Is the EU AI Act future proof?

Submetido(*submitted*): 6 November 2025
Parecer(*reviewed*): 5 March 2026
Revisado(*revised*): 13 March 2026
Aceito(*accepted*): 17 March 2026

Delphine Defossez*
https://orcid.org/0000-0001-7285-0491
Lauren Napier**
https://orcid.org/0009-0004-5035-033X

Artigo submetido à revisão cega por pares (*Article submitted to peer blind review*)

DOI: https://doi.org/10.26512/lstr.v18i2.62431

Abstract

[Purpose] The EU AI Act, adopted in March 2024 and largely effective by 2026, represents the world's first comprehensive horizontal AI regulation. Building on the EU's experience with the GDPR, it employs a risk-based approach, broad definitions for AI systems and General-Purpose AI Models (GPAI) and asserts extensive extraterritorial reach. This article critically examines whether the AI Act is truly "future-proof" against AI's rapid evolution.

[Methodology/approach/design] The article employs doctrinal legal analysis of the EU AI Act's provisions, particularly its risk-based classification framework, examining the Act's structural architecture against established risk governance principles and comparing its approach with emerging national legislation and international frameworks. The analysis focuses on the interaction between Articles 5, 6, 9, 51, and 55, examining how static regulatory classifications interact with dynamic AI capabilities.

[Findings] While the Act demonstrates commendable ambition- including technology-neutral definitions, extraterritorial reach, integration with existing frameworks like the GDPR, and establishment of a centralized AI Office- it suffers from a fundamental architectural flaw that compromises its long-term viability. Key weaknesses include a highly complex and potentially slow enforcement mechanism, risks of EU consumer discrimination due to compliance burdens, and the potential for regulatory circumvention. A more fundamental flaw is the regulation of inherently dynamic AI systems through static risk classifications. This static approach creates three cascading failures. First, it cannot capture AI systems that evolve post-deployment from low-risk to high-risk. Second, rigid thresholds (particularly the 10^25 FLOPs threshold for

*Assistant Professor, Northumbria Law School, Northumbria University, Newcastle, U.K. LL.B., Maastricht University; LL.M., European University Institute; LL.M., Swansea University; Ph.D., Universidade de Brasília. Specialised in European Law, International Dispute Resolution and Aviation law with a strong interest in AI. E-mail: delphine.defossez@northumbria.ac.uk.

**Assistant Professor, Northumbria Law School, Northumbria University, Newcastle, U.K. BSc, University of North Florida; M.A International Politics, Webster University; Ph.D Northumbria University. Specialised in international law and international relations of outer space, cyber, telecommunications, and AI. E-mail: l.napier@northumbria.ac.uk.

systemic risk GPAI) incentivize regulatory arbitrage. Third, enforcement mechanisms remain reactive rather than proactive, creating a 'regulatory firefighting' approach incompatible with genuine future-proofing. While Article 9's risk management framework is theoretically sound, it operates within this static classification system and cannot compensate for the broader structural weakness.
[Practical implications] The Act represents a vital first step in AI governance, but its static classification, internal inconsistencies, and unaddressed challenges severely compromise its long-term adaptability- means it will require continuous reactive amendments to remain relevant. It is less a future-proof edifice than a foundational structure already showing cracks. The Act's static architecture is already prompting Member States to develop conflicting supplementary regulations (exemplified by Italy's AI Law), creating fragmentation rather than harmonization.

Keywords: Artificial intelligence regulation. Future-proof legislation. Risk-based approach. EU AI Act. Dynamic systems.

Resumo

[Propósito] A Lei da IA da UE, adotada em março de 2024 e amplamente em vigor até 2026, representa a primeira regulamentação horizontal abrangente sobre IA do mundo. Com base na experiência da UE com o RGPD, ela emprega uma abordagem baseada em riscos, definições amplas para sistemas de IA e Modelos de IA de Propósito Geral (GPAI) e afirma um amplo alcance extraterritorial. Este artigo examina criticamente se a Lei de IA é realmente "à prova de futuro" contra a rápida evolução da IA.
[Metodologia/abordagem/concepção] O artigo emprega uma análise jurídica doutrinária das disposições da Lei da UE sobre IA, particularmente o seu quadro de classificação baseado no risco, examinando a arquitetura estrutural da lei em relação aos princípios estabelecidos de governança de risco e comparando a sua abordagem com a legislação nacional emergente e os quadros internacionais. A análise centra-se na interação entre os artigos 5.º, 6.º, 9.º, 51.º e 55.º, examinando como as classificações regulamentares estáticas interagem com as capacidades dinâmicas da IA.
[Resultados] Embora a lei demonstre uma ambição louvável — incluindo definições tecnologicamente neutras, alcance extraterritorial, integração com estruturas existentes como o RGPD e a criação de um Gabinete de IA centralizado —, ela sofre de uma falha arquitetônica fundamental que compromete sua viabilidade a longo prazo. As principais fraquezas incluem um mecanismo de aplicação altamente complexo e potencialmente lento, riscos de discriminação dos consumidores da UE devido aos encargos de conformidade e a possibilidade de burla regulamentar. Uma falha mais fundamental é a regulamentação de sistemas de IA inerentemente dinâmicos por meio de classificações de risco estáticas. Essa abordagem estática cria três falhas em cascata. Primeiro, ela não consegue capturar sistemas de IA que evoluem após a implantação de baixo risco para alto risco. Segundo, limites rígidos (particularmente o limite de 10^25 FLOPs para risco sistêmico GPAI) incentivam a arbitragem regulatória. Terceiro, os mecanismos de aplicação continuam sendo reativos em vez de proativos, criando uma abordagem de "combate a incêndios regulatórios" incompatível com uma verdadeira preparação para o futuro. Embora a estrutura de gestão de risco do Artigo 9 seja teoricamente sólida, ela

opera dentro desse sistema de classificação estático e não pode compensar a fraqueza estrutural mais ampla.
[Implicações práticas] A lei representa um primeiro passo vital na governança da IA, mas sua classificação estática, inconsistências internas e desafios não abordados comprometem gravemente sua adaptabilidade a longo prazo, o que significa que exigirá emendas reativas contínuas para permanecer relevante. É menos uma estrutura preparada para o futuro do que uma estrutura fundamental que já mostra rachaduras. A arquitetura estática da lei já está levando os Estados-Membros a desenvolver regulamentos complementares conflitantes (exemplificados pela lei de IA da Itália), criando fragmentação em vez de harmonização.

Palavras-chave: Regulamentação da inteligência artificial; Legislação preparada para o futuro; Abordagem baseada no risco; Lei da IA da UE. Sistemas dinâmicos.

INTRODUCTION

Law in general, and EU law in particular, is in a perpetual state of evolution, striving to keep pace with societal shifts. Some of those changes are so profoundly disruptive that they demand an agile yet effective legislative response. Artificial Intelligence (AI) unequivocally falls into this category. The European Union (EU), strong from its leadership in personal data protection and the General Data Protection Regulation (GDPR), aspires to replicate this success by becoming the global standard-bearer in AI regulation in stark contrast to the more laissez-faire approaches observed in the United States (US) and the United Kingdom (UK), neither of which have yielded binding regulations.[1] (EUROPEAN UNION. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending various Regulations and Directives (Artificial Intelligence Act). OJ L, 2024/1689, 12 July 2024.) The EU is lauded as a "frontrunner in AI regulation, setting the regulatory tone for fostering trustworthy AI globally." (LARSEN E KUSPERT, 2024) Indeed, this ambition has already manifested, with the Brazilian Congress adopting *Projeto de Lei 21/20* shortly after the EU's proposal became public, establishing a legal framework for AI use in Brazil. (CAMARA DOS DEPUTADOS, 2021)

However, this pioneering position in AI regulation has been anything but effortless. Since the publication of its original proposed draft in April 2021, the EU Artificial Intelligence Act (AI Act) has received a distinctly mixed reactions from the AI industry. While the Act has been praised by some from

[1] Regulation (EU) 2024/1689, European Parliament and Council of 13 June 2024, harmonised rules on artificial intelligence, amends various regulations and directives. OJ L, 2024/1689, 12.7.2024.
US: Executive Order 14110, Safe, Secure, and Trustworthy AI, Oct 30 2023.
UK: Secretary of State for Science, Innovation and Technology, AI Regulation, Cmd 815, 2023. See also: GIKAY, 2024

establishing guardrails for responsible AI development, others (including some Member States) have fiercely criticized what they describe as regulatory overreach, heavy compliance burdens, uncertain interpretations, and a reliance on not-yet-developed resources. This significant industry pushback has not only led to calls for the EU to reassess its approach to AI regulation, but to a final text shaped by intensive negotiations and compromises, leading to concerns about its coherence and long-term viability. (TOBEY, et al., 2025) Smuha and Yeung (2025) have already argued that the values foreseen in the Act are "likely to remain primarily aspirational". (p. 33)

Following the footsteps of the GDRP, the Act has a global and significant extraterritorial reach - "companies outside the EU who use EU customer data in their AI platforms will, therefore, need to comply." (CHEE E HUMMEL, 2024) It applies to providers placing or putting AI systems into service on the EU market, irrespective of their establishment, and to deployers within the Union.[2] Crucially, it also extends to providers or deployers established outside the EU when the system's output is utilized within the European Union, or to affected individuals located there, and even to product manufacturers.[3] The Act, however, pays little attentions to distributors. This broad scope signals the EU's intent to shape global AI development and deployment.

Regulating the unknown is inherently a formidable undertaking; typically, law evolves in the wake of technological advancement or societal disruption. Yet, the EU has proactively chosen to be a 'norm entrepreneur' regarding AI, pressing to establish regulatory frameworks and responsible behaviors now. This stems from the European Commission deeming AI systems as becoming "… too important for the economy and society not to be regulated." (EUROPEAN COMMISSION, 2023) As the EU AI Act is still in its infancy – with most parts applicable as of 2026[4]– a critical assessment is vital: is the Act genuinely fit for purpose for current and, more importantly, future AI systems? In essence, is the EU AI Act future-proof? This article argues that while the Act contains commendable features, its fundamental reliance on static risk classifications for inherently dynamic AI systems critically undermines any claim to future-proofing. This architectural flaw manifests in multiple ways: regulatory arbitrage around rigid thresholds, enforcement complexity, dangerous loopholes in prohibited practices, and emerging national fragmentation as Member States attempt to fill gaps the Act cannot address.

