unione europea
e diritti

AI Act, Competition and Fairness. Compliance Issues, Overlaps in EU Legislations and Global Regulatory Scenario*

Andrea Stazi**

SUMMARY: 1. AI Act and Compliance Issues. - 2. Implications for Competition Law and Competitive Dynamics. - 3. Fairness in AI Regulation. - 4. Global Regulatory Dynamics. - 5. Conclusion.

1. *AI Act and Compliance Issues*

Today, we are at a crucial moment for the regulation of artificial intelligence, particularly in the European Union, where the AI Act is on the verge of coming into force, despite many doubts and questions, especially concerning the recent spread of generative artificial intelligence.

If it manages to come into force, the path to compliance with the AI Act appears "arduous", given that it promotes *ex-ante* regulation requiring companies to follow a multi-stage process.

This includes: i) identifying their role: provider, user, etc., ii) classifying their AI system based on the risk level, up to high-risk, which is the most regulated, iii) conducting a conformity assessment if the system is high-risk, iv) registering stand-alone high-risk AI systems in an

* It is published as received. Speech at the VIII Biennial Conference of the Italian Antitrust Association, Florence, 13 June 2025.

** Full Professor of Comparative Law, San Raffaele University of Rome - Visiting Professor in IP Law, National University of Singapore.

EU database, and finally v) signing a declaration of conformity and applying the CE marking before placing the system on the market.

Risk assessment is the most significant legal barrier. The term "risk" appears "blurred," and the regulation is criticized for confusing the sensitive application sector with the nature of the AI system used.

Although AI in sectors like biometrics or education is classified as high-risk based on the sector, it is argued that risk should also consider the autonomy or predictability of an AI system. A seemingly low-risk conversational agent, if autonomous and manipulative, could pose high risks.

This sector-based classification, applied uniformly, proves problematic and potentially harmful to competition, especially for small and medium-sized enterprises in sensitive markets that may not have the financial capacity for compliance.

Adding to this uncertainty is the broad definition of "artificial intelligence systems", which could inadvertently include technologies not typically considered AI, complicating risk assessment and potentially fragmenting the internal market.

Furthermore, the list of high-risk use cases can be amended by the Commission through delegated acts based on broad criteria such as the risk of harm to health, safety, or fundamental rights. While this provision is intended to adapt to rapid technological development, it has been noted that this power to modify the list based on broad criteria creates legal uncertainty and could discourage innovation and new market entrants.

The complexity is compounded by the requirement for companies to assess the risk of harm not only in terms of health and safety but also the impact on fundamental rights.

This implies predicting impacts based on complex, fragmented, and evolving jurisprudence, a task argued to be particularly challenging and potentially unreasonable for companies, especially new entrants without legal expertise.

Compliance with other rules has also been criticized as utopian; data governance obligations, for example, are considered unrealistic in their requirement for complete and error-free datasets. The obligation to maintain extensive technical documentation is deemed cumbersome and

a potential distortion favoring larger companies that can afford the necessary technical and legal expertise.

Finally, a significant issue is clearly the interconnection or overlap with other EU legislation. AI systems or products may be subject to the AI Act along with the GDPR, the Data Act, the Data Governance Act, the Digital Markets Act, the Digital Services Act, the Cloud and AI Development Act, the new version of the Cybersecurity Act soon to be adopted, and sectoral product regulations such as those for medical devices or machinery.

This can lead to significant and complex compliance burdens, duplication of conformity assessments, and legal uncertainty, particularly regarding liability for damages, where the interaction with the proposed AI Liability Directive is unclear.

This fragmentation of sources and overlapping requirements significantly increase compliance costs, acting as a strong economic barrier, especially for financially vulnerable startups and SMEs, and potentially delaying or preventing market entry. The multitude of objectives of the AI Act, moreover, also makes proportionality assessment difficult and can lead to conflicts between fundamental rights and economic freedoms.

2. *Implications for Competition Law and Competitive Dynamics*

Let's now consider the more direct implications of the AI Act for competition law and competitive dynamics. Although the AI Act states that it applies «without prejudice to the provisions of Union competition law», the Act affects competition law in three key ways: procedural powers, computational antitrust, and analysis of anticompetitive practices.

Firstly, regarding *procedural powers*, the AI Act indirectly extends the investigative powers of competition authorities. It requires national market surveillance authorities, responsible for enforcing the AI Act, to annually report to national competition authorities and the Commission information identified during their activities that «may be of potential interest» for the application of EU competition law.

This grants competition authorities indirect access to sensitive information and data, such as documentation, datasets, and even source

code for high-risk AI systems, without the need to first suspect an antitrust violation.

Secondly, regarding *computational antitrust*, i.e., the use of legal informatics to facilitate antitrust analysis, it appears likely that the AI Act will slow its development. The Act classifies AI systems used by law enforcement or judicial authorities for fundamental tasks such as evidence assessment, criminal offense investigation, or assistance with judicial analysis as "high-risk."

