Proceedings of ICGPSH 2026 Symposium: EdTech & AI in Learning: Large Language Models in Business, Politics, and Humanities
DOI: 10.54254/2753-7048/2026.LD33075

From the EU to China: Regulatory Pathways, Diffusion Effects, and Localized Responses to the World's First Comprehensive AI Legislation

Tianyi Xie

School of Humanities, Hebei University, Baoding, China
13505680865@163.com

Abstract. This paper systematically analyzes the background, core provisions, and global implications of the EU's Artificial Intelligence Act. As the world's first comprehensive legislation regulating artificial intelligence (AI), the Act adopts a risk-based regulatory model that categorizes AI technologies into different risk tiers and applies differentiated governance measures. Its enactment reflects both the EU's traditional strategic advantage in digital rule-making and its response to competitive pressures from China and the United States in AI technology. Research indicates that while the Act promotes the safe and trustworthy development of AI, its stringent compliance requirements may stifle innovation, sparking controversy. For China, the EU legislation offers valuable insights in areas such as regulatory sandbox mechanisms, risk-based classification governance, and standardization efforts. Employing literature analysis and comparative research methods, this paper aims to provide reference points for refining China's AI legislation.

Keywords: EU Artificial Intelligence Act, AI regulation, risk-based classification governance, China-EU digital policy, AI legislative reference

1. Introduction

The rapid advancement of artificial intelligence technology has introduced unprecedented institutional challenges to the global governance system. In response, following years of negotiations, the European Union completed its legislative process in 2024 and formally enacted the Artificial Intelligence Act in August. This legislation is widely regarded as the world's first comprehensive regulatory framework for the AI sector. Its development stems from a complex backdrop, reflecting both the EU's ambition to establish leadership in digital rule-making and strategic considerations to counter the technological competition with China and the United States in AI. This study aims to analyze the AI Act's establishment context from a political-economic perspective, systematically examine its core provisions and potential benefits/drawbacks, and further explore its implications for China's AI legislation.

Drawing on EU official documents, academic commentary, and industry feedback, the research traces the legislative journey and core institutional frameworks of the Act. It primarily addresses three questions: What political-economic objectives does the EU pursue through the AI Act? How

DOI: 10.54254/2753-7048/2026.LD33075

does the Act balance institutional arrangements between fostering technological innovation and mitigating societal risks? What legislative insights can China draw from the EU experience? The significance of this study lies in providing international reference points for China's ongoing AI legislation efforts, aiding in the pursuit of equilibrium between innovation promotion and regulatory governance.

2. Analyzing the background of the EU AI Act

2.1. Historical origins: an extension of the EU Digital Single Market strategy

The introduction of the EU AI Act represents a natural extension and deepening of the EU's Digital Single Market strategy within the AI regulatory domain. Its legislative rationale explicitly states that if member states independently develop AI regulations, it would inevitably lead to fragmentation of the internal market's legal framework and significantly reduce legal certainty for AI system providers and users. Given the "cross-border flow of products and services," only unified EU-level legislation can effectively address these issues. Member states acting alone cannot achieve the proposal's objectives, and divergent regulations would impede the seamless circulation of AI-related products and services across the EU [1]. Against this backdrop, the Act establishes "safeguarding the proper functioning of the internal market" as a core objective. It seeks to develop a single market for lawful, safe, and reliable AI applications through a unified regulatory framework, thereby preventing market fragmentation. This reflects the EU's strategic logic of applying its approach to establishing unified rules and eliminating barriers within the Digital Single Market to the emerging critical field of artificial intelligence. The aim is to consolidate the internal market through a unified regulatory framework and lay the groundwork for exporting its rules externally (the "Brussels Effect") [2].

2.2. Political drivers: shaping digital sovereignty and global rule leadership

The EU does not lead in the field of large AI models. Therefore, a key intent of its legislation is to achieve the "Brussels effect," which involves aligning other countries' regulations with the EU's to reduce AI developers' ability to evade or shift regulatory compliance costs. Simultaneously, "Brussels' 'trust seal' could make AI models more attractive and competitive." This explicitly reflects the EU's attempt to export its rules, transforming internal regulatory standards into de facto global norms to gain governance dominance. The EU's approach "leans toward comprehensive control over AI technologies, seeking to protect domestic markets through stringent regulation while seizing rule-making authority by 'internationalizing' regulatory standards." This indicates the bill transcends mere technological regulation, functioning as a geopolitical and economic strategy to construct a "digital fortress" [1] grounded in EU values like fundamental rights protection.