To evaluate the future-proofing capacity of the EU AI Act, this article employs a doctrinal legal analysis of its core architecture. To move beyond a purely descriptive account, the methodology focuses on the internal mechanics of the Act, specifically examining the interaction between Articles 5 (prohibited practices), 6 and 9 (high-risk classification and management), and 51 and 55 (GPAI and systemic risk thresholds). This doctrinal approach allows for a

[2] Article 2(1)(a)
[3] Article 2(1)(c) and Article 2(1)(g) and (e)
[4] Article 113

granular assessment of how static regulatory classifications, anchored to a system's intended purpose at the point of deployment, clash with the inherently fluid and emergent capabilities of advanced AI.

The analysis further anchors this critique in comparative legal research and risk governance theory, which is also its original contribution to the burgeoning field of AI governance. The study benchmarks the Act's risk management provisions against established international standards, namely the IRGC Risk Governance Framework and ISO standards. This provides an objective metric to judge whether the Act's'continuous iterative process' is operationally robust or merely aspirational. Finally, to address the global regulatory landscape, the research employs a comparative lens by contrasting the EU framework with the Italian AI Act (2025), El Salvador's Law for the Promotion of Artificial Intelligence (2025). Further, it will consider the brand-new Council of Europe Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, exploring its potential interactions and implications for the Act's long-term relevance. (COUNCIL OF EUROPE, 2024) By exploring the potential interactions between these divergent precautionary and promotional models, this article offers a rigorous critique of the EU's attempt to govern fluid technological evolution through fixed legislative categories, therefore adding to the debate on the limits of risk-based classification.

THE EU AI ACT- WHAT IS ALL THE FUSS ABOUT?

Building on its data protection legacy, the EU is poised to enact the world's first comprehensive AI regulation. The overarching legislative intent is to empower citizens to safely engage with AI by fostering a sense of control over technological development.[5] Consequently, the Act addresses AI risks to health, safety, and fundamental rights and takes a tiered risk-based approach to evaluating AI systems.

The legislative journey, initiated with a proposal in 2021—at the nascent stages of AI as we now understand it—culminated in formal adoption by the European Parliament only in March 2024 after intense negotiations. (BENIFEI, 2024) The final text, published in the Official Journal on the 12th of July 2024, sees most provisions entering into force on the 1nd of August 2024.[6] The AI Act implements a staggered approach to application, with different provisions engaging over different periods. The European Artificial Intelligence Act (AI Act) entered into force to "… foster responsible artificial intelligence development and deployment in the EU." (EUROPEAN COMMISSION, 2024) As the "first comprehensive horizontal legal framework for AI," (WILMERHALE) the Regulation introduces EU-wide mandates on data quality, transparency, human oversight, and accountability, underpinned by a

[5] Recital 1 of the Act
[6] Article 113

core objective: to enhance the adoption of safe and trustworthy AI systems through transparency and accountability. (LAUX et al., 2024, p. 3.)

Definitions and scope

Like many concepts, a precise, universally accepted definition of AI remains elusive. (STONE et al., 2016, p. 12) Nevertheless, the EU required one, and the Commission, drawing inspiration from the widely accepted OECD definition, drafted a definition- initially criticized for its breadth. (OECD, 2019; BOURA, 2023, p. 115) Article 3(1) defines AI system as

> "a machine-based system designed to operate with varying levels of autonomy, that may exhibit adaptiveness after deployment and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments."

This definition highlights two core characteristics: varying levels of autonomy and the ability to generate outputs influencing physical or virtual environments from input. Recital 12[7] further clarifies the legislative intent, emphasizing that the definition should differentiate AI from simpler software by its "capability to infer," which "transcends basic data processing by enabling learning, reasoning, or modelling." This explicitly broad definition was a deliberate choice, intended to be technology neutral and encompass future AI innovations within the Act's scope and therefore, futureproofing the Act. (OJANEN, 2025)

A major point of contention during negotiations was the regulation of foundation models, the technology underpinning generative AIs, leading to the absence of a direct definition for generative AI. (Bertuzzi, 2023) Instead, models which are capable of generating content such as text and images falls under the category of a General Purpose AI models (GPAI), which are defined in Article 3 (63) as

[7] "The definition should be based on key characteristics of AI systems that distinguish it from simpler traditional software systems or programming approaches and should not cover systems that are based on the rules defined solely by natural persons to automatically execute operations. A key characteristic of AI systems is their capability to infer. This capability to infer refers to the process of obtaining the outputs, such as predictions, content, recommendations, or decisions, which can influence physical and virtual environments, and to a capability of AI systems to derive models or algorithms, or both, from inputs or data. The techniques that enable inference while building an AI system include machine learning approaches that learn from data how to achieve certain objectives, and logic- and knowledge-based approaches that infer from encoded knowledge or symbolic representation of the task to be solved. The capacity of an AI system to infer transcends basic data processing by enabling learning, reasoning, or modelling. The term 'machine-based' refers to the fact that AI systems run on machines"

> "an AI model, including where such an AI model is trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable of competently performing a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications."

The Act intentionally avoids being overly prescriptive about specific technologies, hoping this flexibility will extend its relevance. This definition, too, is notably broad, designed for expansive applicability.

Crucially, not all AI systems fall within the Act's purview. Exclusions include AIs "specifically developed and put into service for the sole purpose of scientific research and development" or AI for military purposes are excluded.[8] The Act also largely exempts systems under free and open-source licenses, unless they are deployed as high-risk AI or fall under Article 5 or 50.[9]

The Act deliberately cast a wide net across the AI value chain to maximize its reach.[10] The Act does not only cover AI providers, i.e., companies that develop AI systems with a view to placing them on the market or putting them into service under their own name or trademark, but also to importers and distributors in Europe.[11] Furthermore, it also applies to 'deployers', which is defined in Article 3(4) as a natural or legal persons or other body using AI under their authority in the course of their professional activities. This comprehensive scope aims to ensure accountability across all stages of an AI system's lifecycle and reach wherever EU citizens might be affected.

Strengths: designed for the long term?

The Act features several elements seemingly designed to ensure its longevity and adaptability in the face of rapid technological change. First, the EU's commitment to a technology-neutral framework is arguably its most significant future-proofing attribute. By adopting general principles adaptable to future trends and technological variations, the Act ostensibly avoids obsolescence. Its extraterritorial reach means it applies to public and private actors globally if the AI system is placed on the EU market or affects individuals within the EU.[12] This universal application, though complex, is a bold move to globalize EU standards. This exerts pressure on non-EU entities, making the Act a potential de facto global norm, which could in turn contribute to its long-term influence and effectiveness.

Second, the Act's strategic integration with existing legal frameworks, particularly the GDPR, is a clever way to build upon established regulatory

[8] Article 2(6) and (3)
[9] Article 2(12)
[10] Article 2(1)
[11] Ibid
[12] Article 2(1) (c), (e) and (g)

muscles.[13] This intersection is logical, as most AI system deployers already operate under GDPR responsibilities as data controllers and processors. (CLARK, et al., 2024) This targeted approach, focusing on the most impactful actors, aligns with other recent EU digital policies like the Digital Services Act (DSA) and Digital Markets Act (DMA), fostering regulatory coherence. This coherence suggests a consistent regulatory philosophy that might prove more resilient over time than isolated legal instruments.

Third, the Act proactively addresses potential threats to fundamental rights and the perpetuation of discrimination, crucial for its sustained societal acceptance. By mandating accountability and transparency for high-risk AIs, including requirements for deepfakes and fundamental rights impact assessments for public services, it seeks to build trust. For instance, deepfakes will be subject to a transparency obligation requiring users to be informed they are interacting with an AI system, albeit with exceptions for evidently artistic, creative, or satirical content to avoid hampering enjoyment.[14] Additionally, public bodies or private entities providing public services via high-risk systems must conduct fundamental rights impact assessments. More critically for future-proofing, its efforts to combat gender and racial biases by requiring technically robust systems, trained on sufficiently representative datasets, and mandating traceability and auditability, aim to embed ethical safeguards into the very design of AI. For instance, the high-risk systems manufacturers will need to keep documentation of the data used to train the algorithm in case of an investigation. The idea is to create a framework that automatically pushes for more equitable AI, regardless of future applications.

Regarding copyright, while a single, clear provision is absent, the Act requires developers of certain AI systems to "draw up and make publicly available a sufficiently detailed summary of the content used for training the general-purpose model" and to "put in place a policy to respect Union copyright law in particular to identify and respect, including through state of the art technologies, the reservations of rights expressed pursuant to Article 4(3) of Directive (EU) 2019/790."[15] Recital 105 clarifies that Text and Data Mining exceptions from the DSM Directive apply to AI training, aiming to increase transparency and facilitate rightsholders in exercising their rights.[16] This mechanism, while potentially insufficient for full enforcement, is designed to offer rightsholders enough information and incentive to investigate infringements. (GUADAMUZ, 2024) The public availability of summaries may also deter developers from problematic data practices. Moreover, providers are mandated to implement technologies enabling them to protect copyright holders opt-outs. The transparency requirement also grants providers with some certainty that they might not be sued if they comply with the rules. This delicate balance between copyright holders' rights and developers' interests is a

[13] Recital 10, Article 5 (h), Article 10(5), Article 26(9).
[14] Article 50(4)
[15] Article 53(1)(c) and (d)
[16] Article 107

commendable effort. It also tries to create a sustainable legal environment for creative industries alongside AI development. By increasing transparency and enabling rights holders to act, the Act attempts to build a more harmonious future where AI innovation and intellectual property rights can coexist.

Finally, the EU appears to have learned from GDPR's enforcement challenges, particularly the difficulties in cooperation among data protection authorities. The AI Act includes provisions for mutual assistance and establishes a new AI Office to centralize efforts and ensure smoother cooperation at the EU level while still mandating national authority engagement.[17] Everything will be centralised at EU level while still requiring national authorities to cooperate. (VAN QUATHEM E VALAT, 2023) While this solution will ensure better enforcement, the major downside of the AI Office relates to its limited powers.