This applies to AI used by competition authorities to detect practices, such as "hard-core" cartels or bid rigging, which are considered criminal offenses in some Member States. Compliance with the requirements for high-risk systems in these cases can lead to technical and organizational problems and discourage the use of AI to detect such harmful practices.

Thirdly, the AI Act has significant implications for the *analysis of anticompetitive practices* that its provisions may facilitate. Various provisions, intended to increase transparency for safety reasons, require the sharing of information that could inadvertently expose commercially sensitive information.

For example, Article 19 requires providers of high-risk AI systems to keep detailed logs, which contain sensitive information about business practices, user behavior, and decisions. Similarly, Articles 16, 23, 24, and 25 on the obligations of providers, importers, and distributors require the sharing of technical documentation, training data, and logs for compliance and market access.

This level of transparency among market participants creates a non-negligible risk of fostering collusive behavior or targeted abuses of dominant positions, potentially leading to cases similar to the one against Amazon for using marketplace sellers' data. In the AI Act, Union institutions have prioritized safety, and competition authorities will have to assess whether this safety objective outweighs the competition concerns raised by such information sharing.

In addition to the direct implications for competition law, the AI Act is expected to impact *competitive dynamics*. While it helps prevent market fragmentation by Member States acting unilaterally, it could still distort the internal market and reduce access.

Distortions arise because the Act's technology-neutral approach regulates deterministic-and thus predictable-and non-deterministic-and

thus unpredictable-AI systems similarly, imposing stringent provisions even on safer systems.

Moreover, the compliance burden is unevenly distributed, potentially favoring large companies over smaller ones, leading to criticisms similar to those regarding the GDPR's impact on SMEs. The limited exemption for SMEs regarding technical documentation and the potential adoption of regulatory sandboxes are considered insufficient to prevent these distortions.

Market access is hampered by vague language in several articles, leading to legal uncertainty and potential litigation. Examples include the definition of prohibited manipulative systems, "real-time," data quality, and human oversight. High fines for non-compliance amplify this uncertainty.

The regulation of general-purpose AI models introduces a new pillar with a capabilities-based approach, but their definition and requirements also suffer from vagueness, high compliance costs for documentation and sharing, and uncertain criteria for systemic risk, raising further concerns about market distortion and access, especially for SMEs.

3. *Fairness in AI Regulation*

This discussion on market dynamics and potential anticompetitive behavior brings us to the concept of *fairness* in artificial intelligence regulation.

Recent EU legislative acts like the DMA, Data Act, and AI Act all significantly elevate the concept of "fairness" or address "unfair practices". However, the definitions of "fairness" or "unfairness" are often not precisely defined for practical application and legal certainty.

The DMA, for instance, links unfairness to an imbalance of rights where a gatekeeper gains a disproportionate advantage. The AI Act defines fairness primarily in terms of «diversity, non-discrimination and fairness», focusing on avoiding discriminatory impacts and unfair biases.

As is known, the concept of fairness in competition law has historically been controversial and often seen as conflicting with economic efficiency. However, research in behavioral and experimental economics seems to demonstrate that humans have a social preference for fair outcomes and an aversion to injustice.

People are wary of unfair prices, based on factors such as past or competitive prices. AI, if left unchecked, can engage in pure profit maximization.

While the AI Act's focus on fairness in the sense of absence of bias differs from that of competition law like unfair pricing, the fact that the Act, like the DMA and Data Act, elevates fairness and often refers to Union competition law suggests that interpreting their fairness dimensions through the lens of established competition law rules on concepts like "unfair price", with the related relationship to cost and assessment of profit margin fairness (see CJEU's *United Brands* decision), could provide a clearer and more objective framework for application.

This is relevant because, as is well known, traditional economic theories struggle to fully grasp the complexities and power dynamics of data-driven and AI markets, while fairness, if clearly defined, can be seen as a subsidiary but eventually objective concept for assessing the management of economic activity.

4. *Global Regulatory Dynamics*

Finally, expanding the horizon to the global scenario, we see that AI regulation is part of a dynamic "regulatory game" in which governments and companies behave strategically to protect their interests.

The basic dynamic involves: i) a national or supranational government decides to regulate a technology in its territory; ii) companies then choose to comply, withdraw, or evade (regulatory arbitrage, moving activities to a less regulated jurisdiction); iii) the government reacts by tolerating evasion or expanding its regulatory reach, possibly even extra-territorially.

Based on countries' political preferences and the importance of economies of scale for technologies, this global game can lead to different outcomes: more local regimes, international harmonization, unilateral imposition (e.g., the "Brussels effect"), or fragmentation ("Splinternet").

Fragmentation imposes costs on companies, forcing product adaptation and loss of economies of scale or network effects, potentially even leading to market withdrawal.

Regarding AI regulation, neither a full Brussels effect nor extensive international harmonization, as is evident from President Trump's

intervention shortly after his inauguration to revoke his predecessor's AI rules, are currently probable.

In today's geopolitical scenario, leadership in artificial intelligence is increasingly seen as vital, pushing governments towards strategic autonomy and using regulation as a lever to shape AI governance in their favor, leading to fragmentation.

