REGULATING ARTIFICIAL INTELLIGENCE UNDER THE EU AI ACT: LEGAL OBLIGATIONS, ENFORCEMENT AND IMPLEMENTATION CHALLENGES

Heldi KODRA

Student, Faculty of Law, University of Tirana
e-mail: heldi_kodra.fdstudent@unitir.edu.al

Abstract

This article examined the European Union Artificial Intelligence Act (Regulation (EU) 2024/1689) as a legal framework for the governance of artificial intelligence and assessed its implications for regulatory accountability, fundamental rights and innovation. Using a doctrinal and analytical approach, the study reviewed the legislative background of the Act, its risk-based classification of AI systems, the obligations imposed on providers and deployers, and the institutional arrangements for supervision and enforcement. Particular attention was paid to prohibited practices, high-risk systems, general-purpose AI models and transparency duties. The analysis also considered the staged application of the Act and the implementation timetable as amended in 2026, together with the preliminary-reference proceedings in Case C-806/24 concerning automated decision-making and the right to explanation. The findings indicated that the Act establishes an important common regulatory baseline while leaving significant challenges relating to implementation capacity, consistent enforcement and the relationship between regulatory duties and civil liability. The discussion further highlighted the need to distinguish systemic-risk obligations for general-purpose models from the classification of individual high-risk AI systems. The article concluded that effective AI governance requires proportionate supervision, legal clarity and continuing adaptation to technological change, without sacrificing the protection of fundamental rights or the conditions for responsible innovation.

Keywords: *artificial intelligence; EU AI Act; regulatory accountability; high-risk systems; enforcement; European Union*

1. Introduction

The rapid advancement of artificial intelligence throughout the twenty-first century has raised numerous questions concerning the security and privacy of users of this technology. This is because AI mechanisms involve processing massive volumes of data and personal information. In the absence of legal regulation, users have rightly expressed concerns about the ethics and legality of exploiting such data. Since its establishment, the European Union has embodied shared values, including the protection and promotion of human rights and democratic principles. The regulation of artificial intelligence therefore had to be aligned with these principles while also supporting the functioning of the European single market. The absence of appropriate legislation would undermine confidence in technological progress and exacerbate social inequality.

2. The Road to the AI Act

In light of these developments, the European Union recognized the need for a uniform legal framework applicable throughout the Union. In 2020, following extensive consultations with stakeholders on artificial intelligence, the European Commission published the document entitled “White Paper on Artificial Intelligence – A European Approach to Excellence and Trust”. The document proposed measures to promote research and strengthen cooperation among Member States in increasing investment in AI. It paved the way for a regulatory

framework establishing legal requirements for relevant actors, with particular emphasis on high-risk applications.[1]
Following consultations and the 2020 White Paper, the Commission presented its proposal on 21 April 2021. The European Parliament adopted its position in March 2024; Regulation (EU) 2024/1689 was published in the Official Journal on 12 July 2024 and entered into force on 1 August 2024. Its provisions apply in stages. The original application timetable was subsequently amended by Regulation (EU) 2026/1744 (Digital Omnibus on AI), which entered into force on 27 July 2026.

3. Content of the AI Act and its Relevant Provisions

The AI Act is based on defining and regulating artificial intelligence systems according to the level of risk they pose in their use or deployment. It also contains rules on the use of general-purpose artificial intelligence (GPAI) models. The provisions of the AI Act will be implemented alongside the existing provisions of the General Data Protection Regulation (GDPR).
General-purpose AI (GPAI) models are governed by model-specific obligations, including transparency and documentation duties; additional obligations arise for GPAI models presenting systemic risk. A computational threshold is relevant to a presumption of systemic risk for GPAI models, but does not, by itself, classify a model as a high-risk AI system under Article 6. The latter classification depends on the applicable product-safety legislation or the use cases listed in Annex III[2].
This fundamental criterion enables European institutions to classify AI systems under the AI Act. A pyramid has also been developed to illustrate the hierarchy of systems according to their respective risk levels.
At the top of the pyramid are prohibited AI practices, including:

- The use of manipulative or deceptive techniques to alter the behavior of one or more persons, impair their ability to make informed decisions, and cause significant harm;
- Exploitation of vulnerabilities arising from age, disability, or socioeconomic circumstances, causing significant harm;
- The use of biometric categorization systems that infer ethnicity, political opinions, trade union membership, religious or philosophical beliefs, or sexual life and orientation (except where used for law-enforcement purposes);
- AI systems that evaluate or classify individuals or groups based on social behavior or personal characteristics, resulting in harmful or disproportionate treatment in unrelated contexts or treatment that is unjustified or disproportionate to their behavior;
- "Real-time" remote biometric identification in publicly accessible spaces for law-enforcement purposes (except for specific and necessary objectives, such as searching for victims of abduction or sexual exploitation or missing persons, preventing substantial and imminent threats to security, or identifying suspects of serious crimes);
- AI systems that assess an individual's risk of committing criminal offenses solely on the basis of profiling or personality traits and characteristics (except where they support human assessments based on objective and verifiable facts linked to criminal activity);
- AI systems that create or expand facial-recognition databases through untargeted collection of data from the internet or closed-circuit television (CCTV) footage;