2.3. Economic considerations: institutional balance between risk prevention and innovation incentives

The bill encourages national authorities to establish regulatory sandboxes—controlled environments where innovative technologies can be tested for limited periods under agreed-upon testing plans with regulators—providing experimental grounds for innovation. The legislation adopts a risk-based approach, imposing regulation only when AI systems pose high risks to fundamental rights and security. For non-high-risk systems, it imposes "limited transparency obligations." This design aims to "minimize costs" and avoid overregulation [1]. In practice, most AI applications are likely to be deemed low-risk and exempt from regulation [2]. The bill clarifies the state's supporting role,

DOI: 10.54254/2753-7048/2026.LD33075

shaping market frameworks rather than dictating plans. Unlike China, EU nations never act as macroeconomic planners at the national level. Their role is to "clear regulatory and administrative hurdles for private actors," "provide a level playing field," and guide private capital as the primary driver of innovation through "economic incentives and guarantees (e.g., de-risking tools)" [3]. In summary, the bill's economic rationale reflects a trade-off between "preventive regulation" and "market-driven innovation." Its fundamental logic is to guard against potentially catastrophic socioeconomic losses in the future through "strict controls in high-risk areas," while simultaneously striving to create a stable, predictable, and relatively lenient regulatory environment for broad AI economic activities through tools like "sandbox testing, risk classification, and state support." The ultimate goal is to safeguard safety and ethical boundaries while preventing overregulation from stifling market vitality and innovation potential, thereby securing sustainable development space for EU industries in global AI competition. However, achieving this balance heavily depends on the clarity and flexibility of rule implementation. Otherwise, high compliance costs could directly translate into competitive disadvantages.

3. Core provisions and analysis of the EU Artificial Intelligence Act

3.1. Core regulatory framework: a four-tier risk-based regulatory model

The core provision of the EU Artificial Intelligence Act is its risk-based, four-tier regulatory classification system. It categorizes AI systems into four levels: unacceptable risk, high risk, limited risk, and minimal risk, imposing differentiated legal obligations accordingly. This tiered approach forms the institutional bedrock of the Act's overall structure and represents the EU's first systematic attempt to integrate "risk prevention" with "targeted regulation" in global AI governance. By clearly defining applicable scenarios, regulatory measures, and exemption rules for each risk level, the system safeguards safety and fundamental rights while preserving flexibility for technological innovation. The unacceptable risk category represents an absolute prohibition "red line zone," targeting AI applications posing fundamental, irreversible threats to EU core values, citizens' fundamental rights, and public safety. Its determination hinges on the core criterion of "significant potential harm," embodying the precautionary principle. Regulatory measures include a general prohibition on placing on the market, putting into service, or using such systems (unless explicitly exempted). Typical scenarios include social scoring systems, untargeted facial image harvesting, and real-time remote biometric recognition in public spaces for non-law enforcement purposes. The underlying logic of this tier is to adopt a "bottom-line mindset" to block the source of technological abuse, preventing AI from structurally eroding core values such as equality and human dignity.

High-risk AI applications are designated as strictly regulated "control zones," focusing on those posing significant threats to citizens' health, safety, and fundamental rights—yet where risks can be mitigated through compliance reviews. These applications are characterized by scenario-specificity and manageable risk levels. The legislation imposes "full lifecycle compliance" obligations on such AI systems, requiring pre-deployment assessments, real-time transparency, and post-use monitoring mechanisms. Systems failing compliance checks are prohibited from deployment. Applicable domains include healthcare (e.g., AI-assisted cancer diagnosis systems must provide patient informed consent documentation, maintain human oversight channels, and submit periodic misdiagnosis rate reports), education and vocational training (e.g., AI vocational skills assessment systems must disclose dimension weightings and permit human review), and employment/human resources (e.g., AI recruitment systems must detect algorithmic bias, notify applicants, and provide traceable selection rationale). This tier embodies a balance between "safety controls" and

DOI: 10.54254/2753-7048/2026.LD33075

"technological usability," mitigating risks through institutionalized compliance requirements while preserving AI's application value in critical domains.

