

ARTICLE

Regulation of Artificial Intelligence: The European Union's Approach and Its Impact on the Rest of the World

Alexandra Mendoza-Caminade*

Abstract

In 2024, the European Union adopted a major text to regulate artificial intelligence (AI): the AI Act. This far-reaching legislation on AI is intended to have effects beyond European borders, and its extraterritorial application could have a major impact on foreign companies in the AI sector.

A Introduction

A true technological revolution, artificial intelligence (AI) is profoundly changing our lives and societies. The development of AI systems is dazzling, as evidenced by the announcement of new models developed in China that are competing with ChatGPT, Perplexity and recent models¹. The performance of these systems offers numerous benefits in various sectors, and the potential for research is considerable. However, these systems have also generated fears: AI technologies present significant risks for individuals in terms of privacy, security and ethics and even competition for companies. Very early, the European Union (EU) decided to adopt a legal framework for AI and was the first to opt for far-reaching regulation, leading to the adoption of the AI Act. The genesis of this text, characterized by a strong political will, began with the European Commission's proposal for a regulation on 21 April 2021, establishing harmonized rules on AI.² Then the Council of the EU communicated its general approach on the text on 6 December 2022.³ However, this legislative process was disrupted by the arrival, in November 2022, of the general-purpose generative AI system ChatGPT: the adoption of the text was delayed due to this sensational appearance and the development of generative AI, which the European Commission's proposal of 21 April 2021 had not been able to anticipate. On 14 June 2023, the text,

* Full Professor of Law, Director of the Master in Intellectual Property, Director of the EPITOUL Research Team (IP/IT), Deputy Director of the Center for Business Law, Toulouse Capitole University.

1 About new Chinese AI tools: Kaiser Kuo, "Why China's AI breakthroughs should come as no surprise", <https://www.weforum.org/stories/2025/06/china-ai-breakthroughs-no-surprise/>, June, 24th, 2025.

2 European Commission, 21 April 2021, COM(2021) 206 final, Proposal for a Regulation establishing harmonized rules on AI and amending certain EU legislative acts.

3 EU Council, 6 December 2022, Artificial Intelligence Legislation: Council calls for promoting safe AI that respects fundamental rights.

amended by the European Parliament, was voted on in a plenary session, marking the start of the trilogues,⁴ and representatives of the European institutions reached an agreement on 9 December 2023. Far from the initial proposals of the Commission and the Council, the regulation evolved to result in a provisional final version made public on 2 February 2024 and adopted by the European Parliament on 13 March 2024. After the European Parliament, the Council of the EU gave its consent on 21 May 2024 to the adoption of the text. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 establishing harmonized rules on AI was published in the *Official Journal of the European Union* on 12 July 2024 and entered into force on 1 August 2024,⁵ with this application taking place in stages until 2027.

To face the global technological challenge, this first European legislative Act is characterized by a will to regulate the development of AI while promoting technological innovation. According to Article 1,

The purpose of this Regulation is to improve the functioning of the internal market and to promote the uptake of human-centric artificial intelligence (AI), while ensuring a high level of protection of health, safety, fundamental rights enshrined in the Charter, including democracy, the rule of law and environmental protection, against the harmful effects of AI systems in the Union and by supporting innovation.

Indeed, despite its many advantages and the benefits it provides, AI can present risks and "... undermine public interests and fundamental rights protected by Union law".⁶ By establishing this regulatory framework, the European legislator aims to ensure that the digital sovereignty of the EU is consistent with previous texts in the digital package, following, in particular, the General Data Protection Regulation (GDPR), the Digital Service Act and the Digital Market Act.

While sectoral approaches have been favoured by some states, such as the United States, the EU has opted for horizontal regulation of AI, covering all sectors of activity by adopting a risk-based approach. These distinct legal approaches reflect a real opposition between states regarding the preferred approach in the light of their respective political choices. A normative competition is at work at the international level and is based on the opposition between the promotion of free business innovation on the one hand and the promotion of ethical principles and risk prevention on the other hand. More than ever, European regulation is the subject of sustained criticism, particularly from American companies as well as political power: according to the Trump Administration, the European regulation on AI unfairly targets American companies to the point of constituting a form of economic taxation. Considered as specifically targeting American companies, such extraterritorial regulations could be described as trade barriers. Recently, the US Administration sent a letter to the European Commission to denounce the

4 The trilogues took place from 14 June 2023 to 9 December 2023, until a final agreement on the text was reached.

5 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401689.

