decisions that may affect the life, liberty or dignity of individuals. The Regulation makes explicit reference to the Charter of Fundamental Rights of the European Union - 2000/C 364/01, underlining the respect for Art. 1 (human dignity), Art. 7 (privacy), Art. 8 (data protection) and Art. 21 (non-discrimination).

Thus, AI systems that may lead to algorithmic discrimination, abusive surveillance or cognitive manipulation are either prohibited or subject to very strict control measures. These provisions are in line with the case law of the ECHR and the CJEU on limiting interference with private life and the need to guarantee transparency in decision-making (ECtHR, Case Big Brother Watch v. UK, 2021, and CJEU, Case Digital Rights Ireland, C-293/12).

c) Transparency and human oversight

The Regulation introduces obligations regarding the explainability, auditability and human oversight of decisions taken by AI systems. According to Art. 14 of the regulation, high-risk systems must be designed in such a way that decisions can be understood and challenged by users or affected persons. This contributes to legal certainty, but also to strengthening public trust in the use of automated technologies (Goodman & Flaxman, 2017).

d) Liability and compliance

The regulation requires a clear distribution of responsibilities between developers, suppliers, importers and users of AI systems. It also establishes obligations regarding technical documentation, testing, auditing and incident reporting, similar to regulations in the field of product conformity.

These requirements ensure the traceability of automated decisions and allow for the intervention of supervisory authorities. In addition, the sandbox mechanisms provided for by the law allow the testing of innovative technologies in a controlled framework, which reflects a flexible and innovation-friendly approach, without compromising legal standards.

2. Sanctioning regime and compliance mechanisms in the EU Artificial Intelligence Law

The adoption of a robust sanctioning and compliance regim
 is an essential component of any regulatory instrument with a horizontal vocation and broad applicability, such as the Artificial Intelligence Regulation (AI Act). Inspired in part by the model of the General Data Protection Regulation (GDPR), the AI Act enshrines a complex institutional and sanctioning architecture, designed to ensure compliance with legal requirements, prevent abuses and guarantee the effective protection of fundamental rights.

2.1. Sanctioning regime: severity and proportionality

Articles 71–74 of the AI Regulation regulate a tiered sanctioning regime, which reflects both the seriousness of the infringement and the systemic nature of the irregularities. Three major categories of infringements are established, each with different levels of penalty:

Infringements of the most serious provisions, such as the use of prohibited systems of unacceptable risk (e.g. social scoring or cognitive manipulation), are sanctioned by administrative fines of up to EUR 35 million or 7% of global annual turnover (Art. 71(3) of Regulation (EU) 2024 on Artificial Intelligence).

Infringements of obligations concerning high-risk systems (technical compliance, transparency, documentation, human oversight, etc.) can attract fines of up to EUR 20 million or 4% of global turnover (Art. 71(2) AI Act).

Incorrect or incomplete declarations in compliance procedures attract penalties of up to EUR 10 million or 2% of turnover (Art. 71(1) AI Act).

This scaling of penalties reflects the principle of proportionality of penalties, enshrined in European criminal and administrative law. Penalties are not exclusively pecuniary: national authorities may order a ban on the marketing of the system, its withdrawal from the market or the suspension of its use.

It is important to note that, as with the GDPR, fines are not automatic, but must be justified by a contextual assessment, which takes into account the severity, duration of the breach, intent or negligence, corrective measures taken, as well as cooperation with competent authorities (See also Art. 83 GDPR, which requires the assessment of the seriousness of the infringement in the light of a number of contextual factors – a principle implicitly taken up in the AI Act).

2.2. Compliance mechanisms: prevention, audit and control

To prevent infringements, the AI Regulation establishes a series of legal, technical and procedural mechanisms that aim to ensure the

compliance of AI systems from design to implementation. Among the most important are:

a) Conformity assessment (ex ante)

AI systems classified as high-risk must undergo a conformity assessment procedure, similar to the existing CE marking mechanism for regulated products. This involves:

- functional testing of the system (accuracy, robustness, security);
- detailed technical documentation;
- risk governance plans;
- human oversight procedures and algorithmic transparency (Art. 19–23 AI Act; Annex IV details the technical requirements and documentation).