The European AI Office is tasked with a mission to develop Union expertise and capabilities in the AI field.[18] The Office will enforce and supervise the new rules for general purpose AI models and ensure coordination regarding AI policy.[19] In other words, it will facilitate the uniform application of the Act. It will also help the Commission publish guidelines to support the practical implementation.[20] Interestingly, the AI Office as a bit of similar power as the Commission under the infringement procedure: namely it can initiate structured dialogue with the provider of general-purpose AI before taking any measures.[21] Its designation as a market surveillance authority is novel, addressing concerns about market concentration, particularly relevant given ongoing investigations into partnerships like Microsoft and OpenAI. (BERTUZZI, 2023; TAR, 2024)

The penalties outlined in Article 99 are substantial, with fines for non-compliance with prohibited practices, Article 5, reaching up to €35 million or 7% of global annual turnover, whichever is higher, reflecting the EU's cautious stance. However, any other non-compliance not related with Article 5 will be subject to a different penalty; namely "up to 15 million Euros or if the offender is an undertaking up to 3% of the total worldwide annual turnover of the preceding financial year, whichever is higher."[22] If the offence relates to the incomplete or incorrect or misleading supply of information to the national competent authorities, the fine will be of maximum "7 500 000 EUR or, if the offender is an undertaking, up to 1 % of its total worldwide annual turnover for the preceding financial year, whichever is higher."[23] Finally, if the offender is a SME which includes start-ups, the fines will be the same but the lowest amount will be taken.[24] This distinction for SMEs is important to ensure that innovation is fostered while still making sure such company comply with the Act's requirements. The substantial penalties are also intended to be a strong deterrent,

[17] Article 75
[18] Article 64
[19] Articles 75, 89 and 92
[20] Article 95
[21] Article 93(2)
[22] Article 99(4)
[23] Article 99(5)
[24] Article 99(6)

aiming to ensure compliance even as AI systems become more complex and widespread.

Moreover, the allowance for industry-developed codes of practice for GPAI models[25], which can formally be approved by the AI Office making it valid throughout the EU[26], introduces a flexible, co-regulatory element, allowing industry to define best practices that can evolve more quickly than legislation, thus contributing to the Act's practical adaptability.[27]

Weaknesses: the chinks in the future-proofing armor

Despite the aforementioned strengths, the EU AI Act exhibits critical weaknesses that severely undermine its claim to be truly 'future-proof.' These issues stem from a combination of legislative compromises, inherent difficulties in regulating a rapidly evolving technology, and predictable practical challenges.

Firstly, while the Act's global reach is ambitious, its aspiration for technology neutrality creates significant practical implementation and enforcement hurdles. The ambitious regulatory layering, requiring each Member State to designate at least one national authority for supervision, immediately raises the spectre of the same enforcement criticisms levelled against the GDPR. (BURGESS, 2022) The Act fails to introduce mechanisms for expedited enforcement, a critical omission given the rapid pace of AI development and the need for swift action to mitigate potential harms. The complex interaction between national authorities, the AI Board, and the AI Office lacks clarity, creating a governance model that is likely too complicated and inefficient due to legislative compromises. The Act does not entirely clearly define who will be responsible for what but instead requires all those authorities to ensure the good implementation of the Act. This ambiguity risks fragmenting enforcement efforts and slowing responsiveness, directly counteracting the goal of future-proofing.

Moreover, the Act's broad scope and stringent requirements could lead to discrimination against EU consumers. To avoid compliance, developers or companies might simply block access to their AI systems within the EU, leaving European users at a technological disadvantage compared to other regions. This risk is compounded by the potential for circumvention: if users employ VPNs to access otherwise restricted AIs, the legal liability of developers (who never intended their AI for EU use) becomes a murky area, especially given the Act's unclear liability provisions for distributors. The Act's ambiguous liability for distributors in such scenarios further exposes a lack of foresight regarding real-world usage patterns, directly undermining its intended reach and enforceability. This loophole could also create unfair outcomes.

The hurried nature of negotiations, particularly the push to pass the Act before the European elections, has resulted in significant lacunas and pervasive

[25] Article 56
[26] Article 56(6)
[27] Article 101(2)

vagueness within the final text which are significant inhibitors of future-proofing. (AKIN, 2024) This has regrettably left the Commission with the unenviable task of filling critical gaps, leading to an Act that is at times unnecessarily unclear and imprecise. For instance, the wording regarding authorized representatives of providers is ambiguous, leaving it unclear whether the "which are not established in the Union" clause refers to the providers or their representatives.[28] Similarly, the Act lacks precision regarding whether importers and distributors must be established within the Union.[29] Such vagueness is a critical flaw, as it inevitably creates unnecessary litigation and demands for interpretation by the Court of Justice of the European Union (CJEU), slowing down clarity and consistent application—a direct impediment to future-proofing. This contrasts sharply with the clearer drafting observed for other actors within the value chain.

Beyond these drafting lacunas, there is a more profound conceptual weakness. By focusing primarily on the system as an output, the Act risks treating AI as an ethereal entity, an approach akin to "catching smoke with one's hand." To truly capture the fluid nature of AI evolution, the regulatory lens must eventually narrow toward the algorithmic architecture - the code and training weights- where the 'intent' of the AI is first crystallized. Without a focus on the structural development of these algorithms, the Act risks merely regulating the symptoms of AI behavior rather than its source. This lack of focus on the 'black box' of the code itself makes the Act's oversight feel reactive and detached from the technical reality of how AI is built.

Perhaps the most glaring structural weakness, severely compromising future-proofing, lies in the compromised regulation of foundation models (GPAI). Initial strong proposals were significantly diluted due to pushback from France, Germany, and Italy, who advocated for self-regulation via codes of conduct, fearing that heavy regulation would stifle promising national start-ups like Mistral or Aleph Alpha. (GOVERNMENTS OF ITALY, FRANCE AND GERMANY, 2023; PIQUARD, 2023) Consequently, direct regulation of foundation models was rejected in favor of categorizing General Purpose AI Models (GPAI) into generic and systemic.[30] Generic GPAI face mere transparency obligations, while systemic GPAI, due to their perceived higher risk, are subjected to more pervasive regulation akin to operators under the Digital Service Act.[31] Worryingly, open-source models are exempted from transparency requirements unless they pose a systemic risk, creating a clear incentive for developers to release open-source models to bypass both transparency and the Regulation itself, unless they are classified as high-risk AI systems.[32]

[28] Article 2(1) (f)
[29] Article 2(1)(d)
[30] Article 51
[31] Articles 51 and 53
[32] Article 53(2) and Article 2(12)

Under Article 55(1)(c), systemic GPAI models must undertake evaluations based on "standardised protocols and tools that reflect the state of the art," including "adversarial tests" to identify and mitigate systemic risks, and must report serious incidents and ensure robust cybersecurity.[33] However, the Act fails to define the term 'incident' (Chatzipanagiotis 2026) The high systemic risk threshold (over 10^25 Floating point operations (FLOPs))[34], a political concession to fears of stifling European champions, is already out of sync with current AI trends towards developing smaller, yet powerful, models. This exceedingly high threshold is severely out of sync with current trends towards developing smaller, yet still impactful, models. This incentivizes developers to deliberately design systems to stay below the threshold, avoiding the most stringent oversight despite posing significant risks as demonstrated by models like Chat GPT-3 or Mistral. (MUKUND, 2024) Currently, only models like Chat GPT-4 and Google Gemini exceed the systemic risk threshold. Models like Mistral 7B and Phi-2 demonstrate that parameter count, and FLOPs are increasingly poor proxies for capability and risk. (HRITIK, et al) The Act's reliance on computational metrics means it will perpetually lag behind architectural innovations.

While the Act grants the European Commission the authority to classify models as high impact even if they don't meet the threshold, or to adapt thresholds based on technological developments[35], this reliance on reactive amendments means the Commission will likely be in a constant state of playing catch-up, undermining the proactive nature. The reliance on vague criteria for designating models as posing "excessive risks" further compounds this, offering broad discretion that could lead to arbitrary classifications and legal challenges. This is not future-proofing; it's regulatory firefighting.

The vagueness extends to the conditions under which a GPAI "may be considered so large as to imply excessive risks with respect to the rest of players," (GENNA, 2024) with designation left to a procedure managed solely by the European Commission based on "quite vague criteria... which can be adapted by the EC itself over time." (GENNA, 2024) This discretionary power, coupled with unhelpful, often tautological definitions in Article 3[36], will undoubtedly raise objections and likely necessitate CJEU interpretation, further delaying clarity and potentially inviting arbitrary classifications of systemic GPAI.

The substandard drafting quality of the Act itself, with unclear interactions between provisions, suggests a lack of the meticulousness needed for resilient legislation and is a concern. The interaction of various provisions is often unclear, suggesting that the final document, arguably rushed, does not meet typical EU legislative drafting standards. While the concept of impact assessment is promising, the practical failures of environmental impact

[33] Such duty exists also for developers under Article 73
[34] Article 51(2)
[35] Article 51(3) and Article 52(4)
[36] Article 3(64) and (65)

assessments and associated case law suggest that applying it to AI might similarly lead to protracted ex-post litigation rather than effective proactive mitigation. (OEP, 2024) While the lighter regulation for free and open-source GPAI models is meant to foster innovation, the challenge of identifying the "obliged subject" for compliance creates another potential loophole and remains a significant oversight.

But the most fundamental and alarming flaw lies in the risk-based approach itself, and its inherent static nature. The Act presumes AI systems will respect predefined boundaries and remain within fixed risk categories- a dangerous oversimplification for technology characterized by emergent properties and post-deployment adaptation. An AI initially classified as 'low risk' can evolve through continuous learning or unforeseen integration to pose 'high' or even 'unacceptable' risks, rendering its initial classification obsolete. The Act's framework struggles to account for this evolutionary capacity. This static classification approach, therefore, critically undermines the Act's ability to be truly "future-proof."

THE RISK-BASED APPROACH: IS IT THE RIGHT CALL?

The EU AI Act's most fundamental structural flaw is not a drafting error that can be corrected through guidance or interpretation- it is an architectural problem embedded in the Act's risk-based framework. Chapter III implements a tiered risk-based approach, dictating the requirements applicable to each tier. The Act defines risk as "the combination of the probability of an occurrence of harm and the severity of that harm"[37] and systemic risk as a

> "risk that is specific to the high-impact capabilities of general-purpose AI models, having a significant impact on the Union market due to their reach, or due to actual or reasonably foreseeable negative effects on public health, safety, public security, fundamental rights, or the society as a whole, that can be propagated at scale across the value chain"[38].