6 Recitals 4 and 5.

framework for implementing the AI Act, going so far as to request the suspension of the regulation's entry into force.⁷

While it may seem difficult to reconcile these two visions, the European regulation advocates a balanced approach to protecting fundamental rights, democracy, the rule of law and environmental sustainability against the risks associated with AI, while also stimulating innovation. However, will this regulation, which has been described as the most ambitious law in the world aimed at regulating AI, achieve its objectives? Will it be implemented effectively and efficiently? The text is already generating numerous reactions, both in Europe and internationally. The merits of this AI regulation are being questioned, and debates are intense between supporters and opponents of this regulation: supporters emphasize the fact that regulation will guarantee the development of AI in an ethical, secure and equitable manner, by protecting citizens against potential abuses and by ensuring the accountability of technological actors; for others, however, overly strict regulation could hamper innovation and slow technological progress. Through its approach, sometimes described as 'over-regulation', the EU could hamper its own ability to produce world-class technology companies and reduce the competitiveness of European companies. Thus, as the EU seeks to assert its leadership in defining ethical and legal standards for AI while stimulating innovation and the competitiveness of its technology industry, one may wonder about the impact of regulation on economic development and business activity, on the AI value chain, as well as beyond the borders of the EU. Therefore, this article is not intended to provide a substantive study of EU law on AI, but to highlight the essential elements that will apply to operators regardless of their location, whether European or not. However, it appears that European regulation of AI (I) enshrines a broad and binding approach for the AI systems and models covered by the regulation and (II) imposes significant responsibility on AI stakeholders.

B Broad and Binding Regulation of Targeted AI

The approach adopted by the EU to regulate AI is based on fundamental values: a humane, ethical and responsible approach involving reliable, transparent and non-discriminatory AI. The AI Act, therefore, broadly encompasses AI technologies, regardless of the actors involved, and subjects them to a regime of stringent, graduated obligations based on risks.

I A Broad Material and Territorial Scope of Application

Based on Articles 16⁸ and 114⁹ of the Treaty on the Functioning of the European Union, the European approach is directed by the risks presented by AI tools: the legislation adopts ethical and secure governance of these technologies, with a gradation of applicable rules according to the significance of the risk of harm to

7 K. Lentschner, Washington puts pressure on European regulation of AI, *Le Figaro* 29 April 2025, p. 26.

8 Right to the protection of personal data.

9 Internal market.

society. AI systems must respect European values and fundamental rights, which leads to the requirement that AI systems be safe in terms of the risks they pose to fundamental rights: obligations are proportionate to these risks, and technologies deemed unacceptable are subject to prohibitions. However, it is first necessary to determine what AI is covered by the text. The choice of a broad definition was made for several reasons, including to align the European definition of AI with those of other institutions,¹⁰ but also to avoid rapid obsolescence of the given definition. Thus, according to Recital 12, the concept of AI system

should be closely aligned with the work of international organizations working on AI to ensure legal certainty, facilitate international convergence and wide acceptance, while providing the flexibility to accommodate the rapid technological developments in this field.

With respect to AI, the regulation covers both AI systems and general-purpose AI models. It is Article 3.1 that defines an AI system as

a machine-based system that is designed to operate with varying levels of autonomy and 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 refers to two different algorithmic approaches: machine learning and symbolic AI. Only complex systems resulting from one of these approaches will be subject to the regulation, which is not intended to govern all automated processing. Furthermore, the text refers to the general-purpose AI model, which is defined as

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, except AI models that are used for research, development or prototyping activities before they are placed on the market.

Article 3.66 specifically targets a general-purpose AI system “based on a general-purpose AI model and which has the capability to serve a variety of purposes, both for direct use as well as for integration in other AI systems”.

