About the Author:

Chiara Dinarello

Chiara Dinarello holds a Master's degree with honours in European and International Studies. Her research focuses on security dynamics in the Middle East and the Mediterranean, with particular attention to Turkey and regional conflicts. She has gained experience in diplomatic and research settings, contributes to think tanks, and is currently expanding her expertise through an Executive Master in International Marketing, Events & Media.

About the publication:

3 Main Points:

This article investigates whether the EU AI Act can balance fundamental rights protection with economic competitiveness. While the Act strengthens a value-based approach to AI governance, its broad regulatory framework combined with considerable exceptions risk undermining both effectiveness and innovation. Ultimately, without stronger industrial support, the Act may weaken the EU's international stance rather than reinforce its global leadership

Highlight Sentence:

"Brussels has favoured a "rights-driven" model to AI governance, crowned by the adoption of the AI Act (2023), which prioritises risk mitigation and the safeguard of fundamental rights."

Definition:

AI systems defined - in accordance with the OECD definition as "a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment"

The EU's Strategic Dilemma: Balancing Rights, Innovations, and Competitiveness under the AI Act

The EU's AI Act in a Geopolitical Context

Artificial Intelligence (AI) has seamlessly spread and integrated into every aspect of human life, becoming omnipresent yet often invisible in its operations. Its influence extends beyond everyday activities into critical domains, shaping scientific progress, underpinning economic systems, and affecting international relations.

Truly, AI spearheads technological progress in fields like big data and robotics, while also transforming practices of governance and warfare - ranging from facial recognition systems used in law enforcement to the identification, prioritisation, and targeting of objectives in ongoing conflicts.

As the world appears to have entered what Mark Weiser described as an era of "*ubiquitous computing*" reality (Yoo, 2025), geopolitical competition surrounding AI has skyrocketed. While Washington and Beijing have chosen divergent strategies - respectively through a deregulated and market-driven approach and a mass mobilisation of state resources, both are investing substantial sums in start-ups, research labs and advanced semiconductors (Csernatoni, 2025). In contrast, Brussels has favoured a "rights-driven" model to AI governance, crowned by the adoption of the AI Act (2023), which prioritises risk mitigation and the safeguard of fundamental rights. Aligned with the EU's Digital Decade policy programme, the AI Act enables the European Union to project itself as a normative power in global technology governance, promoting clear rules, ethical guidelines, and specific mechanisms for the regulation of AI (Biscaia Gonçalves, 2026). Nonetheless, this piece of legislation has drawn considerable criticism and sparked vivid debates among experts, as fears that its regulatory focus may undermine the bloc's economic and technological competitiveness. These concerns are grounded, as the USA has already produced up to 40 AI foundation models, China around 15, whereas the EU has developed just three, leading many to question if enacting AI laws before actually possessing effective AI might just be regression masked behind the facade of progress. (Cabanas, Heinz 2026)

Given this context, this article will analyse the dichotomy intrinsic to the AI Act: on one hand, the need to uphold the EU's values-based regulatory model, also taking into consideration the considerable exclusion of the defence sector from the scope of the Act; on the other, the economic trade-offs that may stem from this approach.

The AI Act: A Risk-based Approach Between Human Rights Protection and Military Exception

The European Union's effort to promote a normative approach to algorithmic and computational technologies did not begin with the AI Act, but dates back in time. As early as 1995, the EU adopted the Data Protection Directive, whose principles were later updated and modernised with the introduction of the General Data Protection Regulation (GDPR) in 2016 - widely regarded as the world's strongest privacy and security law. The GDPR not only defines the fundamental rights of individuals in the digital era, but also lists clear obligations for data processors and provides for sanctions in case of non-compliance. Crucially, this regulation already reflects the human-centric approach to AI (Scarpellino, 2024), as Article 22 GDPR guarantees that "*the data subject shall have the right not to be subject to a decision based solely on automated processing* (...) *the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision*".