This inclusion of a probability of an occurrence of harm or a reasonably foreseeable misuse safeguards against future AI models that are not yet known by ensuring that AI is used with an intended purpose and is risk-assessed from the start. (FRASER et al., 2023) In this way, the Act is futureproofing consideration of high-risk AI that could be created and brought to market within the EU.

The EU identifies various level of risks. (MAHLER) Minimal-risk AI falls outside of the scope of the Act, such as spam filters. However, minimal-risk AI companies could still choose to comply with codes of conduct on a

[37] Article 3(2)
[38] Article 3(65)

voluntary basis. Most AI systems currently in used are likely to fall within this category. The second, is specific transparency risk AI, such as chatbots, which are only subject to the transparency requirements under Article 50. This level of risk ensures that users clearly understand they are interacting with AI and not humans. The third relates to high-risk AI systems which are subject to stricter requirements such as "… risk-mitigation systems, high-quality of data sets, clear user information, human oversight, etc" (EUROPEAN COMMISSION, 2024) before being placed on the market.[39] This category includes AI in recruitment, medical software, and any system performing profiling. Finally, unacceptable risk AI are prohibited under the Act and, therefore, banned from the European market. Unacceptable risk AI systems are those that result in unacceptable social scoring[40], exploitation of people's vulnerabilities[41], or "are considered a clear threat to people's fundamental rights." (EUROPEAN COMMISSION, 2024) These prohibited AI practices are outlined in Article 5 of the Act. The Act does not provide a general methodology to assess risks. (NOVELLI, et al., 2024; NOVELLI, 2024)

For General Purpose AI Models, the Act distinguishes between Generic GPAI, which faces only transparency obligations, and Systemic GPAI. Those exceeding 10^25 FLOPs or deemed high-impact face more pervasive regulation similar to operators under the Digital Services Act, including adversarial testing, serious incident reporting, and robust cybersecurity measures.[42]

The Fundamental mismatch

The EU AI Act's most fundamental structural flaw is not a drafting error correctable through guidance- it is an architectural problem embedded in the risk-based framework. The Act treats AI risk classification as a one-time determination made at deployment, when the defining characteristic of advanced AI systems is their capacity for post-deployment evolution. This mismatch between regulatory stasis and technological dynamism undermines any claim to future-proofing.

For instance, an AI system deploys as a 'minimal risk' customer service chatbot under Article 6- trained on general knowledge, designed for simple queries, requiring no special compliance. Post-deployment, the system continues learning. Six months later, it has developed capacity to analyse customer sentiment and flag 'problematic' users, begun making autonomous decisions about service prioritisation, integrated with other systems to access sensitive customer data, and started exhibiting emergent behaviors its designers never programmed.

Has this system evolved from 'minimal risk' to 'high-risk' under Article 6(2) and Annex III? Almost certainly. Does the Act provide mechanisms

[39] Article 6(3). See Chapter III of the Act.
[40] Recital 31
[41] Article 5(1)(b)
[42] Article 55

for automatic reclassification? No. Risk categorization under Article 6 is determined by the system's 'intended purpose' at deployment, with Recital 56 emphasizing classification depends on the function "for which the AI system is placed on the market or put into service." This creates a regulatory gap. The Act assumes AI systems have fixed, knowable purposes; risk levels remain stable throughout operational life; and providers will voluntarily reclassify systems that evolve beyond initial parameters. None of these assumptions hold for modern AI systems, particularly foundation models and adaptive learning systems.

Risk Management System: a flawed pillar?

The EU AI Act positions itself as a risk management framework, specifically for high-risk AI systems. According to Section 2, Article 9.1 the Act calls upon operators to establish, implement, document, and maintain a risk management system for high-risk AI systems.[43] Before understanding how the risk management system approach is to be interpreted and applied within the Act, it is important to consider why such a system is prevalent in the Act. A risk-based approach to governance is not novel, with precedents in sectors like aviation and automotive, and strong academic foundations from researchers like Renn and Klinke, and frameworks like the International Risk Governance Council (IRGC) Risk Governance Framework. (RENN E KLINKE, 2016) Risk governance is a broad term that, according to the IRGC, "applies the principles of governance to the identification, assessment, management, evaluation and communication of risks in the context of plural values and distributed authority." (INTERNATIONAL RISK GOVERNANCE COUNCIL, 2017, p. 5-6.) While the definition of risk governance is a bit broader than what can be implied from Article 9 of the EU AI Act as it is specifically discussing a risk management system, this management system can be part of a broader risk governance framework. Looking at the IRGC risk governance framework which includes pre-assessment, appraisal, characterisation and evaluation, and management (INTERNATIONAL RISK GOVERNANCE COUNCIL, 2017, p.9-10); the EU AI Act prescribes a similar understanding. Both the IRGC and the EU AI Act consider risk governance or risk management to be a continuous process and can be run in a sequence of steps but can also loop back to previous steps where needed. Within the EU AI Act, Article 9.2 (a-d) the steps of identification and analysis, estimation and evaluation, further evaluation, and adoption of appropriate measures is extremely close to the framework created by the IRGC. What this suggests is that Article 9 is not a completely unrealistic or novel way of addressing risk management and can be understood very clearly from an operational perspective. Speaking about the operational perspective, further to alignment with risk governance, the EU AI Act risk management system approach is also aligned with International Standards Organisation (ISO) standards 3100:2018 Risk Management - Guidelines and 23894:2023 Information Technology – Artificial Intelligence – Guidance on Risk

[43] Article 9.1

Management. Recital 65 of the Act articulates that risk management systems should identify and mitigate known and reasonably foreseeable risks especially for those high-risk AI systems relating to health, safety, and fundamental rights.

Given the broad understanding of what a risk management system should be and how it should be applied to high-risk AI systems in Article 9 and further elaborated on in Recital 65, the risk management system approach can be future proofed. Specifically, because "the risk management system should adopt the most appropriate risk-management measures in light of the state of the art in AI." This idea of keeping the risk management system up to date with AI as well as considering identifying and mitigating against reasonably foreseeable risks means that there is room for the risk management cycle to adapt and be updated as needed. However, the question arise on how can one 'reasonably foresee' capabilities that designers might not be able to predict? For instance, GPT-3 illustrates this perfectly. Initially viewed as a text completion tool, users discovered emergent capabilities only post-deployment: code generation, mathematical reasoning, multi-step planning, and rudimentary theory of mind. Had the Act been in force, GPT-3 would have been classified based on its intended text-generation purpose, not its emergent multi-modal reasoning capabilities. Article 9 also addresses testing procedures even outside of a sandbox scenario which must be in compliance with the requirements set out in Article 9. Finally, under Article 9.2 the entire life cycle of a high-risk AI system shall be understood within the risk management system as continuous iterative process and requires "regular systematic review and updating."[44]

Article 9 is indeed well-designed- for high-risk systems already properly classified. It prescribes a continuous iterative process throughout the AI system's entire lifecycle. In this narrow aspect, the Act achieves future-proofing. However, while the framework itself is designed to be dynamic, its effectiveness is critically undermined by the Act's broader limitations. The ability to "adapt and be updated as needed" within the confines of Article 9 is severely constrained by the static nature of the AI Act's overall risk classification thresholds and definitions, as discussed in the weaknesses section. The very flexibility envisioned in Article 9 (continual updates and adaptation to the state of the art) is rendered problematic by the Act's other rigidities, such as the high FLOPs threshold for systemic GPAI that encourages regulatory arbitrage, or the pervasive vagueness that necessitates constant reactive interpretation by authorities and courts. The risk management system, while conceptually robust, cannot compensate for an underlying legal framework that is already struggling to define and categorize the technology it seeks to govern, or one that lacks swift and decisive enforcement mechanisms. Thus, while Article 9 presents a well-structured approach to risk management, its practical efficacy as a future-proofing mechanism for the entire Act remains questionable due to foundational structural and definitional weaknesses.

[44] Article 9.2

MAJOR OMISSION: THE DANGEROUS LOOPHOLES IN PROHIBITED PRACTICES

Beyond the structural and definitional weaknesses, the Act contains highly concerning loopholes regarding what it purports to prohibit, particularly concerning the use of 'real-time' live facial recognition in publicly accessible spaces.

The facial recognition exception

While Article 5(1)(h) seemingly prohibits such use, the string of exceptions included effectively gut the prohibition, creating significant avenues for abuse. The Act allows use when "strictly necessary," a term left dangerously undefined. The article permits live facial recognition for critical objectives such as searching for victims of crime, preventing specific terrorist attacks, or identifying suspects of serious criminal offenses. While these aims appear noble, the breadth of these exceptions – particularly "searching for victims of crime" or "identifying suspects of serious criminal offenses" – opens a pandora's box. The ambiguity surrounding "serious criminal offenses" leaves ample room for interpretation and expansion, risking a slippery slope towards ubiquitous surveillance. Indeed, live facial recognition is allowed to help

> "(iii) the localisation or identification of a person suspected of having committed a criminal offence, for the purpose of conducting a criminal investigation or prosecution or executing a criminal penalty for offences referred to in Annex II and punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least four years."

Recital 33 of the preamble places the burden on individual Member States to define which criminal offenses would permit such surveillance, virtually guaranteeing significant disparities across the Union. This lack of harmonization, exacerbated by the right for Member States to introduce "more restrictive laws,"[45] creates a fragmented legal landscape ripe for legal uncertainty and regulatory arbitrage. Critically, this exception could even be weaponized against migrants suspected of irregular residency, if such an offense carries a minimum four-year detention period, thereby enabling disproportionate targeting based on immigration status. (AMNESTY INTERNATIONAL UK, 2024) The low four-year detention threshold appears chillingly disproportionate to the severe fundamental rights abuses this technology enables. The Act fails to impose sufficiently rigorous safeguards against the disproportionate application of these exceptions, offering little comfort that fundamental rights will not be systematically eroded.