These definitions appear very broad due to the absence of any reference to the notion of product or service: general-purpose AI systems, like general-purpose AI

10 In particular, the definition adopted by the OECD, which defines an AI system as “an automated system that, for explicit or implicit objectives, infers, from received inputs, how to generate output results such as predictions, content, recommendations or decisions that can influence physical or virtual environments. Different AI systems exhibit varying degrees of autonomy and adaptability after deployment”: OECD Recommendation on AI, adopted on 22 May 2019 and revised on 8 November 2023.

models, could not be understood as mere products. This was, though, the initial intention of the text, which originally aimed to develop new product safety legislation applicable to the products on the European market and, specifically, applicable to AI systems. However, the global launch in November 2022 of ChatGPT, a general-purpose AI system, has forced a review of the text's philosophy, since general-purpose AI systems go beyond the notions of mere products or services. In addition, there are exclusions from the scope of the AI Act for AI systems used solely for military purposes and, more broadly, in the areas of national security. The exclusions also concern public authorities of a third country or international organizations, where these authorities or organizations use AI systems in the context of international cooperation or police and judicial cooperation agreements with the EU or with one or more member states. The AI Act also does not apply to systems specifically developed and put into service for scientific research and development purposes, nor to their results. Finally, the text also excludes free and open-source models, subject to certain exceptions.

Despite these exclusions, the definition of the subject matter of the AI Act is very broad because the European approach is transversal, based on the uses made across all sectors of activity. In addition, from a territorial point of view, the approach is focused on the European AI market, and Article 2 – relating to the scope of application – envisages heads of jurisdiction linked to the impact of AI on European territory: AI actors established on European territory are targeted, but also actors located in a third country, in particular in the event of placing on the market or putting into service of AI systems or general-purpose AI models in the EU, deployment of AI systems in the EU or use in the EU of outputs produced by an AI system. Thus, the scope of application of the text appears broad, since the regulation benefits from an extraterritorial effect. The objective of regulating the European market, therefore, leads to cases of extraterritorial application of the AI Act, involving actors who are not established in the EU but whose activities are directed there. The EU represents a very important economic market for foreign companies, not only due to its size, with its 27 countries and nearly 450 million inhabitants, but also because of its economic power. Moreover, the single market offers a privileged space for trade in the absence of customs barriers. By complying with these rules, foreign companies will be able to access the European market. It is now important to determine what the impact of this regulation will be, including outside the EU, and whether the various actors will benefit from a clear regulatory framework promoting responsible innovation and consumer trust in their AI systems and models.

Foreign companies will have to comply with European AI rules due to the extraterritoriality of the legislation: like the GDPR, the AI Act constitutes extraterritorial legislation that applies to any organization providing, distributing or deploying AI systems in the EU, regardless of its place of establishment. This objective, chosen for the scope of the text, is all the broader given that the approach is also based on the risks presented by AI systems.

II A Heavy Regime of Progressive Obligations Based on Risks

The regulation establishes a classification of AI systems according to the risk levels associated with their use: the legal regime for each AI system depends on the risks

posed by the use of the system to the values of the EU, as well as to fundamental rights and freedoms. According to Recital 6 of the AI Act, “AI should be a human-centric technology. It should serve as a tool for people, with the ultimate aim of increasing human well-being”.

In an approach described as horizontal, as opposed to sectoral, the classification ranges from minimal risk to unacceptable, and a special regime has been established for generative AI, all based on the importance of protecting fundamental rights. The regulation is not intended to govern all automated systems, and light obligations are imposed for low-risk AI systems such as chatbots. These systems are subject, in particular, to transparency obligations in order to inform the users that they are interacting with an AI or that the content has been generated by an AI.¹¹ Thus, for AI systems that generate content, in particular audio, image, video or text, included in the category of general-purpose AI systems, their providers are subject to a transparency obligation:¹² the results generated by the AI systems must be marked in a machine-readable format and identifiable as having been generated or manipulated by an AI. However, there are two exceptions to this obligation: when

AI systems perform an assistive function for standard formatting or do not substantially modify the input data provided by the deployer or their semantics, or when their use is authorized by law for the prevention, detection, investigation or prosecution of criminal offences.¹³

The purpose of the AI Act is to regulate the riskiest AI, and strict obligations are set for this type of system, with a classification targeting unacceptable risk, high risk and systemic risk AI systems.