Against this backdrop, in 2021 the European Commission proposed the first comprehensive EU law on artificial intelligence, which was ultimately adopted in 2024 with the AI Act, designed to "*promote the uptake of human centric and trustworthy artificial intelligence (AI) while ensuring a high level of protection of health, safety, fundamental rights as enshrined in the Charter of Fundamental Rights of the European Union*" (Article 1, AI Act).

Enshrined in the very first article, this commitment underpins the Act's ambition to foster a trustworthy AI ecosystem through a risk-based approach, meaning that as the level of risk associated with an AI system increases, the greater the obligations imposed on its developers and users, up to the point where applications deemed to pose an unacceptable risk may be prohibited (Italiano, 2024). Thus, the AI Act classifies AI applications into four risk profiles. First, *unacceptable risk*, which includes AI programs that are banned within the EU,

including social scoring, biometric identification, and systems enabling behavioural manipulation. Second, *high-risk* systems, which may pose significant threats to safety or fundamental rights; this category encompasses AI used in safety components of regulated products (e.g. medical devices, automotive systems, aviation equipment), as well as applications in sensitive areas, such as border control management, health, or law enforcement, which must be registered in a dedicated database. Third, *limited risk*, primarily covering generative AI systems, which are subject to transparency requirements and copyright-related requirements to ensure users are aware that the content is AI-generated and legally compliant. Finally, low-risk systems, such as spam filters and video games, are considered to pose minimal risk and are therefore largely unregulated, even if the Union encourages MSs to adhere to voluntary codes of conduct. (Torregrosa Basco, 2026).

The obligations stemming from this risk-based approach are to be applied to all the AI systems defined - in accordance with the OECD definition 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"* (Article 3, AI Act). Despite this broad definition, the Act provides for several exceptions, the most significant of which is the "Security Exception". Reflecting Article 4(2) TEU - according to which competences related to essential State functions remain within MSs - Article 2(3) of the AI Act excludes from its scope all AI systems developed or used exclusively for military, defence, or national security purposes (Vogiatzoglou, 2024), while still formally covering dual-use AI systems. The Council's General Approach on the AI Act confirmed this exclusion, underlying that systems developed for defence and military purposes fall under the scope of public international law.

In doing so, however, it effectively leaves the most dangerous application of AI largely unregulated in the face of rapidly evolving technologies and geopolitical landscapes, notwithstanding the technology's capacity to influence and transform every dimension related to the defense realm - from innovation and industry supply

chains, to training protocols, military strategies and battle management (Csernatoni, 2024). This tension is further complicated by the inherently dual-use nature of numerous AI technologies, which can operate across both civilian and military contexts - such as drones and biometric recognition systems - thereby blurring the boundaries of the Regulation's scope. In the face of this regulatory imbalance, many analysts have raised concerns about the EU's effective ability to emerge as a global leader in AI governance. These concerns are compounded by strong backlashes from the economic and industrial sector, where the lack of a clear strategic push to scale up domestic innovation and investment in AI has called into question the Union's regulatory credibility.

The Limits of a Regulatory Superpower: Can the EU move on without a credible industrial policy?

The core tension of the AI Act lies within its own distinctive feature and strength: extensive regulation. Truly, many fear that the vast regulatory framework embedded in the Regulation risks constraining innovation in a strategically vital field. Particularly, three main critiques have been directed at the AI Act. Firstly, by placing excessive emphasis on regulating outputs, rather than developing the necessary conditions required for competitiveness - including access to capital, high-quality data, and domestic talent - the EU might undermine its "cognitive sovereignty", as external technological standards and non-European values become embedded in AI systems operating within the Union. Secondly, the strict regulatory framework may hinder innovation, discouraging experimentation and delaying the deployment of AI technologies. Lastly, the rapid evolution of the AI market and technologies is in stark contrast with the slower pace of the legislative process, raising the risk that regulatory frameworks may already be outdated by the time they are implemented (Rangone, 2026). These critiques reflect structural weaknesses in the European AI market. Although the EU boasts 30% more AI professionals per capita than the US, it struggles to retain this talent, as more attractive funding opportunities and career prospects are found across the ocean. At the same time, a substantial gap exists in

investment levels: while the US allocates up to $60-70 billion annually to AI ventures, the EU invests only around $7-8 billion. This disparity is also reflected in early-stage financing, with European AI startups raising approximately $8.5 million in initial funding rounds, compared to roughly $13 million in the US. Collectively, these differences undermine the ability of startups to scale, adopt AI technologies more broadly, and compete effectively for talent, leaving the EU heavily dependent on external players, as leading AI language models are either American or Chinese (Cabanas & Heinz 2026).