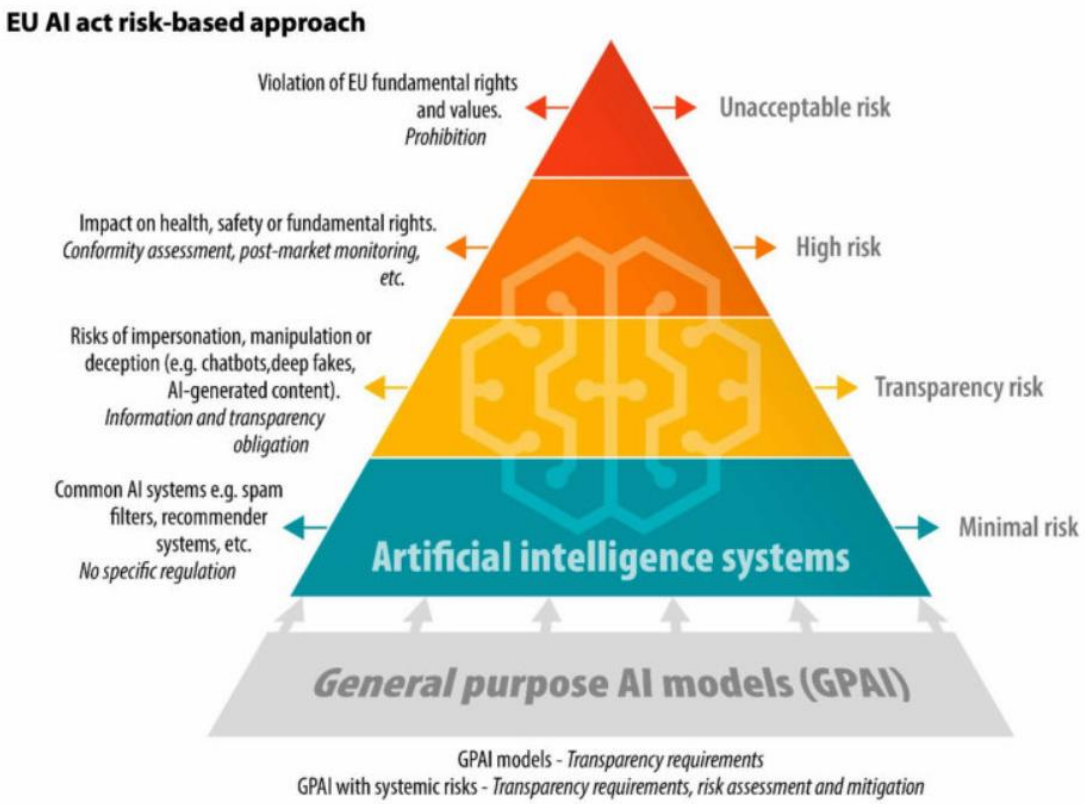
[1] https://digital-strategy.ec.europa.eu/en/consultations/white-paper-artificial-intelligence-european-approach-excellence-and-trust - 19 February 2020
[2] Giannelli, Nicola. "The European Union Policy Design for AI Regulation." Working Papers Series in Economics, Mathematics and Statistics, 2024, p. 7

- ❖ AI systems that infer emotions in workplaces or educational institutions, except for medical or safety reasons.

The next level of the pyramid comprises systems that pose transparency risks. In relation to such systems, the European Union has formulated the following description:

"Certain artificial intelligence systems intended to interact with natural persons or generate content may present specific risks of impersonation or deception, regardless of whether they are classified as high-risk AI systems. These systems are subject to information and transparency requirements. Users must be aware that they are interacting with chatbots. Deployers of AI systems that generate or manipulate visual, audio, or video content (e.g., deepfakes) must disclose that the content has been artificially generated or manipulated, except in very limited circumstances (e.g., when used for the prevention of criminal offenses). Providers of AI systems that generate large quantities of synthetic content must apply sufficiently reliable, interoperable, effective, and robust techniques and methods (such as watermarks) to enable the marking and detection of output generated or manipulated by an AI system rather than by a human. Employers using AI systems in the workplace must inform employees and their representatives."