AI systems are prohibited because they present an unacceptable risk of harm to individuals or society. Their list has been considerably extended and targets, in particular, AI systems for the purposes of cognitive manipulation of behaviour and social scoring. Predictive policing based on profiling is also prohibited, as also the use of real-time remote biometric identification systems in publicly accessible spaces for law enforcement purposes and the development of facial recognition databases through the untargeted harvesting of images from the internet.¹⁴

Furthermore, the regulation provides for the supervision of high-risk AI systems, with a view to prevention. Their authorization implies numerous due diligence obligations for operators wishing to access the European market. High-risk AI systems will have to undergo conformity assessment procedures before they can be placed on the EU market. Several provisions of the regulation allow for the identification of high-risk AI, particularly Article 6. The latter stipulates two cumulative conditions that must be met to fall into this category:

11 Ibid.

12 Biometrics, education and vocational training, employment, workforce management and access to self-employment, access and entitlement to essential private services and essential public services and social benefits, law enforcement, migration, asylum and border control management, administration of justice and democratic processes.

13 Technical standards are set within the framework of a standardization procedure under conditions specified in Art. 40.

14 Art. 8 to 15.

the system itself must constitute the product or be a safety component of the product, and the system must undergo a conformity assessment before being placed on the market or put into service. In addition, Annexes II and III provide lists of products and sectors of activity that qualify as high-risk AI. Annex II, thus, covers 20 products, including medical imaging devices and elevators, while Annex III lists eight high-risk sectors of activity, such as workforce management and access to self-employment.¹⁵

In addition to requirements guaranteeing trustworthy AI, conformity assessment procedures must be carried out before placing an AI on the EU market. In a self-assessment approach, technical standards¹⁶ must be met in order to benefit from a presumption of compliance with the regulation's obligations. Operators placing on the market or in service a high-risk AI system under the AI Act under Annex II or who develop an AI system in a sector qualified as high-risk must comply with all the due diligence obligations relating to high-risk AI systems under the Act. In particular, it is necessary to take into account a risk management system, a training data governance, a duty of transparency towards professional users of the AI system and robustness and cybersecurity obligations.¹⁷

For general-purpose AI models, a specific mechanism is provided.¹⁸ Thus, the obligations of AI providers are detailed in Article 53 of the AI Act. Certain general-purpose AI models may fall into the category of AI presenting systemic risks under Article 51. The criteria for this classification are based, in particular, on impact capabilities or on a decision by the European Commission;¹⁹ there is also a presumption of systemic risk for AI whose computing power exceeds a certain threshold.²⁰

For AI without systemic risk, the obligations imposed on providers depend on the type of licence under which the AI model is operated: under a free and open-source licence, the obligations are lighter for providers and essentially consist of compliance with copyright provisions and making a summary of the training data available to the public. For models not under an open-source licence, obligations apply, particularly regarding technical documentation, which must be established and kept up to date.

Companies must, therefore, implement a genuine self-regulation policy to meet European requirements; failing to do so, various stakeholders incur liability and are exposed to significant penalties.

C Significant Responsibility for AI Stakeholders

By identifying several categories of operators, the text puts pressure on a variety of stakeholders, who face a very complex European ecosystem.

15 See Annexes XI to XIII.

16 Art. 51.

17 Additional obligations are provided for in Art. 56, namely, "testing, risk assessment and mitigation, cybersecurity, notification of serious incidents to the AI office".

18 The operator is defined by Art. 3.8, with Article 3 being devoted to definitions.

19 Art. 3.3.

20 Recital 13.

I A Broad Scope of Application for Operators

The regulation sets out numerous obligations accompanied by heavy penalties for several categories of companies.

Grouped under the term “operator”,²¹ the companies subject to the obligations set out in the regulation are diverse. Indeed, the text broadly addresses provider, product manufacturer, deployer, authorized representative, importer or distributor. An undertaking is qualified as a provider if it is

a natural or legal person, public authority, agency or other body that develops an AI system or a general-purpose AI model or that has an AI system or a general-purpose AI model developed and places it on the market or puts the AI system into service under its own name or trademark, whether for payment or free of charge.

It will be a deployer when the AI system is used under its own authority, except where the AI system is used in the course of a personal, non-professional activity.

Other categories of actors are covered by the text and could play an important role in the chain of responsibility. Thus, the authorized representative is defined as

a natural or legal person located or established in the Union who has received and accepted a written mandate from a provider of an AI system or a general-purpose AI model to, respectively, perform and carry out on its behalf the obligations and procedures established by this Regulation.

