

Opinion | Technology | Mar 10, 2026

The Paradoxes of the European Union’s AI Regulation

Nicoletta Rangone



The EU’s regulation of AI uniquely balances innovation and the protection of fundamental rights.

The European Union has positioned itself as promoter of a “rights-driven” model to artificial intelligence (AI) governance. The EU exercised its regulatory powers to “promote the uptake of human-centric and trustworthy artificial intelligence (AI), while ensuring a high level of protection of health, safety, fundamental rights ... and supporting innovation.” The European approach aims to guarantee a high level of protection for fundamental rights and to rebalance power asymmetries by

constraining large technology companies while empowering users and smaller firms. Yet this model **faces** strong criticism—particularly in contrast with the “**market-driven**” regulatory environment of the United States and the state-driven coordinated model of China, both of which have facilitated the rise of global tech champions.

Experts **argue** that European regulation has increasingly functioned as a substitute for investment. Faced with limited fiscal capacity to support large-scale innovation, the European Commission has relied heavily on regulation as a policy lever, compensating for the absence of a coherent industrial strategy in AI.

By focusing primarily on output regulation rather than cultivating the necessary inputs for competitiveness—such as access to capital, computing infrastructure, high-quality data, and talent—the EU **risks** losing what has been described as its “cognitive sovereignty,” as non-European values and technological standards become embedded in systems deployed across Europe and might shape imagination, tastes, ideas and, ultimately, democracy. This regulatory emphasis, combined with comparatively weaker innovation ecosystems, has contributed to persistent concerns about the EU’s capacity to compete in the global AI race.

Another recurring critique **targets** innovation stagnation, despite authoritative opposing **views**. Stringent regulatory obligations may deter experimentation and delay deployment, preventing AI applications from improving everyday life for European citizens. The cumulative effect is the danger of relegating the EU to the role of a consumer rather than a producer of advanced AI technologies.

Closely **linked** to this concern is the problem of regulatory lag. Digital markets evolve at a pace that is difficult to reconcile with lengthy legislative processes, raising the possibility that by the time regulatory frameworks enter into force, they may be already outdated. This dynamic creates pressure for continuous amendments, increasing uncertainty for both regulators and regulated actors. Within this context, the EU has **struggled** to cultivate and retain AI talent, which often migrates to jurisdictions where funding opportunities, research ecosystems, and career prospects appear more robust.

At the heart of the debate lies a fundamental tension between innovation and the protection of fundamental rights. For many Europeans, **safeguarding** human dignity, privacy, and non-discrimination is not a negotiable trade-off for technological progress. This tension is especially clear in education, where future generations are shaped.

Although most people want personalized learning, few would accept their children being labelled as “slow” for years—or exposed to the risk that AI misreads emotions or invents conclusions about their inner states. The EU draws this boundary in the [EU AI Act](#): Outcome-based personalization is permitted but tightly regulated as high-risk, whereas systems that infer or analyze students’ emotions are prohibited for posing an unacceptable risk to fundamental rights. This approach blocks some educational pilots [explored](#) outside the EU. Similar tensions arise elsewhere, including the use of AI in [hiring](#) and chatbots offering [electoral advice](#).

The EU’s stated objective is not to slow innovation but to [ensure](#) that progress “remains human.” Nevertheless, this normative commitment does not preclude legitimate concerns about specific regulatory choices. The risk-based legislative model underpinning the EU AI Act, structured around predefined categories such as “unacceptable” and “high-risk,” may struggle to keep pace with emerging uses of AI that fall [outside](#) these rigid classifications. Certain applications, including AI tools used in law-making or rule-setting processes, may [evade](#) scrutiny altogether. Moreover, the risk-based framework was conceived in a pre-generative AI context. General-purpose AI models, characterized by multifunctionality and adaptability, [challenge](#) prescriptive regulatory approaches that rely on static categorizations.

These structural limitations are compounded by the sheer scale and complexity of the EU AI Act. With over 1,000 recitals, articles, and annexes, the Act [represents](#) the most extensive regulatory framework within the EU’s digital ecosystem. Its implementation is further elaborated on through guidelines, codes of practice, technical standards, and voluntary codes of conduct. Although such instruments aim to enhance clarity and compliance, their cumulative effect has been described as overregulation. This complexity risks undermining legal certainty and, paradoxically, the rule of law itself. Concerns of this nature were echoed in the 2024 [Draghi Report](#) on EU competitiveness, which warned that excessive regulatory density could deter investment and innovation.

In response to mounting criticism, the European Commission proposed a [Digital Omnibus](#) on AI, framed as a simplification exercise to support innovation and reduce compliance costs. The Omnibus, however, would introduce significant substantive changes shortly before the AI Act’s entry into force, raising serious rule-of-law concerns.