At the base of the pyramid are systems presenting minimal risk, such as spam filters, whose use is already covered by existing legislation.[3]



Source: European Parliament, AI Act, Legislative Briefing, March 2024, p. 7

The risk-based structure establishes distinct legal consequences for prohibited practices, high-risk AI systems, transparency-related uses and other systems. The diagram above is a useful explanatory illustration, not a substitute for the operative provisions and exceptions in Articles 5, 6 and 50 and Annex III. Some biometric and emotion-recognition applications require context-specific assessment rather than automatic classification as high-risk or prohibited.

[3] Ibid., pp. 9–10

4. Obligations Imposed on Providers of Artificial Intelligence Systems

Since high-risk artificial intelligence systems include those used for biometric identification, biometric categorization, emotion recognition, creditworthiness assessment, critical infrastructure management, student assessment, risk assessment and pricing in life and health insurance, employment-related decision-making, certain law-enforcement activities, migration control, the administration of justice and elections, as well as other systems specified by law, their providers are subject to specific obligations under the AI Act. Furthermore, an AI system that constitutes a safety component of a regulated product (for example, a product subject to EU health and safety legislation), or that is itself a regulated product, will also be classified as "high-risk" (e.g., vehicles, toys, and aviation products).
These high-risk AI systems will be subject to a range of requirements, including:

- Establishing a risk-management system covering risk identification, testing, and the adoption of mitigation measures;
- Implementing data-governance and data-management practices during model training;
- Preparing and updating technical documentation and maintaining automatic event logs;
- Providing instructions for use to entities deploying the AI system;
- Ensuring human oversight (for example, including a "stop" button enabling human reviewers to interrupt the operation of the AI system);
- Achieving an appropriate level of accuracy, robustness, and cybersecurity for AI systems;
- Developing a post-market monitoring system capable of detecting malfunctions;
- Undergoing conformity-assessment procedures before being placed on the market;
- Registering the AI system in a public database administered by the European Commission;
- Notifying EU regulators if the AI system poses risks to health, personal safety, or fundamental rights, or in the event of a serious incident.[4]

5. Entry into Force, Implementation, and Enforcement of the AI Act

Regulation (EU) 2024/1689 entered into force on 1 August 2024, 20 days after publication in the Official Journal on 12 July 2024. Its provisions apply progressively: the general provisions and initial prohibitions have applied since 2 February 2025; the GPAI model rules since 2 August 2025; and major transparency provisions and enforcement arrangements since 2 August 2026. Regulation (EU) 2026/1744 revised the timetable: new prohibitions concerning certain non-consensual intimate content and child sexual abuse material apply from 2 December 2026; principal requirements for Annex III high-risk AI systems apply from 2 December 2027; and those for high-risk systems covered by Annex I product legislation apply from 2 August 2028. As the AI Act represents the first legal framework governing AI, the European Union established a dedicated authority, the European AI Office, in January 2024. This office serves as the EU-wide center of expertise on artificial intelligence, playing a key role in implementing the AI Act, particularly in relation to general-purpose AI systems, while supporting the development and trustworthy use of artificial intelligence and international cooperation. In establishing this body, the European Union emphasizes that the principal objective remains the safe and trustworthy use of AI. Other responsibilities include supporting Member States' governing bodies on AI matters, assessing general-purpose systems, supervising providers and ensuring their accountability, and imposing sanctions in cases of infringement. The AI Office also involves a broad community of specialists, civil society representatives, industry

[4] Wilson Sonsini Co. "10 Things You Should Know About the EU Artificial Intelligence Act", April 2024, p. 6

participants, and others, ensuring an inclusive approach to this sensitive issue. Most responsibility for enforcing the AI Act will fall to Member States through national supervision by designated market-surveillance authorities. Implementation will most likely be entrusted to existing institutions. It remains to be seen how data-protection authorities will position themselves in this debate. For example, the Netherlands has made clear that its national data-protection authority will bear responsibility for implementing the AI Act. In Germany, the relevant data-protection authority is advocating a key role in this regard. Nevertheless, critics remain skeptical about assigning extensive powers to fragmented domestic authorities because of political and economic overlap and uncertain levels of expertise and experience in artificial intelligence. In recent years, the Irish data-protection authority has faced criticism for its frequent dealings with US technology companies whose European subsidiaries are based in Ireland, bringing benefits primarily to the domestic economy. For general-purpose systems, whose monitoring requires greater capacity and substantial expertise, European lawmakers have assigned this responsibility to the European AI Office.
For certain infringements involving prohibited AI practices, Article 99 provides for administrative fines of up to EUR 35 million or 7% of the undertaking's total worldwide annual turnover in the preceding financial year, whichever is higher, subject to the Regulation's specific conditions and differentiated treatment of certain operators. These are administrative enforcement sanctions and should not be confused with civil compensation for harm[5].