[45] Article 5(5)

Moreover, the process for authorizing these exceptions is often opaque or relies on national judicial authorization, which may not always be subject to the robust independent oversight required for such intrusive technologies. The absence of strict, universally applied criteria for initiating and terminating such surveillance, along with a lack of clear accountability mechanisms for potential misuse, means that the de facto prohibition becomes a de jure permission for widespread deployment under loosely defined circumstances. This critical omission, or rather, the inclusion of such expansive exceptions, fundamentally undermines the Act's commitment to protecting fundamental rights and calls into question its genuine ability to future-proof against the rise of a pervasive surveillance society.

Furthermore, the exception in Article 5(1)(h)(ii) allowing for terrorism or imminent threat use carries inherent risks of perpetuating racist biases and leading to the screening of innocent individuals without consent. For instance, if Member States A uses statistics and said statistic reveals that in 70% of cases, terrorist attacks are perpetrated by males in their 30s with a beard and of a certain origin, law enforcement could ask the AI to list all the persons corresponding to this description.

The loophole widens further: the Act only bans real-time remote biometric identification for law enforcement purposes, leaving the door wide open for private entities to deploy such invasive technologies. This glaring omission fails to future-proof against widespread private surveillance.

Insufficient regulation of deepfakes and CSAM

The Act is critically under-ambitious in its regulation of deepfakes, merely subjecting them to a transparency requirement despite their devastating potential consequences.[46] Deepfakes can generate persuasive misinformation and even rewrite history. (ALI et al., 2021) Most alarmingly, there has been a significant rise in AI-generated child sexual abuse materials (CSAM), specifically the "generation of deepfake pornography featuring real children." (ATHERTON, 2024) Concrete cases underscore this chilling reality: a man in Canada sentenced to eight years for CSAM possession and production; (SEREBIN, 2023) a man in Spain digitally altering photos of girls; (INCIDENT DATABASE) and a North Carolina psychiatrist sentenced to 40 years for sexually exploiting a minor and using AI to create child pornography images. (JUSTICE.GOV) However, there are doubts as to the legal classification of those acts. (NIEDBALA, 2023)

Despite the increase in readily available child images from 'kidfluencers' (child influencers) on social media, the EU legislator inexplicably failed to include a potential ban on AIs repeatedly used for reprehensible content creation. Even more disturbing, the Act's exception to transparency obligations for "artistic or creative work" could provide a dangerous loophole for the creators of such abhorrent content. This profound oversight leaves the primary burden of addressing these heinous crimes to fragmented national laws,

[46] Article 50(4)

demonstrating a severe failure to future-proof against one of AI's most heinous foreseeable abuses.

Additional omissions

Another critical oversight is the Act's silence on the hotly debated question of copyright remuneration for AI-generated content. This omission allows Member States to enact their own, potentially conflicting, laws—as exemplified by the recent Italian Law on AI (Law No. 132 of 23 September 2025).[47] This Italian legislation explicitly clarifies that works are protected by copyright only when created by humans, and AI-assisted works require a "standard of creative character" reflecting "adequate human involvement" to qualify for protection.[48]

The practical volatility of this legal vacuum is further highlighted by the landmark case *Like Company v. Google Ireland Ltd* (Case C-250/25), currently before the Court of Justice of the European Union. Hungarian publishers allege that the Gemini AI system 'memorizes' copyrighted news articles and reproduces substantial portions of their content without permission or remuneration (HONG, 2026). This case underscores a fundamental tension: while the AI Act focuses on the 'transparency' of training data, it remains silent on whether the probabilistic outputs of such models constitute a 'reproduction' under the Digital Single Market Directive. By leaving these questions to the courts, the EU fails to provide a clear, harmonized stance, increasing legal uncertainty for both the creative industries and AI developers. Yet again, it is a missed opportunity for future-proofing the Act.

Similarly, the Act's omission of product liability claims for defective AI, deferring it to separate, potential forthcoming legislation, (European Parliament Think Tank, 2023) adds unnecessary complexity to the regulatory framework, hindering its immediate and coherent application. The Act also reveals a lack of foresight regarding open-source AI models. While free and open-source GPAI models fall outside the Regulation's scope unless deemed high-risk, the Act fails to define what constitutes an 'open-source licence'.[49] This ambiguity is perilous: is simply labelling a model 'open source' enough, or must it conform to specific FOSS (Free and Open Source Software) licenses? With myriad FOSS licenses available, the absence of clear criteria or an approval body means this critical question is left unanswered, destined for the CJEU to untangle, (GUADAMUZ, 2024) further delaying legal clarity for an increasingly vital sector of AI development.

[47] Legge 23 September 2025, n.132, Disposizioni e deleghe al Governo in materia di intelligenza artificiale
[48] THALER v. PERLMUTTER, Civil Action No. 22-1564 (BAH). D.D.C., 2023
[49] Recitals 102-104

EMERGING CHALLENGES AND FRAGMENTATIONS

The Act's loopholes and operational delays have already prompted Member States to develop their own AI regulations, threatening to create a fragmented regulatory landscape.

National initiatives: the Italian and Salvadoran examples

Italy has approved its own AI Law to complement the EU AI Act, aiming to balance opportunities with risks through an 'Italian Way' to AI. (Comunicato stampa del Consiglio dei Ministri n. 78, 2024) Similarly to the EU AI Act, the main purpose of the proposal is to establish regulatory criteria to balance the opportunities offered by recent technologies with the risks associated with improper and harmful use. As Enrica Massalin (2024) described it "Despite the harmonising intent of EU-level legislation, the country is working on an "Italian Way" to AI that will have interesting implications for companies." In fact, Gianluca Campus argued that

> "At the core of the AI Law Proposal is the national AI Governance; in particular, the attribution of competences for developing a National AI Strategy to the Department of Technical Innovation and Digital Transition within the Prime Minister Office and the appointment of AGID (Agency for Italian Digitization) and ACN (National Cybersecurity Agency) as main local competent Offices for AI (for technical and security matters respectively). In addition, the AI Law Proposal aims to authorize the government to introduce – via legislative decrees – new rules for the implementation of the EU AI Act." (CAMPUS, 2024)

Crucially, unlike the EU AI Act's more general approach, the Italian Law includes specific provisions for AI use in key economic sectors such as healthcare, employment, public administration, cybersecurity, and explicitly addresses copyright. For instance, AI are seen as a solution to improve the overall national system and living conditions of persons with disabilities. Article 11 proposes the establishment of an observatory to monitor and propose AI-related policies and strategies.[50] Employees must be informed of the use of AI, and it can only perform ancillary and support activities to avoid the materialisation of fear of machine replacement of humans. (BOURA, 2024.) Similarly, the use of AI in public administrations can be as a support tool.[51]

More importantly, this Law does not just ignore the debate surrounding copyrighted work or data and the obligation to remunerate the right holders but

[50] Osservatorio sull'adozione dei sistemi di intelligenza artificiale nel mondo del lavoro.
[51] Article 13

instead, makes the position clear. Article 24 makes it clear that works are protected by copyrights when created by humans and can be protected if AI-aided work meets a "standard of creative character" with "adequate human involvement." (CAMPUS, 2024) This reflects a precautionary, human-centric approach that seeks to protect traditional creative industries from algorithmic encroachment. This direct approach contrasts sharply with the EU Act's silence, highlighting a significant future-proofing gap in the EU framework. This inclusion seems quite normal following the 2023 Italian Supreme Court ruling which left the door open for the protection of works generated by machine learning tools as long as there is an adequate level of human involvement.[52]

Furthermore, the Italian Law deviates from the GDPR's consent age for minors by allowing those over 14, compared to 16 in the GDPR[53], to provide consent for AI system data processing, while requiring parental consent for under-14s. It also takes a different stance on risk, treating all AI systems with the same level of risk, which could make compliance daunting for businesses navigating both EU and national law. (MASSALIN, 2024)

Importantly, Article 25 of the Italian Law provides for more severe penalties for AI-related crimes, including prison sentences for unlawful deepfake dissemination (six months to three years, or one to five years if unjust damages occur), and introduces "exceptional aggravating circumstances" for offenses propagated by AI, potentially including CSAM. (LUSARDI E FARANDA, 2024) The Law also deals with deepfakes and the associated risks of misinformation by proposing some amendments to the Consolidated Text on Audiovisual and Radio Media Services. For instance, the inclusion of a general principle that prohibits the manipulation of information through AI. Similarly, to the AI Act copyright owners or rightsholders are under an obligation to clearly mark content generated by AI.

Once in force, businesses in these sectors would have to comply with both EU Regulation and Italian law. In the healthcare sector, for instance, the use of AI is already regulated in this sector through the EU AI Act but also other European Regulations specific to the sector. The Italian Law will just make regulatory compliance more costly for companies. This exemplifies how the EU Act's inadequacies are already necessitating supplementary or conflicting regulations.

In stark contrast to both the EU's silence and Italy's human-centric restrictions, El Salvador's Law for the Promotion of Artificial Intelligence and Technologies of 2025 (Decreto N.º 234) offers a radically different vision of future-proofing.[54] Rather than leaving training data rights to protracted litigation, the Salvadoran law mandates that proprietary datasets belong unambiguously to their developers, Article 23. Furthermore, registered companies receive explicit protections against judicial measures that could

[52] COURT OF CASSATION, Civil Section 1, order 1107/2023
[53] Article 8(1) GDPR
[54] Ley de Fomento a la Inteligencia Artificial y Tecnologías adopted on 6 February 2025, published 3 March 2025 Tomo 446

disrupt AI research and development as found in Article 19 a). This creates a 'regulatory safe harbor' that prioritizes developer immunity over the EU's precautionary transparency obligations. This divergence highlights a critical weakness in the AI Act: while the EU relies on 'catching smoke' through vague definitions of AI systems, other nations are successfully attracting investment by legally codifying the algorithmic assets (the data and code) as protected, shielded property.