Among other measures, it would [postpone](#) the application of obligations for high-risk AI systems, including certain generative AI models, and remove registration

requirements for systems performing narrowly defined procedural or preparatory tasks. Even if these systems are exempt under the high-risk rules, they can shape outcomes, such as by selecting risky taxpayers, and even [jeopardize](#) rights, such as by introducing errors in origin determinations that affect asylum grants.

More controversially, the proposal, if enacted, would [expand](#) the legal basis for processing sensitive personal data by treating bias detection and correction as a matter of substantial public interest. In practice, this shift would move the regulatory paradigm from opt-in to opt-out, allowing companies to rely on broad assertions of anonymization to circumvent stricter data protection rules. Experts have [warned](#) that these safeguards are insufficient and particularly concerning limits on data reuse and onward transfers. The effect may be to legitimize large, previously noncompliant datasets, entrenching the advantages of dominant players while making it harder for European competitors to catch up.

Beyond these substantive implications, the Omnibus would exacerbate legal uncertainty by undermining stability and predictability. Altering core regulatory provisions just months before their application would challenge legitimate expectations and weaken trust in the regulatory framework. The proposal includes unclear and convoluted rules: In three articles, it [modifies](#) 30 articles of the AI Act and adds two new additional articles. The use of fast-track procedures [without](#) full public consultation or impact assessment further raises [concerns](#) about procedural integrity and democratic accountability—as also [stressed](#) by the [European Ombudsman](#), which investigates maladministration complaints about EU bodies—especially given the growing reliance on [omnibus legislation](#) across multiple policy areas.

Ultimately, the effectiveness of the EU AI Act will [depend](#) less on its textual ambition than on its implementation. AI governance in the EU unfolds within a complex system of multi-level governance, where EU-wide rules must be enforced by national authorities. This structure represents both a strength and a vulnerability. One key challenge lies in ensuring vertical coordination between European norms and national implementation measures. Overly burdensome domestic transposition, often [driven](#) by regulatory “gold-plating”—where the powers granted under an EU norm are extended when the directive is transposed onto national domains of individual member states, can significantly increase compliance costs and undermine the coherence of EU law. This risk is particularly acute for a technically complex instrument such as the AI Act.

A second challenge concerns horizontal coordination among member states within the EU. Although the Act [grants](#) national authorities' discretion to address local contexts, excessive divergence may erode investor confidence and fragment the internal market. Sensitive provisions allowing exemptions from conformity assessments or flexibility in sanctioning regimes require careful coordination to prevent circumvention, especially in areas such as public security, migration management, or law enforcement.

A third challenge arises from institutional fragmentation. Member states have adopted diverse approaches to designating [notifying authorities](#), independent bodies that carry out pre-market conformity assessment, and [market surveillance bodies](#), which supervise and enforce compliance with the rules for AI systems, including prohibitions and requirements for high-risk AI. Market surveillance bodies may include government-controlled agencies or formally independent regulators with varying sectoral mandates. Italy, Spain, and Ireland have authorities under government influence—prompting European Commission [criticism](#) of Italy and a call for truly independent oversight because independence must be not only formal but also substantive. Countries such as [Lithuania](#), [Cyprus](#), [Slovenia](#), [Latvia](#), and [Luxembourg](#) chose to use independent bodies. Even among these countries, mandates from their independent bodies vary. Some are in the telecommunication fields, others are in data or consumer protection. Such diversity risks generating divergent interpretations of the same legal provisions, echoing earlier [experiences](#) under the previous regulatory framework of the [General Data Protection Regulation](#).

These challenges are not unique to the EU. With due distinctions, parallels can be drawn with the United States, where AI legislation is advancing in the absence of a comprehensive federal framework—considering the limited federal guidance on AI and the numerous national bills [enacted](#)—and [cooperation](#) regime. Both systems face a shared dilemma: how to maintain coherence and legal certainty without suppressing legitimate diversity and experimentation. The comparison underscores that the central difficulty of AI governance is not merely regulatory design but also practical enforcement.

Thus, the key questions might be: How can decentralized systems—whether federal or supranational like the EU—maintain legal certainty while fostering innovation, and which coordination mechanisms across decentralized authorities provide effective consistency without over-centralization? As legal scholar [Roscoe Pound](#)

famously [observed](#), the gap between “law in books” and “law in action” determines the success of legal systems.

For AI regulation on both sides of the Atlantic, the challenge is not only to write rules that reflect societal values but also to ensure that enforcement mechanisms [promote](#) innovation, safeguard rights, and ultimately enhance human well-being. The future of AI governance will be judged not by regulatory volume but by regulatory performance.



Nicoletta Rangone is a professor of Administrative Law at LUMSA University and Director of the [Jean Monnet Centre of Excellence on Sustainable AI for Regulation on SUSTAIN-AI-REG](#).

This essay draws on the author’s presentation at the [Transatlantic Dialogue on AI and Regulation](#) held on December 10, 2025.

Tagged: AI, data governance, EU, European Union, General Data Protection Regulation