6. The AI Act and its Interpretation by the Court of Justice of the European Union

The Court of Justice of the European Union (CJEU) has been asked to consider issues touching on Article 86 of the AI Act, but the procedural disposition of the relevant reference must be distinguished from a substantive ruling on the provision.
On 25 November 2024, the Sofia District Court submitted a request for a preliminary ruling in Case C-806/24, YETTEL BULGARIA, concerning automated billing decisions, consumer protection and the potential significance of Article 86. The case was closed by an order of the Court of Justice dated 3 June 2026 (ECLI:EU:C:2026:466).
The request concerns claims brought by a telecommunications company against a subscriber who had failed to fulfill contractual payment obligations. The subscriber, in turn, argues that the use of an automatic method for calculating charges constitutes an automated decision-making (ADM) system. Consequently, the method amounts to an ADM system subject to Article 86(1) of the AI Act, raising questions about the system's transparency and fairness.[6]
Broadly speaking, the Bulgarian court raises three groups of questions for the Court of Justice of the European Union (CJEU):

- Questions concerning the consumer's right to information and to request a review of decisions made through automated decision-making (ADM);
- Questions concerning the appropriateness of imposing a compensation charge after the contract has ended, under consumer-protection law;
- Clarification of whether a consumer may be required to bear part of the legal costs for failing to fulfill contractual obligations when the company did not explain the ADM system clearly and comprehensibly but subsequently provided an explanation during court proceedings[7].

[5] Ibid., p. 15
[6] *Any affected person who is subject to a decision taken by a deployer on the basis of the output from a high-risk AI system listed in Annex III, with the exception of systems listed under point 2 thereof, and which produces legal effects or similarly significantly affects that person in a way that they consider to have an adverse impact on their health, safety or fundamental rights, shall have the right to obtain from the deployer clear and meaningful explanations of the role of the AI system in the decision-making procedure and the main elements of the decision taken.*
[7] https://www.insideglobaltech.com/2025/02/24/cjeu-receives-questions-on-the-ai-act-relating-to-automated-decision-making/, February 2025

The first group of questions focuses on the interpretation of Article 86(1) of the Artificial Intelligence Regulation (AI Act). This provision establishes that any individual subject to a decision based on the output of a high-risk AI system that produces legal effects or significantly affects that individual is entitled to receive from the AI deployer "clear and meaningful explanations of the role of the AI system in the decision-making procedure and the main elements of the decision taken".

Among other matters, the Bulgarian court asks the following questions regarding Article 86(1) of the AI Act, read in conjunction with other EU legislation:

- Should Article 86(1) be interpreted as requiring the trader to inform the consumer how a decision is reached using ADM (in this case, for example, which algorithm calculates automatically generated bills and which elements and parameters are entered into it)?
- Does the court have the authority to require the trader to disclose the "black box" data, source code, and algorithm relating to how decisions are made using an ADM system?
- Does the consumer have the right, under Article 86(1), to request from the company an explanation or the algorithm relating to the decision-making process?
- Does the consumer have the right to request human review of ADM-based decisions, and must that human review be conducted by a judge in formal judicial proceedings?[8]

As of October 2026, Case C-806/24 has been closed by the order of 3 June 2026. Its referred questions illustrate potential tensions between automated decision-making, consumer information rights and Article 86, but they did not yield a substantive judicial interpretation of that provision. Article 86 itself concerns explanations of qualifying decisions based on the output of specified Annex III high-risk AI systems; not every automated invoice necessarily falls within its scope.

7. Regulatory Accountability, Civil Liability and Implementation Challenges

The AI Act primarily regulates the placing on the market, putting into service and use of AI systems. It imposes ex ante and continuing compliance duties, supervision and administrative penalties. It does not itself establish a general cause of action allowing every person harmed by AI to recover damages. Accordingly, regulatory accountability must be distinguished from private-law liability, which depends on other applicable EU and national rules.

The allocation of obligations is role-sensitive. Providers are responsible for duties such as conformity assessment, technical documentation, risk management and post-market monitoring when those duties apply. Deployers have separate responsibilities, including appropriate use, human oversight and, in relevant circumstances, information duties. Treating all actors as "providers" would obscure this allocation.

The Digital Omnibus amendments address implementation readiness by delaying major high-risk requirements. The postponement can reduce immediate compliance pressures but also defers some protections. Whether this balance succeeds depends on timely harmonised standards, competent national authorities and effective coordination with the European AI Office.