Concerns of this nature were also enshrined in the 2024 Draghi Report on EU competitiveness, which criticized Europe's stagnating innovation and regulatory approach, and urged the EU to: strengthen its position in the AI global landscape, by securing a competitive edge in key industrial sectors - such as robotics and biotechnology - through the development of sectors specific AI models; expand its computing capacity, by scaling up the EuroHPC network to better support research; ensure control over data security and residency within European infrastructures; and, advance research in quantum computing and integrating it with high-performance computing system as a central pillar of the EU's long-term technological strategy (Draghi, 2024).

To address these challenges, on November 19th, 2025, the Commission published a proposal for a Digital Omnibus on AI as a part of a broader digital package aimed at simplifying and enhancing the effectiveness of the AI Act and all the others european digital laws - helping domestic business to innovate, scale, and save on administrative costs - simultaneously ensuring fundamental rights protection (Briefing EU, 2026). While the package is yet to be approved through the ordinary legislative process of the EU, it has stoked fears as it would delay the application of key obligations for high-risk AI systems, while expanding the legal basis for processing sensitive data by framing bias mitigation as a public interest objective, embracing a more permissive opt-out approach (Rangone, 2026).

What's next? The Future of EU AI Governance

As geopolitical tensions increase and historical alliances falter, European leaders have come to realise that the future of AI must be "made in Europe" - a pursuit grounded in the idea that control over critical technologies underpins strategic security and autonomy. (Hechema, 2026). The AI Act tried to enshrine this objective by merging ethics, safety, and innovation principles. (Baltioğlu, Celik, Altindağ, 2025). Yet, many argue that it has struggled to deliver. On one hand, broad exemptions and national security derogations allow law enforcement authorities significant leeway to deploy controversial AI practices, including predictive policing and biometric recognition (Rodelli, C.; Chander, S., 2025). On the other hand, by prioritizing regulation over market–driven growth, the EU risks widening the economic gap with the US and China, as companies from outside the EU may decide to retain their technologies in the union due to excessive regulation hampering the competitiveness of European business (The Choice, 2024).

If the Union wishes to dominate the future of this technology, these shortcomings must be addressed. The Act should therefore be complemented by initiatives such as the Apply AI and investments in AI Factories under the EuroHPC - reflecting a growing emphasis on technological sovereignty and reducing dependence on external actors; as well as growing investments in open-source models, computational and cloud capacities. (Mariniello, 2026) Only through an integrated approach can the AI Act fulfil its original ambition of safeguarding fundamental rights while fostering innovation and sustainable competitiveness.

References

BALCIOĞLU, Y. S., ÇELİK, A. A., & ALTINDAĞ, E. (2025). A Turning Point in AI: Europe's Human-Centric Approach to Technology Regulation. *Journal of Responsible Technology*, *23*, 100128. https://doi.org/10.1016/j.jrt.2025.100128

Artificial Intelligence Act, Regulation (EU) 2024/1689, OJ L 1689 (2024). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689

Biscaia Gonçalves, L. (2026, March 8). *Ethics and Regulation of Military AI: Europe's Strategic Dilemma*. Eurodefense.pt. https://eurodefense.pt/ethics-and-regulation-of-military-ai-europes-strategic-dilemma/

BRIEFING EU Legislation in Progress Digital Omnibus on AI CONTEXT. (2026). https://www.europarl.europa.eu/RegData/etudes/BRIE/2026/782651/EPRS_BRI(2026)782651_EN.pdf