The rigor of respecting fundamental rights and freedoms goes beyond the framework of the Communities, becoming a strong point in the external relations existing at the Union level. The existence of the multitude of agreements concluded with numerous countries includes provisions that can go as far as providing for the suspension of relations or the denunciation of agreements in the event of a serious violation of human rights and fundamental freedoms by one of the parties (Corsei, Zisu & Țoncu, 2023, p. 55).

The assessment can be carried out either internally, by the developer, or by external assessment bodies (third-party notified bodies), depending on the complexity and sensitivity of the application. Each approved system must also be registered in a publicly accessible European database (Art. 60 AI Act).

b) Control mechanisms and competent national authorities

Each Member State must designate one or more national supervisory authorities, responsible for monitoring the application of the regulation, receiving notifications, carrying out inspections and imposing sanctions. These authorities cooperate through the European AI Board, a newly created body that plays a similar role to the European Data Protection Board (EDPB) in the case of the GDPR (Art. 64–66 AI Act. Compare with the role of the EDPB in the enforcement of the GDPR).

The Board has the following tasks:

- issuing interpretative guides and best practices;
- coordinating decisions in cross-border cases;
- promoting convergence between Member States;
- advising the European Commission on updating the list of high-risk systems.

c) The "sandbox" mechanism and legislative flexibility

To stimulate innovation, the AI Act introduces the possibility of establishing experimental legal regimes ("regulatory sandboxes"). They allow for the testing of innovative AI systems in a controlled environment, under the supervision of the authorities, without temporarily applying all the standard requirements. The aim is to strike a balance between technological development and ex ante protection of rights.

This mechanism joins other instruments of regulatory flexibility, such as the possibility of periodic review of the Regulation (Art. 85) or updating of the annexes by delegated acts (e.g. extension of the lists of prohibited or high-risk systems).

3. Impact on economic operators and public administrations

The entry into force of the Artificial Intelligence Regulation (AI Act) implies a profound transformation of the way in which economic actors and public institutions develop, implement and supervise systems based on artificial intelligence. The legal regime established by the law generates a multiple impact on responsibilities, compliance costs, decision-making processes and organizational culture, with direct implications for their competitiveness, legitimacy and efficiency.

3.1. Impact on economic operators
a) Compliance burden and regulatory costs
For companies that develop or market AI systems classified as high-risk, the law imposes a complex set of technical, legal and organizational obligations. These include:

- developing and maintaining complete technical documentation (art. 11–13);
- conducting an assessment of risks and the impact on fundamental rights;
- guaranteeing human supervision and auditability of automated decisions;
- establishing internal procedures for post-sale monitoring and incident notification (Art. 9–13 AI Act).

For small and medium-sized enterprises (SMEs), these requirements can constitute significant barriers to market entry. Impact studies carried out by the European Commission estimate that full implementation of the requirements could generate upfront costs of between €85,000 and €400,000 per high-risk AI system, depending on its complexity (European Commission, 2021, pp. 88–90).

However, the law also introduces support measures for SMEs, including the possibility of participating in sandbox regimes, temporary exemptions or tailored guidance for compliance. These provisions aim to maintain a balance between regulation and innovation, without disproportionately favouring large technology platforms.

b) Legal certainty and competitive advantage

In the medium and long term, some economic operators may benefit from the clarification of the regulatory framework. According to the principle of "compliance as a competitive advantage", companies that invest in ethical, secure and compliant systems could gain reputational and commercial advantages, especially in relation to the increasingly stringent requirements of consumers and business partners (Hildebrandt, 2019).

Furthermore, by establishing a common legal standard, the AI Act reduces the risk of legislative fragmentation between Member States and fosters cross-border interoperability. This harmonisation is essential for integrated digital markets and for the export of European technologies to other jurisdictions that will eventually adopt models inspired by EU law.

c) Legal liability and risk management

The Regulation does not directly regulate civil liability for damage caused by AI, but it has important implications for the existing liability regime. Obligations of technical compliance, transparency and control become standards of professional diligence, the non-compliance of which may entail contractual, tortious or criminal liability, depending on the case (European Commission, 2022).

In parallel, the European Commission has proposed a Directive on civil liability for AI systems, which is to complement the AI Act, facilitating compensation for victims in cases of damage caused by automated systems. Thus, economic operators are required to invest not only in technical compliance, but also in legal mechanisms for assurance and ethical governance.