8. Conclusions

It is worth emphasizing that the AI Act represents not only an important legal framework for regulating artificial intelligence but also a legal innovation in the approach to a technological development with far-reaching effects. By taking the initiative as the first regulator in this field, the European Union has established a precedent expected to have an impact both within its

[8] Court of Justice of the European Union, Case C-806/24: "Summary of the request for a preliminary ruling pursuant to Article 98(1) of the Rules of Procedure of the Court of Justice", November 2024, pp. 2–4

territory and globally. This act positions the EU as a normative actor that not only responds to technological developments but also seeks to guide them toward safe, ethical use consistent with fundamental human rights.

A central aspect of the AI Act is the balance it seeks to strike between innovation and the protection of the public interest. On the one hand, clear rules aim to ensure transparency, safety, and accountability in the use of artificial intelligence; on the other, overly rigid regulation could slow technological development and affect the competitiveness of the European market relative to other powers such as the United States and China. This dilemma remains one of the greatest challenges in the practical implementation of the act.

It also remains to be seen how Member States will adapt to and implement this legal framework at the national level. Uniform implementation is essential to avoid regulatory fragmentation and ensure a functioning single market. Moreover, the AI Act is expected to directly affect relations between private actors and public institutions, requiring technology companies to invest in new compliance and control systems.

In a context of rapidly evolving technology, the AI Act is clearly a first step, but not the last. The future will require continuous revisions and adaptations to ensure that regulation does not lag behind technological developments. Thus, beyond its normative role, the act also serves a symbolic function: it demonstrates the EU's willingness to assume responsibility in a field that directly affects democracy, human rights, and economic competitiveness.

In conclusion, the AI Act is a foundational instrument of EU AI governance, but it should be understood principally as a regulatory and enforcement framework, not a comprehensive civil-liability regime. Its differentiated obligations reflect the risks and uses of AI systems and GPAI models. The 2026 amendments show that regulatory ambition must be reconciled with implementation capacity, standardisation and legal certainty. Effective application will require consistent national supervision, transparent decisions, technical expertise and judicial clarification of unresolved questions, including the scope of the right to explanation. Future research should assess the practical enforcement of the phased high-risk-system requirements and their interaction with data-protection, consumer-protection and liability rules.

References

[1] Court of Justice of the European Union. (2024). Case C-806/24, YETTEL BULGARIA: Summary of the request for a preliminary ruling pursuant to Article 98(1) of the Rules of Procedure of the Court of Justice (November 2024).

[2] Court of Justice of the European Union. (2026). Case C-806/24, YETTEL BULGARIA, Order of 3 June 2026, ECLI:EU:C:2026:466. https://curia.europa.eu/juris/liste.jsf?num=C-806/24

[3] European Commission. (2020, February 19). White Paper on Artificial Intelligence: A European approach to excellence and trust (COM(2020) 65 final). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0065

[4] European Commission. (2026). AI Act Service Desk: Article 86—Right to explanation of individual decision-making. https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-86

[5] European Commission. (2026). AI Act Service Desk: Timeline for the implementation of the EU AI Act. https://ai-act-service-desk.ec.europa.eu/en/ai-act/eu-ai-act-implementation-timeline

[6] European Parliament. (2024, March). Artificial Intelligence Act: Legislative briefing (figure on the risk-based approach, p. 7). [Exact briefing identifier to be verified against the figure source.]

[7] European Parliament and Council of the European Union. (2024). Regulation (EU) 2024/1689 of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union, L 2024/1689, 12 July 2024. https://eur-lex.europa.eu/eli/reg/2024/1689/oj

[8] European Parliament and Council of the European Union. (2026). Regulation (EU) 2026/1744 (Digital Omnibus on AI). Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2026/1744/oj

[9] Giannelli, N. (2024). The European Union policy design for AI regulation. Working Papers Series in Economics, Mathematics and Statistics. [Working-paper number and institution not specified in original manuscript.]

[10] Gstrein, O. J., Haleem, N., & Zwitter, A. (2024). General-purpose AI regulation and the European Union AI Act. Internet Policy Review, 13(3), 1–26. https://doi.org/10.14763/2024.3.1790
[11] Inside Global Tech. (2025, February 24). CJEU receives questions on the AI Act relating to automated decision-making. https://www.insideglobaltech.com/2025/02/24/cjeu-receives-questions-on-the-ai-act-relating-to-automated-decision-making/
[12] Wilson Sonsini. (2024, April). 10 things you should know about the EU Artificial Intelligence Act. [Original source does not specify an individual author or stable publication URL.]