Overall, the EU's four-tier risk classification organically integrates the "precautionary principle, bottom-line thinking, and innovation protection" to form a closed-loop governance system: implementing the precautionary principle through absolute prohibition of unacceptable risks, safeguarding critical areas through high-risk lifecycle management, and preserving flexibility for over 90% of AI applications via relaxed regulation for limited and minimal risks. This logic addresses the uncertainty of AI technological risks while balancing the dual objectives of safety and development, offering a tiered, categorized, and precise model for global AI governance.

Second, it introduces special regulations for General Purpose Artificial Intelligence (GPAI) by introducing the concept of "systemic risk," using computational capacity (floating-point operations per second, FLOPs) as the threshold for determination [4]. Providers of GPAI models reaching this threshold (regardless of whether they are open-source) must undertake additional obligations such as model evaluation and adversarial testing [2]. This marks a shift in regulatory focus from specific applications to the foundational models themselves. Concurrently, a responsibility framework centered on "providers (suppliers)" is established: the vast majority of obligations for high-risk AI fall on providers (developers), requiring them to establish quality management systems, ensure data quality, maintain technical documentation, and implement human oversight [5]. The bill seeks to provide a safe testing environment for innovation through a "regulatory sandbox."

The EU AI Act's four-tier risk classification system, special regulations for General Purpose Artificial Intelligence (GPAI), and provider-centric liability framework do not operate in isolation. Instead, they form a synergistic institutional structure centered on risk control, innovation safeguards, and accountability. The four-tier risk classification establishes uniform risk assessment criteria for overall regulation, clarifies regulatory boundaries for different AI system types, and provides a foundational basis for subsequent specialized oversight and liability allocation. Within this framework, the Act introduces a threshold-based regulatory mechanism for GPAI systems posing systemic risks, extending oversight from specific applications to foundational models and addressing limitations of purely application-based classification. The provider-centric liability system provides clear accountability for these regulatory requirements. By centrally assigning compliance obligations and supplementing them with regulatory sandboxes, it ensures the enforceability of risk-tiered regulation and GPAI-specific oversight. Together, these three elements form a governance system where regulatory intensity is determined by risk levels, regulatory dimensions are supplemented by technological characteristics, and regulatory implementation is secured through designated responsible entities. This framework preserves necessary space for technological innovation while effectively mitigating risks.

3.2. The positive significance and potential challenges of the bill

The most prominent strengths and positive aspects of the EU AI Act lie in its pioneering and systematic nature. The bill is widely recognized as the world's first comprehensive, binding regulation targeting trustworthy artificial intelligence and the first global legislation specifically addressing AI risks, providing the first integrated paradigm for global AI governance. Simultaneously, its risk-based approach concentrates regulatory resources on high-risk domains, avoiding a "one-size-fits-all" approach to minimize costs and prevent overregulation. However, the bill's drawbacks cannot be overlooked: (1) High compliance costs may stifle innovation and competition. The legislation fails to provide legal certainty for AI developers and deployers, potentially generating substantial compliance expenses—particularly for SMEs and startups. This

DOI: 10.54254/2753-7048/2026.LD33075

could not only stifle innovation but also weaken Europe's industrial competitiveness in the global AI race. (2) Ambiguity and potential loopholes in the rules. For instance, the systemic risk threshold (10^25 FLOPs) has been criticized as "arbitrary" and may soon be surpassed by next-generation models. Legal uncertainties surround the definitions of prohibited behaviors like "manipulation" and "social scoring," potentially hindering effective enforcement [5]. (3) Enforcement challenges and regulatory resource constraints: The bill primarily relies on provider self-assessment and de facto standards established by private organizations (e.g., CEN, CENELEC), raising legitimate concerns about "substantially transferring public rule-making authority to private entities." Additionally, Market Surveillance Authorities (MSAs) may face resource shortages, while individuals and groups affected by AI lack direct complaint and judicial remedy rights, potentially leading to weak enforcement. "Maximum Coordination" May Restrict Member States' Rational Regulation: The Act's broad scope may pose multiple challenges to enforcement mechanisms, potentially restricting member states' legitimate attempts to manage the societal impacts of AI systems under the guise of free trade [5].