However, fragmentation is costly for AI models that rely on significant scale. This could push industry and even governments towards a certain level of limited harmonization, to allow for economies of scale and increase isolation costs for competitors.

On the other hand, there is also a risk that companies successfully play governments against each other in a "race to the bottom" on regulation.

5. *Conclusion*

In conclusion, while the AI Act is a significant step in AI regulation, it presents substantial compliance challenges, particularly for smaller entities, due to its complex, sometimes vague, and overlapping requirements.

The Act fundamentally impacts the enforcement of competition law and reshapes competitive dynamics by extending investigative powers and creating transparency obligations that could facilitate anticompetitive behavior.

Similar to other EU digital regulations such as the DMA and Data Act, the AI Act highlights the concept of fairness, presenting an opportunity to draw on established principles of competition law.

Globally, AI regulation involves managing complex trade-offs between preventing regulatory arbitrage and managing the costs of fragmentation.

Given the strategic importance of AI, a future characterized by fragmentation, perhaps with limited cooperation within certain blocks, appears more likely than widespread international harmonization, reflecting the dynamic ongoing game between national interests and corporate strategies.

ABSTRACT (ita)

L'AI Act è un nuovo regolamento sul digitale dell'Unione europea con un'ampia portata, che si applica a diversi soggetti con sede nell'Unione o che hanno un impatto su di essa. Esso estende indirettamente i poteri investigativi delle autorità di concorrenza, consentendo l'accesso a documentazione, *dataset* e persino al codice sorgente per l'IA ad alto rischio. Le disposizioni che promuovono la trasparenza potrebbero inavvertitamente facilitare la collusione o l'abuso mirato di posizione dominante esponendo dati aziendali sensibili. In tal senso, l'AI Act creerebbe barriere all'ingresso nel mercato e distorcerebbe il mercato unico, gravando in modo sproporzionato sulle PMI a causa degli elevati costi di compliance. Il linguaggio vago o ambiguo in disposizioni chiave potrebbe dare luogo a una significativa incertezza giuridica e a potenziali contenziosi, esacerbati da elevate multe per la non conformità. La classificazione del rischio per settore è problematica e il potere della Commissione di modificare l'elenco ad alto rischio potrebbe creare ulteriore incertezza. Esiste una sovrapposizione e un potenziale conflitto con altre legislazioni dell'UE - DMA, DSA, GDPR, Data Act, Data Governance Act, Cloud and AI Development Act e nuova versione del Cybersecurity Act, norme settoriali - che causa la duplicazione degli oneri di *compliance*. L'incertezza riguardo al regime di responsabilità civile per i danni causati dall'IA può ostacolare il *private enforcement* del diritto della concorrenza. Il concetto di *fairness* è rilevante, in particolare in relazione a "diversità, non discriminazione e correttezza" nello sviluppo dell'IA, e appare distinto dalla correttezza tradizionale del diritto della concorrenza (ad esempio, prezzi sleali). A livello globale, la regolamentazione dell'intelligenza artificiale implica la gestione dei complessi compromessi tra la prevenzione dell'arbitraggio normativo e la gestione dei costi della frammentazione. Data l'importanza strategica dell'IA, un futuro caratterizzato dalla frammentazione, forse con una cooperazione limitata all'interno di alcuni blocchi, appare più probabile di una vasta armonizzazione internazionale, riflettendo il dinamico gioco in corso tra interessi nazionali e strategie aziendali.

ABSTRACT (eng)

The AI Act is a new EU digital regulation with a broad scope, applying to various entities based in or impacting the Union. It indirectly expands the investigative powers of competition authorities, granting access to documentation, datasets, and even source code for high-risk AI. Provisions promoting transparency could inadvertently facilitate collusion or targeted abuse of dominant positions by exposing sensitive business data. In this sense,

the Act would create market entry barriers and distort the single market, disproportionately burdening SMEs due to high compliance costs. Vague or ambiguous language in key provisions could lead to significant legal uncertainty and potential litigation, exacerbated by high fines for non-compliance. The risk classification by sector is problematic, and the Commission's power to amend the high-risk list could create further uncertainty. There is overlap and potential conflict with other EU legislation - DMA, DSA, GDPR, Data Act, Data Governance Act, forthcoming Cloud and AI Development Act and new Cybersecurity Act, sector-specific rules - causing duplicated compliance burdens. Uncertainty regarding the civil liability regime for AI-caused harm may hinder the private enforcement of competition law. The concept of fairness is significant, particularly in relation to 'diversity, non-discrimination, and fairness' in AI development, and appears distinct from traditional competition law fairness (e.g., unfair pricing). Globally, AI regulation involves managing complex trade-offs between preventing regulatory arbitrage and managing the costs of fragmentation. Given the strategic importance of AI, a fragmented future, perhaps with limited cooperation within some blocs, seems more likely than broad international harmonization, reflecting the ongoing dynamic interplay between national interests and corporate strategies.