Country/Region	**Regulatory Strategy**	**IP/Training Data Approach**	**Liability Model**
European Union	Risk-Based (Static)	Transparency & TDM Opt-outs	High (Global Turnover Fines)
Italy	Sector-Specific	Human-centric (Human input req.)	Criminal (Deepfake penalties)
El Salvador	Promotion-Based	Statutory Developer Ownership	Shielded (Sandbox/Immunity)

The Council of Europe Convention

Beyond national initiatives, the Council of Europe's adoption of the first-ever international Convention on Artificial Intelligence and Human Rights, Democracy, and the Rule of Law on 17th of May 17, 2024, represents another significant development. (COUNCIL OF EUROPE, 2024) Open to both EU and non-EU countries, this Convention aims to cover the "entire lifecycle of AI systems" to ensure consistency with human rights, democracy, and the rule of law, as set out in its Articles 1 and 3(1)(a). While the AI Act directly targets private companies within the EU market, the Convention focuses on measures taken by Signatory States to ensure AI compliance, with an exception for national security interests.[55] This Convention is broader in its coverage of activities likely to undermine human rights, democracy, and rule of law, but leaves the implementation for the private sector to individual states.[56] Its administrative authority, much like the EU AI Act, may authorize intrusive AI systems for biometric data collection.

While also adopting a risk-based approach, the Convention, despite its potential, seems to fall short of effectively filling the fundamental rights protection gaps left by the EU AI Act. These emergent national and international frameworks underscore the Act's inadequacy as a standalone solution, revealing

[55] Article 3(2)
[56] Article 3(1)(b)

a complex, rather than harmonized, future for AI governance. They underscore how the Act's ambiguities and omissions are already necessitating supplementary or even conflicting regulations, creating a complex, rather than harmonized, future for AI governance in the EU. This legal fragmentation is now being compounded by a secondary crisis: a breakdown in the Act's operational timeline.

Implementation delays and industry pressure

Adding to these concerns are significant operative delays and mounting external pressure. Reports in May 2025 indicated the European Commission might postpone application and enforcement of certain provisions, stemming from a Polish-led initiative pushing for a pause until technical standards are developed, expanded SME exemptions for high-risk AI, waivers for low-complexity systems, and creation of a cross-regulatory forum for consistency. (TOBEY et al., 2025)

This proposed delay aligns with broader Commission efforts to simplify complex EU legislation through "Omnibus packages" (e.g., green agenda, agriculture, product regulation, and even GDPR) to boost competitiveness in a fragmented geopolitical scenario. The EU has actively gathered industry feedback on the AI Act's implementation challenges, signalling a potential future "simplification exercise." Since 2021, the Commission has faced mounting industry pressure to reconsider its approach, often focusing on innovation hurdles caused by compliance uncertainty and high barriers for smaller organizations. Despite provisions for SMEs (cost reductions, simplified measures), these concerns persist. Critics also argue that supplementary compliance materials, like the General-Purpose AI Code of Practice, extend the law beyond its original purpose, unfairly burdening organizations. (RANGONE E MEGALE, 2024)

International pressure further calls into question the Act's position as the "international gold standard." Changes in administrations, both EU and trading partners, and initial implementation issues contribute to this shift. The US government has vocally disapproved, with Vice President JD Vance cautioning in February 2025 at the Paris AI Summit that excessive regulation "could kill a transformative industry," pushing for free-market innovation. (MILMO E COUREA, 2025) The US Mission to the EU has even provided feedback suggesting streamlining and deleting provisions from the Code of Practice. This disparity in US and EU approaches creates potential trade friction, likely leading to further international pressure to pause the Act's application until details are ironed out.

The biggest pressure point remains timing. Even before finalization, Member States and tech organizations worried about negotiation speed, leading to "unclear provisions and ambiguous regulations since the technology kept changing under its feet." (TOBEY, et al., 2025) Now, after enactment, many EU-operating organizations complain that critical guidance materials are significantly delayed. The General-Purpose Code of Practice, originally due

May 2025, was published in July 2025. (EUROPEAN COMMISSION) Harmonized standards from CEN-CENELEC, crucial for demonstrating compliance, have also been pushed from August 2025 to "well into 2026," leaving little time for preparation before the next wave of rules. (TOBEY et al., 2025) Even guidance on prohibited AI practices was released just two days before those provisions took effect in February 2025. (PAUL E WEISS) This cascade of delays means the AI Act is not yet fit for purpose in regulating AI, and won't be until all its components are drafted, finalized, and shared, creating immense uncertainty for businesses.

CONCLUSION

The EU AI Act stands as a commendable, pioneering legislative effort, positioning the European Union at the forefront of global AI regulation. Its ambition to establish a comprehensive, horizontal framework, its broad extraterritorial reach, and its attempt to integrate with existing data protection laws are undeniable strengths. The explicit focus on accountability, transparency, and the mitigation of bias in high-risk systems, alongside robust penalties and the establishment of a centralized AI Office, reflect a genuine commitment to fostering trustworthy AI. The conceptual soundness of its risk management system, particularly as articulated in Article 9, provides a theoretically solid framework for continuous adaptation. In this narrow aspect, the Act is indeed future-proofed, if the entities comply diligently and enforcement is robust.

However, the question of whether the EU AI Act is truly 'future-proof' must be answered with significant reservations, leaning towards a qualified 'no' in its current form. The Act is fundamentally a product of intense political negotiation, and its hurried finalization has left a legacy of pervasive vagueness, structural complexities, and critical lacunas. For instance, the European Parliament was in favour of banning AI with facial recognition while some Member States found such systems were important in the law enforcement context. (PEETS, et al., 2021) The intricate, multi-layered governance model, coupled with a lack of fast-track enforcement mechanisms, risks replicating the very same issues that have plagued the GDPR. More fundamentally, the Act fails because it attempts to regulate inherently dynamic technology through inherently static categories. By freezing risk classifications at deployment and setting rigid thresholds, like the 10^25 FLOPs limit, the Act has built obsolescence into its architecture. This static approach does not merely risk becoming outdated- it actively incentivizes regulatory arbitrage and creates dangerous blind spots for emergent risks. The Act is therefore not 'future-proof' but rather 'present-locked,' destined to require constant reactive amendments while remaining perpetually behind the technology it purports to govern.

This explains the cascade of problems identified throughout this analysis. The 10^25 FLOPs threshold already invites arbitrage. Enforcement mechanisms are reactive rather than proactive. National authorities rush to fill gaps with conflicting legislation. Industry pushes for delays as rules quickly age.

Dangerous loopholes in prohibited practices emerge because static rules cannot anticipate dynamic applications. These are not independent failures but symptoms of the same underlying pathology: attempting to apply fixed classifications to evolving systems. Article 9's risk management framework is theoretically sound and represents genuine future-proofing- but only for systems already properly classified as high-risk. It cannot compensate for the broader framework's inability to capture systems that evolve post-deployment or deliberately design themselves to evade classification thresholds.

The Act's broader weaknesses compound this central flaw. Enforcement complexity through multi-layered governance without expedited mechanisms creates bureaucratic inertia. Pervasive vagueness and legislative gaps require constant judicial interpretation. Dangerous loopholes in facial recognition exceptions gut fundamental rights protections, while insufficient regulation of deepfakes and CSAM demonstrates failure to address foreseeable harms. National fragmentation through Member States developing conflicting supplementary laws undermines harmonization. Implementation delays with critical guidance materials released months or years late create immediate compliance uncertainty.

The Act's future-proofing is also severely undermined by its ongoing operational challenges and external pressures. The staggered application dates are already proving problematic, with significant delays in the release of crucial guidance materials, codes of practice, and harmonized standards. This means businesses are expected to comply with complex regulations without the necessary tools or clarity, creating immense uncertainty. The mounting industry and international pressure for delays and simplifications (part of a broader EU initiative) underscores that the Act, even before full implementation, is facing an uphill battle for practical viability and global acceptance.

True future-proofing would require fundamentally different design choices, each carrying distinct trade-offs in comparison to the Act's current static model. Capability-based triggers would mandate continuous monitoring with automatic reclassification based on demonstrated capabilities. While this offers superior protection against emergent risks (like those seen in GPT-3), it significantly increases regulatory uncertainty for developers, who may find their compliance obligations shifting unpredictably post-deployment. Graduated compliance would create sliding scales where requirements escalate with capabilities. This offers a more nuanced approach than the Act's binary 'high-risk vs. not' classification, potentially fostering innovation for smaller models. However, it requires a sophisticated technical oversight body capable of real-time auditing, a resource the current EU governance structure -split between national authorities and the AI Office- is not yet equipped to provide. Sunset provisions would require periodic reauthorization forcing regular reassessment. While this prevents 'built-in obsolescence,' it imposes a heavy administrative burden on both companies and regulators, risking a backlog similar to those seen in pharmaceutical licensing. The Act contains none of these. Instead, it prioritizes legal certainty and market entry at the cost of long-term technical resilience. By locking in classifications at deployment, the EU has chosen a

'snapshot' model over a dynamic 'lifecycle' model putting major burden on providers, national authorities, and the Commission to keep pace through reactive interventions.

Finally, to move beyond 'catching smoke,' future iterations of the Act must pivot from regulating the AI 'system' as a finished product to regulating the algorithmic architecture itself. Without this shift to the algorithmic 'blueprint,' the Act remains a set of limitations on an object it cannot fully grasp.

In essence, the EU AI Act represents a courageous, first-of-its-kind attempt to regulate a technology whose future contours remain largely unknown. While its intentions are laudable and some of its mechanisms are well-conceived, its practical implementation is severely hampered by its legislative compromises, its inherent static approach to dynamic AI, and its failure to adequately address foreseeable harms. The Act is a crucial stepping stone, setting global norms for AI governance, but it is less a finished, future-proof edifice and more a foundational structure that is already showing cracks and will require constant, significant amendments, reactive interventions, and extensive judicial interpretation to remain relevant and effective against the tide of technological advancement. Its true test will lie not only in its initial enforcement but in its capacity to evolve beyond its current limitations without sacrificing its core protective principles.

The EU has achieved something significant: it has moved first in comprehensive AI regulation. But moving first is not the same as building to last. Until the EU confronts the fundamental architectural flaw of static classification for dynamic systems, the AI Act will remain what it currently is: a well-intentioned but ultimately static response to a fundamentally dynamic challenge.

REFERENCES

AKIN. **Final Approval of Ground-Breaking EU AI Act**. 2024. Disponível em: https://www.akingump.com/en/insights/alerts/final-approval-of-ground-breaking-eu-ai-act. Acesso em: 29 out. 2025

ALI, Safinah et al. **Children as Creators, Thinkers and Citizens in an AI-Driven Future.** Computers and Education: Artificial Intelligence, 2021.