3.2. Impact on public administrations

a) Extended responsibilities in the use of AI

Public administrations become, through the AI Act, active regulated subjects, in particular when using AI systems in sensitive areas such as:
- education (e.g. automated student assessment),
- employment (e.g. candidate selection),
- public order and criminal justice (e.g. facial recognition, predictive analytics) (Art. 6–7 AI Act and Annex III – List of high risk systems).

In these cases, authorities must ensure that the systems used comply with all applicable requirements, including registration in the European database, human supervision, auditability of decisions and the impact on fundamental rights.

Failure to comply with these obligations can lead to sanctions, litigation and loss of public trust, especially in the context in which authorities are perceived as having an increased duty of care in protecting citizens.

b) Paradigm shift in digital governance

The implementation of the AI Act obliges administrations to adopt coherent institutional strategies for AI governance, which include:
- designating compliance officers;
- developing sustainable public procurement policies (only compliant technologies);
- training public personnel on the responsible use of AI.

In the long term, this regulation can become a catalyst for the modernization of public administration, promoting an institutional culture centered on algorithmic accountability, decision-making transparency and ethical public services.

Conclusions

The European Union Regulation on Artificial Intelligence (AI Act) marks a turning point in the development of technology law at European and international level. For the first time, a general, coherent and binding regulatory framework regulates the use and development of artificial intelligence systems, in a manner that combines technological innovation with the legal imperatives of the protection of fundamental rights, security and transparency.

The analysis carried out reveals that the AI Act is built on solid legal foundations, respecting the principles of subsidiarity, proportionality and legality, and offering an adaptable regulatory architecture, through mechanisms such as risk classification, differentiated compliance obligations and sandbox regimes for controlled innovation. Thus, the regulation reflects a balanced approach, in which excessive regulation is avoided, without compromising the protection of citizens or public safety.

From the perspective of regulatory impact, the law generates a reconfiguration of legal responsibilities for developers and users of AI systems, in particular for economic actors operating in sensitive areas. In parallel, public administrations are called upon to assume an exemplary role in the ethical and transparent use of new technologies. Compliance becomes not only a legal obligation, but also a condition of institutional legitimacy and democratic trust.

This is why it is rightly stated that human rights issues are of international concern and do not fall under the domestic jurisdiction of states, which legitimizes not only the right of intervention of international bodies, but also their obligation to intervene whenever violations of human rights, which characterize any human community, are at issue (Corsei & Ștefănoaia, 2022, p. 73).

The AI Act is, in conclusion, asserting itself as a transformative instrument, not only for the EU internal market, but also as a global reference model. By promoting a regulatory framework focused on rights and responsibility, the European Union asserts its vocation as a regulatory leader in the governance of technology, in line with its legal tradition of protecting human dignity and the rule of law. It remains to be seen to what extent the effective transposition of the rules, harmonisation between Member States and continuous adaptation to technological dynamics will consolidate this framework into a living law of artificial intelligence, capable of responding to the challenges of the digital future.

References

Charter of Fundamental Rights of the European Union, 2000/C 364/01.
CJEU, Case C-376/98 (German Tobacco Advertising), para. 84-86.
Corsei, A.,& Ștefănoaia, M.A. (2022). Romania and Human Rights According to European Regulations. *Acta Universitatis Danubius* Vol. 18, No. 2.
Corsei, A., Zisu, M.A.,& Țoncu, S. (2023). The European Union and fundamental human rights. *AGIR Bulletin* no. 4.
European Commission. (2022). *Proposal for a Directive on adapting non-contractual civil liability rules to artificial intelligence*. COM(2022) 496 final.
Regulation (EU) 2017/745 on medical devices.
ECtHR. (2021). Case Big Brother Watch v. UK
CJEU. Case Digital Rights Ireland, C-293/12.

European Commission. (2021). *Impact Assessment Accompanying the AI Act Proposal*, SWD 84 final.

Goodman, B., & Flaxman, S. (2017). European Union regulations on algorithmic decision-making and a 'right to explanation. *AI Magazine*, 38(3).

Hildebrandt, M. (2019). Law for Computer Scientists and Other Folk. *Oxford University Press*, cap. 5.

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.

Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act – "AI Act").

TFEU – Treaty on the Functioning of the European Union.

Veale, M., & Borgesius, F. Z. (2021). Demystifying the Draft EU Artificial Intelligence Act – Analysing the Good, the Bad, and the Unclear Elements of the Proposed Approach. *Computer Law Review International*, 22(4).