Cabanas, L. B., & Heinz, E. (2026, January 27). *AI power play: Can Europe catch up with the US and China?* Euronews; euronews.com. https://www.euronews.com/my-europe/2026/01/27/the-ai-race-can-europe-catch-up-to-the-us-and-china

Csernatoni, R. (2024, July 17). *Governing Military AI Amid a Geopolitical Minefield*. Carnegieendowment.org; Carnegie Endowment for International Peace. https://carnegieendowment.org/research/2024/07/governing-military-ai-amid-a-geopolitical-minefield?lang=en

Csernatoni, R. (2025, May 20). *The EU's AI Power Play: Between Deregulation and Innovation*. Carnegie Endowment for International Peace. https://carnegieendowment.org/research/2025/05/the-eus-ai-power-play-between-deregulation-and-innovation

GDPR. (2016). *Art. 22 GDPR – Automated individual decision-making, including profiling | General Data Protection Regulation (GDPR)*. General Data Protection Regulation (GDPR). https://gdpr-info.eu/art-22-gdpr/

Hechema, K. (2026, February 10). *AI for Strategic Autonomy: Europe's Bid for AI Independence*. EuropeanRelations.com. http://europeanrelations.com/ai-for-strategic-autonomy-europes-bid-for-ai-independence/

Italiano, A. (2024b, February). *Cos'è l'Artificial Intelligence Act e cosa prevede per l'AI*. Osservatori Digital Innovation Del Politecnico Di Milano. https://www.osservatori.net/blog/artificial-intelligence/artificial-intelligence-act-cosa-prevede-ai/

Mariniello, M. (2026, February 19). *Europe's artificial intelligence strategy should be built on European strengths*. Bruegel | the Brussels-Based Economic Think Tank. https://www.bruegel.org/first-glance/europes-artificial-intelligence-strategy-should-be-built-european-strengths

Rangone, N. (2026, March 10). *The Paradoxes of the European Union's AI Regulation | The Regulatory Review*. The Regulatory Review. https://www.theregreview.org/2026/03/10/rangone-the-paradoxes-of-the-european-unions-ai-regulation/

Rodelli, C., & Chander, S. (2025, August 7). *One Year On, EU AI Act Collides with New Political Reality*. Tech Policy Press. https://www.techpolicy.press/one-year-on-eu-ai-act-collides-with-new-political-reality /

The Draghi report on EU competitiveness. (2024). European Commission. https://commission.europa.eu/topics/competitiveness/draghi-report_en

Scarpellino, C. (2024). *EU and US regulatory approach to AI: a comparative perspective*. https://sog.luiss.it/sites/sog.luiss.it/files/E.U.%20and%20U.S.%20regulatory%20approach%20on%20AI%20comparative%20perspectives_REV_v3_0.pdf

The Choice by ESCP Business School. (2024, July 4). *How Europe's AI Act could affect innovation and competitiveness - The Choice by ESCP*. The Choice by ESCP. https://escp.eu/thechoice/tomorrow-choices/how-europes-ai-act-could-affect-innovation-and-competitiveness/

Torregrosa Basco, C. (2026). Emerging Technologies and the Laws of War: AI Warfare under IHL and the EU Regulation Gap J A N U A R Y 2 0 2 6 F I N A B E L. In *Finabel*. https://finabel.org/wp-content/uploads/2026/01/RR-Clara-3.pdf

Vogiatzoglou, P. (2024). *The AI Act National Security Exception*. VB Security and Crime: A Cooperation Project of Verfassungsblog and MPI-CSL. https://doi.org/10.59704/292082becc7cc8e6

Yoo, Y. (2025, January 14). *AI is Eating the World: Why Ubiquitous Intelligence is Inevitable and How It Will Happen | xLab | Case Western Reserve University*. XLab | Case Western Reserve University. https://case.edu/weatherhead/xlab/about/news/ai-eating-world-why-ubiquitous-intelligence-inevitable-and-how-it-will-happen