AMNESTY INTERNATIONAL UK. **EU proposed legislation on artificial intelligence falls short**. 2024. Disponível em: https://www.amnesty.org.uk/press-releases/eu-proposed-legislation-artificial-intelligence-falls-short?utm_source=google&utm_medium=grant&utm_campaign=BRD_AWA_GEN_dynamic-search-ads&utm_content=&gad_source=1&gclid=CjwKCAjw0aS3BhA3EiwAKaD2ZR_9E0csxwtp3q-

YxpixogshR2UXRreAxkIWCM3GZ6r5D4AgD6nchxoCo-MQAvD_BwE. Acesso em: 29 out. 2025.

ATHERTON, Daniel. **Deepfakes and Child Safety: A Survey and Analysis of 2023 Incidents and Responses**. Incident Database, 9 jan. 2024. Disponível em: https://incidentdatabase.ai/blog/deepfakes-and-child-safety/. Acesso em: 29 out. 2025.

BANSAL, Hritik et al. Smaller, Weaker, Yet Better: Training LLM Reasoners via Compute-Optimal Sampling. 2023. Disponível em: https://openreview.net/pdf?id=HuYSURUxs2. Acesso em: 22 out. 2025.

BENIFEI, Brando. Foreword by Brando Benifei AI Act: A European Way for Artificial Intelligence. In: PEHLIVAN, C. Necati; FORGO, N.; VALCKE, P. (Eds.). **The EU Artificial Intelligence (AI) Act: A Commentary**. Wolter Kluwer, 2024.

BERTUZZI, L. The AI Act: Negotiations bloquees a cause de divergences sur les modeles de fondation. **EURACTIV**, 2023. Disponível em: https://www.euractiv.fr/section/intelligence-artificielle/news/ai-act-negociations-bloquees-a-cause-de-divergences-sur-les-modeles-de-fondation/. Acesso em: 29 out. 2025.

BERTUZZI, Luca. Are EU regulators ready for concentration in the AI market?. **Euractiv**, 7 nov. 2023. Disponível em: https://www.euractiv.com/section/artificial-intelligence/news/are-eu-regulators-ready-for-concentration-in-the-ai-market/. Acesso em: 29 out. 2025.

BOURA, Marta. The Digital Regulatory Framework through EU AI Act: The Regulatory Sandboxes' Approach. **Athens Journal of Law**, Athena, v. 10, 2024, p. 387.

BURGESS, M. How GDPR is Failing. **Wired**, 2022. Disponível em: https://www.wired.com/story/gdpr-2022/. Acesso em: 29 out. 2025.

CÂMARA DOS DEPUTADOS. **Câmara aprova projeto que regulamenta uso da inteligência artificial**. 29 set. 2021. Disponível em: https://www.camara.leg.br/noticias/811702-camara-aprova-projeto-que-regulamenta-uso-da-inteligencia-artificial?utm_source=POLITICO.EU&utm_campaign=25c6120bdd-EMAIL_CAMPAIGN_2021_11_17_09_59&utm_medium=email&utm_term=0_10959edeb5-25c6120bdd-190866048. Acesso em: 29 out. 2025.

CAMPUS, Gianluca. Artificial Intelligence and Copyright: The Italian AI Law Proposal. **Kluwer Copyright Blog**, 28 maio 2024. Disponível em: https://copyrightblog.kluweriplaw.com/2024/05/28/artificial-

intelligence-and-copyright-the-italian-ai-law-proposal/. Acesso em: 29 out. 2025.

CHATZIPANAGIOTIS, Michael. Incident reporting and investigation under the AI act: some insights from aviation. **International Journal of Law and Information Technology**, Vol. 34, 2026.

CHEE, Foo Yun; HUMMEL, Tassilo. Europe sets benchmark for rest of the world with landmark AI laws. **Reuters**, 22 maio 2024. Disponível em: HYPERLINK "https://www.reuters.com/world/europe/eu-countries-back-landmark-artificial-intelligence-rules-2024-05-21/" \t "_blank" https://www.reuters.com/world/europe/eu-countries-back-landmark-artificial-intelligence-rules-2024-05-21/ . Acesso em: 29 out. 2025.

CLARK, J. et al. **Europe: The EU AI Act's relationship with data protection law: key takeaways**. DLA Piper, abr. 2024. Disponível em: HYPERLINK "https://privacymatters.dlapiper.com/2024/04/europe-the-eu-ai-acts-relationship-with-data-protection-law-key-takeaways/" \t "_blank" https://privacymatters.dlapiper.com/2024/04/europe-the-eu-ai-acts-relationship-with-data-protection-law-key-takeaways/ . Acesso em: 29 out. 2025.

CONSELHO DA EUROPA. **Council of Europe adopts first international treaty on artificial intelligence**. 2024. Disponível em: HYPERLINK "https://www.coe.int/en/web/portal/-/council-of-europe-adopts-first-international-treaty-on-artificial-intelligence" \t "_blank" https://www.coe.int/en/web/portal/-/council-of-europe-adopts-first-international-treaty-on-artificial-intelligence . Acesso em: 29 out. 2025.

COURT OF CASSATION, Civil Section 1, order 1107/2023. [Itália]. Disponível em: HYPERLINK "https://deap.web.uniroma1.it/sites/default/files/allegati/Cass_ord_1107_2023.pdf" \t "_blank" https://deap.web.uniroma1.it/sites/default/files/allegati/Cass_ord_1107_2023.pdf . Acesso em: 29 out. 2025.

EL SALVADOR. Decreto N.º 234, **Ley de Fomento a la Inteligencia Artificial y Tecnologías.** 6 fev. 2025, Tomo 446

ESTADOS UNIDOS. Executive Order 14110, **Safe, Secure, and Trustworthy AI**. 30 out. 2023.

EUROPEAN COMMISSION. **AI Act Enters into Force**. 1 ago. 2024. Disponível em: HYPERLINK "https://commission.europa.eu/news/ai-act-enters-force-2024-08-01_en" \t "_blank" https://commission.europa.eu/news/ai-act-enters-force-2024-08-01_en . Acesso em: 29 out. 2025.

EUROPEAN COMMISSION. **Artificial intelligence – questions and answers**. 12 dez. 2023. Disponível em: HYPERLINK "https://ec.europa.eu/commission/presscorner/detail/en/QANDA_21_1683" \t "_blank" https://ec.europa.eu/commission/presscorner/detail/en/QANDA_21_1683 . Acesso em: 29 out. 2025.

EUROPEAN COMMISSION. **Contents Code GPAI**. Digital Strategy. Disponível em: https://www.google.com/search?q=https://digital-strategy.ec.europa.eu/en/policies/contents-code-gpai%23:~:text%3DThe%2520General%252DPurpose%2520AI%2520(GPAI,drafting%2520process%2520of%2520the%2520code. Acesso em: 29 out. 2025.

EUROPEAN PARLIAMENT THINK TANK. **The Proposed AI Liability Directive (AILD) and the Proposed Revisions to the Product Liability Directive (PLD)**. 2023.

FRASER, Henry; BELLO Y VILLARINO, José-Miguel. Acceptable Risks in Europe's Proposed AI Act: Reasonableness and Other Principles for Deciding How Much Risk Management Is Enough. **European Journal of Risk Regulation**, v. 15, 2023, p. 431.

GENNA, I. **The Regulation of Foundation Models in the EU AI Act**. International Bar Association, 2024. Disponível em: HYPERLINK "https://www.ibanet.org/the-regulation-of-foundation-models-in-the-eu-ai-act" \t "_blank" https://www.ibanet.org/the-regulation-of-foundation-models-in-the-eu-ai-act . Acesso em: 29 out. 2025.

GIKAY, Asress Adimi. Risks, Innovation, and Adaptability in the UK's Incrementalism Versus the EU's AI Regulation. **Int. J. Law Info. Tech**, 2024.

GOVERNMENTS OF ITALY, FRANCE AND GERMANY. **An Innovation-Friendly Approach Based on European Values for the AI Act – Joint Non-Paper By IT, FR and DE**. 2023. Disponível em: HYPERLINK "https://logistic-natives.com/wp-content/uploads/2023/11/9aaf68af_2128_4aa6_b8d6_a61212e5fd46_France_German_231122_140916.pdf" \t "_blank" https://logistic-natives.com/wp-content/uploads/2023/11/9aaf68af_2128_4aa6_b8d6_a61212e5fd46_France_German_231122_140916.pdf . Acesso em: 29 out. 2025.

GUADAMUZ, Andres. **The EU AI Act and Copyright**. TechnoLlama, 14 mar. 2024. Disponível em: HYPERLINK "https://www.technollama.co.uk/the-eu-ai-act-and-copyright" \t "_blank" https://www.technollama.co.uk/the-eu-ai-act-and-copyright . Acesso em: 29 out. 2025.

HONG, Eunseo. *News publisher rails against lack of compensation for Google AI overviews in EU.* 11 March 2026. https://www.courthousenews.com/news-publisher-rails-against-lack-of-compensation-for-google-ai-overviews-in-eu/. Acesso em: 12 mar. 2026.

INCIDENT DATABASE. **Incident ID: 610**. Disponível em: HYPERLINK "https://incidentdatabase.ai/cite/610" \t "_blank" https://incidentdatabase.ai/cite/610 . Acesso em: 29 out. 2025.

INTERNATIONAL RISK GOVERNANCE COUNCIL. **Introduction to the IRGC Risk Governance Framework: Revised Edition**. IRGC, 2017.

ITÁLIA. Comunicato stampa del Consiglio dei Ministri n. 78, 23 aprile 2024. Disponível em: HYPERLINK "https://www.governo.it/it/articolo/comunicato-stampa-del-consiglio-dei-ministri-n-78/25501" \t "_blank" https://www.governo.it/it/articolo/comunicato-stampa-del-consiglio-dei-ministri-n-78/25501 . Acesso em: 29 out. 2025.

ITÁLIA. Legge n.132, Disposizioni e deleghe al Governo in materia di intelligenza artificiale. 23 sep. 2025.