3.3. Case study

The bill prohibits the use of "real-time" remote biometrics (e.g., facial recognition) in public spaces but lists three exceptions, such as "preventing a specific, substantial, and imminent threat to the life or physical safety of a natural person" [1]. This reflects the rule's attempt to balance security and rights, yet sparks debate over potential abuse of exceptions. Second, regulatory practices for high-risk systems. For instance, an AI system used in recruitment is classified as high-risk, requiring its provider to register in a database, submit detailed technical documentation, establish a risk management system, and ensure human oversight [5]. This demonstrates the concrete burden of compliance. Third, limitations of transparency requirements. The bill requires users of emotion recognition systems to inform scanned individuals. Critics note this often merely duplicates existing GDPR obligations, and "attributing the primary problem with emotion or biometric profiling to a lack of transparency risks legitimizing a practice with scant scientific basis..." [5].

These three examples, originating from different risk tiers, concretely illustrate how the AI Act's risk-tiered governance logic operates in practice. Real-time remote biometric identification in public spaces faces strict restrictions due to its significant infringement on fundamental rights, while exceptions are established to address urgent public safety needs—reflecting an institutional balance between rights protection and security safeguards. AI recruitment systems are classified as high-risk with multiple compliance obligations, demonstrating the bill's stance of stringent regulation in critical domains. Conversely, emotion recognition systems bear only transparency obligations, revealing a light-touch intervention approach for limited-risk scenarios. These examples transform risk classification from an abstract framework into tangible regulatory practice [6]. However, while these institutional arrangements demonstrate differentiated regulatory advantages, they also expose potential issues: the real-time biometric exception clause raises concerns about ambiguous application boundaries and potential abuse; compliance requirements for high-risk systems increase corporate costs and technical burdens; and transparency obligations for emotion recognition systems overlap with GDPR provisions and fail to adequately address scientific validity disputes. Thus, while risk-based classification frameworks theoretically enable precise allocation of regulatory resources, they still face challenges in rule clarity and institutional coordination at the implementation level.

DOI: 10.54254/2753-7048/2026.LD33075

4. Implications and references for China's AI legislation

4.1. Current status of China's AI legislation

China has yet to enact a unified national AI law but has preliminarily established a governance framework combining "decentralized legislation with sector-specific regulation" [7]. The top-level legislative layout is clear: The State Council has included the "Draft Artificial Intelligence Law" in its preliminary review agenda, and the national level has repeatedly emphasized strengthening AI legislative research. Specific regulatory provisions targeting particular scenarios have been issued, such as the Interim Measures for the Administration of Generative AI Services and the Administrative Measures for the Safe Application of Facial Recognition Technology, reflecting a "small-scale, agile, and responsive" legislative approach. While the governance system has taken shape—covering data, algorithms, content, ethics, and other domains—it lacks systematic coordination, posing risks of fragmented regulation.

4.2. Lessons to learn: institutional design and regulatory tools

First is risk-based classification and tiered governance. The EU regulation categorizes AI risks into four levels—"unacceptable, high, limited, low"—enabling differentiated oversight. This model facilitates targeted interventions, avoiding a "one-size-fits-all" approach.

Second, lifecycle-based regulation warrants attention. The legislation mandates oversight across all stages—design, development, deployment, and use—while establishing obligations for providers, deployers, and other stakeholders. This systemic approach addresses dynamic risks arising from technological evolution. Strict legal liability and substantial fines are equally instructive. The EU imposes penalties of up to 7% of global turnover, enhancing deterrence and incentivizing proactive compliance.

Simultaneously, safeguarding rights and transparency must not be overlooked. The legislation prioritizes human rights protection, mandating high-risk systems to fulfill obligations regarding transparency and explainability.

4.3. Local adaptation: pathways aligned with China's national context

China still lags behind the United States in AI technology, industry, and talent. Legislation should prioritize supporting innovation while avoiding excessive regulation that stifles vitality [8]. "As a 'leading follower,' China's legislative approach should prioritize 'promoting development' to align with its developmental needs." A "unified legislation + sector-specific legislation" model can be adopted: enacting a foundational, comprehensive Artificial Intelligence Law to establish development principles, regulatory frameworks, and international cooperation mechanisms, while preserving flexibility for sector-specific legislation [9]. Simultaneously, establish a lightweight, agile regulatory system. First, embrace risk tolerance: accept reasonable risks inherent in technological innovation, avoiding a "zero-risk" mindset. Second, implement tiered classification: establish principles in the AI Law, with specific standards refined through sector-specific legislation or industry standards. Additionally, encourage self-regulation: design due diligence exemption clauses to guide enterprises in establishing autonomous mechanisms. A national-level coordination mechanism should be established, creating a cross-departmental AI governance body to integrate policy and regulation, preventing fragmentation. International legal elements should also be incorporated: China's AI legislation should possess extraterritorial applicability to counteract the

DOI: 10.54254/2753-7048/2026.LD33075

"long arm jurisdiction" of the US and Europe, while promoting the incorporation of Chinese proposals like the Global AI Governance Initiative into the law [10].