The importer is a natural or legal person located or established in the EU who places on the market an AI system that bears the name or trademark of a natural or legal person established in a third country, while the distributor is a natural or legal person in the supply chain, other than the provider or the importer, who makes an AI system available on the EU market.

Thus, the actors targeted are clearly identified by the regulation, but their respective responsibilities appear more difficult to determine. The text primarily targets providers, who create and place on the market products and services with AI components; then deployers, who target AI users, are also subject to obligations when they use AI professionally. Other operators do not interfere directly with the AI systems, but with their placing on the market. Responsibilities are provided along the AI value chain by Article 25, and reclassification as a provider of a high-risk AI system is possible for a distributor, importer, deployer or other third party. Transfers of liability could occur within the chain, particularly in cases where providers are located outside the EU.

The respective qualifications constitute a considerable challenge given the heavy sanctions that the European Commission may impose. Under Article 99(1) of the regulation, member states shall organize the sanctions regime: “The penalties provided for shall be effective, proportionate and dissuasive. They shall take into account the interests of SMEs, including start-ups, and their economic viability”.

Financial penalties may be as high as 3% of the total worldwide turnover for the previous financial year or €15 million, whichever is higher in cases of intent or

21 Art. 99, § 4.

negligence. Providers, authorized representatives, importers, distributors or deployers who fail to comply with their obligations are liable to this penalty. In addition, penalties apply to the supply of incorrect, incomplete or misleading information to notified bodies or national competent authorities in reply to a request, with administrative fines of up to EUR 7,500,000 or, if the offender is an undertaking, up to 1% of its total worldwide annual turnover for the preceding financial year, whichever is higher.²²

According to Article 99(3), penalties are increased for the use of AI systems that pose unacceptable risks: the administrative fines can be up to a maximum of EUR 35,000,000 or, if the offender is an undertaking, up to 7 % of its total worldwide annual turnover for the preceding financial year, whichever is higher.

Given these considerable penalties, it is important to determine what impact this new regulatory framework will have on operators covered by the regulation, who are faced with a complex ecosystem.

II A Complex Legal Ecosystem for Operators

The regulation will subsequently be supplemented by numerous acts, including guidelines, standardized norms and national laws. In other words, the AI Act is not yet fully operational. Thus, a General-Purpose AI Code of Practice is currently being developed, and the European Commission has just published the third draft of this Code.²³ The EU has also launched several public consultations to gather stakeholder feedback on the development of guidelines. This is the case for high-risk AI systems, for which the EU is seeking to determine the implementation of the applicable rules, with the launch of a public consultation on 6 June 2024. In accordance with Article 6 of the regulation, on the classification of high-risk AI systems, the aim is to determine the scope of the applicable obligations, interpret the relevant provisions of the regulation and illustrate, through concrete use cases, the situations in which an AI system should or should not be classified as high risk. This ongoing consultation will enable the European Commission to fulfil its obligation to adopt guidelines, by 2 February 2026, specifying the concrete modalities for implementing Article 6.

The incompleteness of the text is likely to delay its implementation. Given the delay in developing certain standards, Commissioner Virkkunen has even considered a partial postponement of the application of the AI Act.²⁴ On 6 June 2025, she mentioned the 'Stop the Clock' mechanism that could be activated to defer the implementation of certain obligations under the AI Act. This temporary suspension mechanism could allow for the postponement of provisions for which delegated acts, such as technical standards or guidelines, have not yet been adopted. Therefore, Commissioner Virkkunen is reportedly considering a targeted

²² Art. 99, § 5.

²³ <https://digital-strategy.ec.europa.eu/en/library/third-draft-general-purpose-ai-code-practice-published-written-independent-experts>.

²⁴ Henna Virkkunen, Communication from the Commissioner for Digital Sovereignty, 6 June 2025.

postponement of certain obligations in the absence of implementing standards available within the required time frame.