JUSTICE.GOV. **Charlotte Child Psychiatrist Is Sentenced To 40 Years In Prison For Sexual Exploitation of A Minor And Using Artificial Intelligence To Create Child Pornography Images Of Minors**. 8 nov. 2023. Disponível em: HYPERLINK "https://www.justice.gov/usao-wdnc/pr/charlotte-child-psychiatrist-sentenced-40-years-prison-sexual-exploitation-minor-and" \t "_blank" https://www.justice.gov/usao-wdnc/pr/charlotte-child-psychiatrist-sentenced-40-years-prison-sexual-exploitation-minor-and . Acesso em: 29 out. 2025.

LARSEN, Benjamin Cedric; KUSPERT, Sabrina. **Regulating General-Purpose AI: Areas of Convergence and Divergence Across the EU and the US**. Brookings Institute, 21 maio 2024. Disponível em: HYPERLINK "https://www.brookings.edu/articles/regulating-general-purpose-ai-areas-of-convergence-and-divergence-across-the-eu-and-the-us/" \t "_blank" https://www.brookings.edu/articles/regulating-general-purpose-ai-

areas-of-convergence-and-divergence-across-the-eu-and-the-us/ . Acesso em: 29 out. 2025.

LAUX, J.; WATCHER, S.; MISTELSTADT, B. Trustworthy Artificial Intelligence and the European Union AI Act: On The Conflation of Trustworthiness and Acceptability Of Risk. **Govern Regulat.**, v. 18, n. 3, 2024.

LUSARDI, Giacomo; FARANDA, Alessandra. **Italian AI Bill: Main Issues and Risks**. DLA Piper, 17 maio 2024. Disponível em: HYPERLINK "https://www.technologyslegaledge.com/2024/05/italian-ai-bill-main-issues-and-risks/" \t "_blank" https://www.technologyslegaledge.com/2024/05/italian-ai-bill-main-issues-and-risks/ . Acesso em: 29 out. 2025.

MAHLER, T. **Between Risk Management and Proportionality: The Risk-Based Approach in the EU's Artificial Intelligence Act Proposal**. Disponível em: HYPERLINK "https://papers.ssrn.com/abstract=4001444" \t "_blank" https://papers.ssrn.com/abstract=4001444 . Acesso em: 29 out. 2025.

MASSALIN, Enrica. **AI Policy in Italy: Key Provisions and What You Need to Know**. Fiscal Note, 26 jul. 2024. Disponível em: HYPERLINK "https://fiscalnote.com/blog/ai-policy-italy" \t "_blank" https://fiscalnote.com/blog/ai-policy-italy . Acesso em: 29 out. 2025.

MILMO, Dan; COUREA, Eleni. US and UK refuse to sign Paris summit declaration on 'inclusive' AI. **The Guardian**, 11 fev. 2025. Disponível em: HYPERLINK "https://www.theguardian.com/technology/2025/feb/11/us-uk-paris-ai-summit-artificial-intelligence-declaration" \t "_blank" https://www.theguardian.com/technology/2025/feb/11/us-uk-paris-ai-summit-artificial-intelligence-declaration . Acesso em: 29 out. 2025.

MUKUND. **AI Chatbots Falling Short of EU Law Standards, a Stanford Study Reveals**. Weam, 2024. Disponível em: HYPERLINK "https://weam.ai/blog/ai-news/ai-chatbots-falling-short-of-eu-law/" \t "_blank" https://weam.ai/blog/ai-news/ai-chatbots-falling-short-of-eu-law/ . Acesso em: 29 out. 2025.

NIEDBALA, Marcin. The Problem of Criminal Liability for Generating Pornography Using Artificial Intelligence. **Krytyka Prawa**, v. 15, p. 69, 2023.

NOVELLI, C. L'Artificial Intelligence Act Europeo: alcune questioni di implementazione. **Federalismi.it**, v. 2, p. 2, 2024.

NOVELLI, C. et al. AI Risk Assessment: A Scenario-Based, Proportional Methodology for the AI Act. **Digital Society**, v. 3, p. 1, 2024.

OECD. **Recommendation of the Council on Artificial Intelligence**. 2019. Disponível em: HYPERLINK "https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449" \t "_blank" https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449 . Acesso em: 29 out. 2025.

OJANEN, Atte. Technology Neutrality as a Way to Future-Proof Regulation: The Case of the Artificial Intelligence Act. **European Journal of Risk Regulation**, vol. 1, p. 8, 2025.

OSSÉRVATORIO SULL'ADOZIONE DEI SISTEMI DI INTELLIGENZA ARTIFICIALE NEL MONDO DEL LAVORO.

PEETS, M. et al. **European Parliament votes in favour of banning the use of facial recognition in law enforcement**. Covington, 2021. Disponível em: HYPERLINK "https://www.insideprivacy.com/artificial-intelligence/european-parliament-votes-in-favor-of-banning-the-use-of-facial-recognition-in-law-enforcement/" \t "_blank" https://www.insideprivacy.com/artificial-intelligence/european-parliament-votes-in-favor-of-banning-the-use-of-facial-recognition-in-law-enforcement/ . Acesso em: 29 out. 2025.

RANGONE, Nicoletta; MEGALE, Luca. Risks Without Rights? The EU AI Act's Approach to AI in Law and Rule-Making. **European Journal of Risk Regulation**, v. 1, 2024

REGULAMENTO (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024. **Regras harmonizadas em matéria de inteligência artificial e que alteram diversos regulamentos e diretivas**. JO L, 2024/1689, 12 jul. 2024.

REINO UNIDO. Secretary of State for Science, Innovation and Technology. **AI Regulation**. Cmd 815, 2023.

RENN, Ortwin; KLINKE, Andreas. Risk. In: ANSELL, Christopher; TORFING, Jacob. (Ed.). **Handbook on Theories of Governance**. Edward Elgar Publishing, 2016.

SEREBIN, Jacob. Quebec Man Who Created Synthetic, AI-Generated Child Pornography Sentenced to Prison. **CBC**, 26 abr. 2023.

SMUHA, N.A.; YEUNG, K. The European Union's AI Act: Beyond Motherhood and Apple Pie?. In: SMUHA, N.A. (ed.). **The Cambridge Handbook on the Law, Ethics and Policy of Artificial Intelligence**. Cambridge University Press, 2025.

STONE, Peter et al. **Artificial Intelligence and Life in 2030: One Hundred Year Study on Artificial Intelligence: Report of the 2015-2016 Study Panel**. Stanford University, set. 2016. p. 12. Disponível em:

HYPERLINK "https://arxiv.org/pdf/2211.06318" \t "_blank" https://arxiv.org/pdf/2211.06318 . Acesso em: 29 out. 2025.

TAR, Julia. EU Commission to examine Microsoft-OpenAI partnership. **Euractiv**, 9 jan. 2024. Disponível em: HYPERLINK "https://www.euractiv.com/section/competition/news/eu-commission-to-examine-microsoft-openai-partnership/" \t "_blank" https://www.euractiv.com/section/competition/news/eu-commission-to-examine-microsoft-openai-partnership/ . Acesso em: 29 out. 2025.

THALER v. PERLMUTTER, Civil Action No. 22-1564 (BAH). D.D.C., 2023.

THE OEP. **Environmental assessments are not as effective as they should be, due to practical barriers**. 2024. Disponível em: < HYPERLINK "https://www.theoep.org.uk/report/environmental-assessments-are-not-effective-they-should-be-due-practical-barriers" \l ":~:text=implementation%2C%20says%20OEP-,Environmental%20assessments%20are%20not%20as%20effective%20as%20they%20should%20be,barriers%20to%20implementation%2C%20says%20OEP&text=Practical%20issues%20with%20how%20assessment,(OEP)%20report%20has%20found" \t "_blank" https://www.theoep.org.uk/report/environmental-assessments-are-not-effective-they-should-be-due-practical-barriers#:~:text=implementation%2C%20says%20OEP-,Environmental%20assessments%20are%20not%20as%20effective%20as%20they%20should%20be,barriers%20to%20implementation%2C%20says%20OEP&text=Practical%20issues%20with%20how%20assessment,(OEP)%20report%20has%20found .>. Acesso em: 29 out. 2025.

TOBEY, Danny et al. **The European Commission considers pause on AI Act's entry into application**. DLA Piper, 4 jun. 2025. Disponível em: HYPERLINK "https://www.dlapiper.com/en/insights/publications/ai-outlook/2025/the-european-commission-considers-pause-on-ai-act-entry-into-application" \t "_blank" https://www.dlapiper.com/en/insights/publications/ai-outlook/2025/the-european-commission-considers-pause-on-ai-act-entry-into-application . Acesso em: 29 out. 2025.

VAN QUATHEM, Kristof; VALAT, Diane. **Spain Creates AI Regulator to Enforce the AI Act**. Covington, 13 out. 2023. Disponível em: HYPERLINK "https://www.insideprivacy.com/artificial-intelligence/spain-creates-ai-regulator-to-enforce-the-ai-act/" \t "_blank" https://www.insideprivacy.com/artificial-intelligence/spain-creates-ai-regulator-to-enforce-the-ai-act/ . Acesso em: 29 out. 2025.

WEISS, Paul. **European Commission Publishes Guidance on Prohibited AI Practices under the EU AI Act**. Paul, Weiss Insights. Disponível em: HYPERLINK "https://www.paulweiss.com/insights/client-memos/european-commission-publishes-guidance-on-prohibited-ai-practices-under-the-eu-ai-act" \t "_blank" https://www.paulweiss.com/insights/client-memos/european-commission-publishes-guidance-on-prohibited-ai-practices-under-the-eu-ai-act . Acesso em: 29 out. 2025.

WILMERHALE. **Essentials of the European Union's Artificial Intelligence Act**. 2 maio 2024. Disponível em: HYPERLINK "https://www.wilmerhale.com/en/insights/events/20240502-essentials-of-the-european-unions-artificial-intelligence-act" \t "_blank" https://www.wilmerhale.com/en/insights/events/20240502-essentials-of-the-european-unions-artificial-intelligence-act . Acesso em: 29 out. 2025.

Journal of Law and Regulation
Revista de Direito Setorial e Regulatório

Contact:
Universidade de Brasília - Faculdade de Direito - Núcleo de Direito Setorial e Regulatório
Campus Universitário de Brasília
Brasília, DF, CEP 70919-970
Caixa Postal 04413

Phone: +55(61)3107-2683/2688

E-mail: ndsr@unb.br

Submissions are welcome at: https://periodicos.unb.br/index.php/RDSR