5. Conclusion

The enactment of the EU Artificial Intelligence Act marks a new phase in global AI governance characterized by rule-making. This study demonstrates that the Act constitutes a vital component of the EU's digital strategy, aiming to enhance its global influence through regulatory export while addressing pressures from Sino-American technological competition. The Act's innovative "risk-tiered regulation" model provides a systematic framework for AI governance, categorizing AI technologies into four risk levels (unacceptable, high, limited, minimal) and implementing differentiated oversight. This classification method establishes stringent safety safeguards for high-risk AI applications while preserving innovation space for low-risk ones. However, the study also identifies significant challenges. On one hand, stringent compliance requirements—such as end-to-end risk management for high-risk systems and transparency obligations for generative AI—may substantially increase corporate burdens, raising concerns about stifling innovation. On the other hand, questions persist regarding enforcement capacity, as regulatory bodies lack the technical capabilities for substantive oversight. The bill's dedicated regulations for generative AI and general AI models demonstrate foresight, though their practical implementation remains to be seen.

For China, the EU experience offers multiple insights. China could draw on the bill's tiered classification approach to refine its existing Interim Measures for the Administration of Generative Artificial Intelligence Services. Simultaneously, the EU's "regulatory sandbox" mechanism—which provides testing space for innovation within a strict regulatory framework—is worthy of reference. Furthermore, China should accelerate the development of its national AI standards system and play a more significant role in international standard-setting. Future research could focus on the actual outcomes of the Act's implementation and variations in enforcement across member states. As AI technology advances rapidly, the formation of global AI governance rules will be a dynamic process. China should actively participate in this process, ensuring both technological security and controllability while promoting innovative applications, thereby contributing Chinese wisdom to global AI governance.

References

[1] Fang, X., Wei, Y., Zhang, Y., et al. (2022) Overview of the EU Artificial Intelligence Act. Computer Times, (05): 92-95. https: //doi.org/10.16644/j.cnki.cn33-1094/tp.2022.05.023.
[2] Li, Y., & He, G. (2024) The EU Artificial Intelligence Act: Key Provisions, Evaluation, and Implications. Science and Technology China, (05): 5-8.
[3] Xuan, L., & Xing, L. (2025) Regulating AI in a Fragmented World: The Diverging Paths of the EU and China and Their Impact on Global Governance. Innovation and Development Policy, 7(01): 27-47. https: //doi.org/10.20046/j.cnki.2096-5141. 2025.0002.
[4] Computer Law Review International. (2019) A Journal of Information Law and Technology. Computer Law Review International, 19(20): 3-3. https: //doi.org/10.9785/cri-2019-192002.
[5] Lessons and Implications for China's AI Regulation from the EU's Artificial Intelligence Act: A Perspective Based on Risk Classification and Multi-stakeholder Collaboration.
[6] Sun, L.Y. (2026) A Comprehensive Interpretation of the EU Artificial Intelligence Act. Journal of Hubei University of Economics (Humanities and Social Sciences Edition), 1-12. https: //link.cnki.net/urlid/42.1855.C.20251218.1739.004.
[7] Wang, Y. (2026) Regulatory Implications of Predictive Policing AI in the EU Artificial Intelligence Act. Journal of the Chinese People's Public Security University, 1-10.

DOI: 10.54254/2753-7048/2026.LD33075

[8] Sun, N., & Qu, Z. (2026) Research on China's AI Risk Classification and Tiered Regulatory System: Extraterritorial Comparisons and Domestic Construction. Science and Technology Progress and Policy, 43(01): 114-123.
[9] Zhi, Z.F. (2025) Key Concerns and Future Trends in Global Artificial Intelligence Legislation. Comparative Law Research, (06): 17-36.
[10] Zhan, Y, K. (2025) Implications of the EU Artificial Intelligence Act for China's AI Safety Regulation. China Market Regulation Research, (09): 71-76.