Clarifications will also need to be provided regarding the relationship between the AI Act and other existing legislation. In particular, the links between the AI Act and the GDPR raise many questions and represent a significant challenge in terms of the protection of personal data by AI operators. However, AI exploits large quantities of data in an indiscriminate manner where the law on personal data distinguishes non-personal data from personal data and, within the latter, sensitive data. The GDPR and the national legislation of the EU member states affirm principles that seem to contradict practices in the field of AI, such as the principle of data minimization. Respect for the rights of the data subject induces rights that are difficult to exercise in the context of the operation of AI, such as the right of access to data, the right to object and the right to rectification and deletion. It is difficult to conceive how the prior exercise of these rights is possible. While the national information science and liberties Commission (CNIL), the competent French authority, has published measures to support companies prior to the deployment of their AI, sanctions have been imposed by other authorities for GDPR violation.²⁵ Complying with the GDPR, therefore, poses a challenge for AI operators, as does complying with other European digital regulations, including Regulation 2022/2065 of 19 October 2022 on a single market for digital services. The accumulation of potentially applicable texts requires effective coordination on the part of the European legislator and the competent authorities to ensure a clear understanding of the rules applicable to the companies concerned.

The ecosystem is all the more difficult to grasp given that the application of the AI Act is planned in stages, which complicates the understanding of the text.²⁶ Published in the *Official Journal* on 12 July 2024, the IA Act entered into force on 1 August 2024, but various stages will follow until 2027.²⁷ For example, the ban on AI systems presenting unacceptable risks entered into force on 2 February 2025. The General-Purpose AI Code of Practice was published on 10 July 2025,²⁸ in accordance with Article 56. The next stage is due on 2 August 2025, for the application of the rules for general-purpose AI models and the appointment of competent authorities at member state level. On 2 August 2026, two years after the text entered into force, almost all of the provisions of the regulation will become applicable, including the rules relating to high-risk AI systems in Annex III – “AI systems in the areas of biometrics, critical infrastructure, education, employment, access to essential public services, law enforcement, immigration and the administration of justice” – with the implementation by member state authorities of at least one regulatory sandbox. The application of the rules relating to high-risk AI systems in Annex I, which covers the categories of toys, radio equipment, *in vitro*

25 For example, on 20 December 2024, the Italian Data Protection Authority (Autorita Garante per la protezione dei dati personali) fined OpenAI €15 million for non-compliance with the GDPR of its ChatGPT service.

26 Art. 113.

27 For an overview of the calendar: <https://artificialintelligenceact.eu/implementation-timeline/>.

28 <https://digital-strategy.ec.europa.eu/en/policies/contents-code-gpai>.

diagnostic medical devices, civil aviation safety, agricultural vehicles and so,²⁹ will remain until 2 August 2027. Beyond the challenges encountered, the European Commission's objective is to achieve consistent, progressive and effective implementation of the AI regulation across the EU.

Another challenge for this is the coordination of the various authorities involved in AI regulation, as well as the protection of personal data and competition law. To enable the regulation's implementation and monitoring, several authorities will ensure proper application of the legislation, including the AI Office, which is part of the European Commission. This office is responsible for enforcing common rules across the EU in conjunction with national market surveillance authorities. There are three advisory bodies governing the AI legislation: the European Artificial Intelligence Board; the Scientific Panel, composed of independent experts in the field of AI; and the Advisory Forum, which represents a wide range of stakeholders, both commercial and non-commercial. The European Board, composed of representatives of the member states, will advise and assist the Commission and the member states in ensuring consistent and effective implementation of the AI legislation. Member states must also designate competent authorities to monitor the implementation of the legislation at their level. In France, the CNIL has been designated for this purpose.

Despite the adoption of the AI Act, the framework for AI is still largely under construction. Whether European or not, companies must integrate the constraints of this legislation, which directly targets them as major platforms providing AI systems and models, but also all others companies that use AI in their business.

Although the European market offers significant opportunities for companies, including foreign ones, they must be prepared to navigate a complex legal environment and adapt to the specific requirements of the EU.

The complexity of the legal ecosystem and the proliferation of European digital legislation raise questions about the effectiveness and efficiency of this horizontal approach. Will this regulation make it possible to regulate AI effectively and quickly? Beyond the complexity of the construction, or even the articulation with other legislation, there is the question of its adaptation to the technological evolution that has been underway since the adoption of the text. Ultimately, will Europe be able to appear as a key player in these technologies or will the cumbersome nature of the regulation risk paralysing the much-sought-after innovation? The coming months will be crucial to determine whether the EU will succeed in implementing its regulatory project.

29 Recital 50.