Innovation and Development Policy

Available online at http://idp-journal.casisd.cn/

Regulating AI in a Fragmented World: The Diverging Paths of the EU and China and Their Impact on Global Governance

Xuan Li[a, b, *], Xing Li[c]

[a] Institute of International and Regional Studies, Zhejiang University of Technology, Hangzhou 310023, China

[b] Global Institute for Zhejiang Merchants Development, Zhejiang University of Technology, Hangzhou 310023, China

[c] Guangdong Institute for International Strategies, Guangdong University of Foreign Studies, Guangzhou 510420, China

Abstract

This study examines the contrasting AI regulatory frameworks of the European Union (EU) and China, shaped by their distinct political cultures and strategic objectives. The EU adopts a rights-oriented, risk-based model, categorising AI systems based on their potential impact on civil liberties. Conversely, China employs a sector-specific, security-driven model that emphasizes national security, social stability, and economic growth. The findings highlight three key differences: (1) Regulatory Philosophy: The EU prioritises rights protection, while China focuses on security and technological competitiveness. (2) Focus and Approach: The EU uses a universal risk-based model, while China tailors regulations to specific sectors. (3) Key Characteristics: The EU mandates explainability and accountability, while China prioritizes data labelling and content control. In conclusion, the EU envisions AI as an extension of its human rights-first philosophy, constrained by legal and ethical frameworks. China, by contrast, views AI as a tool for industrial and geopolitical dominance, driving what may be termed "AI-facilitated re-industrialization." While global AI governance convergence is unlikely, pragmatic adaptation and mutual recognition of differing norms could facilitate cooperation.

Keywords

AI regulatory approaches; Global AI governance; EU; China

* Corresponding author. E-mail address: lixuanuk@126.com

10.20046/j.cnki.2096-5141.2025.0002

1. Introduction

Over the past years, key international organizations, like the G7, EU, OECD, United Nations, Global Partnership on Artificial Intelligence (GPAI) have shaped the global governance conversation but also fragment it. The Western-led AI coalition such as G7, EU, OECD and G7-led GPAI have achieved some distinctive regulatory milestones such as the first international network of AI Safety Institutes uniting the European Union and 10 countries at AI Safety Summit, the world's first legally binding international treaty on artificial intelligence led by the Council of Europe with 57 countries ratified. Of essence, these coalition outcomes are to put the use of AI in compliance with human rights, democracy and the rule of law. However, China, notably, does not appear on this Western-led AI coalitions and explicitly resort to the UN General Assembly in incorporating the countries of the Global South into the global deliberation forum. At the UN General Assembly a China-led resolution in 2024 July on enhancing international cooperation and capacity building for AI for enhancing international AI cooperation, with over 140 countries supporting it, underscores to "increase financing and technical assistance to developing countries in the field of capacity-building" and "support developing countries' effective, equitable and meaningful participation in international process" (Xinhua, 2024). While major powers—the EU, representative to Western-led coalition and as the normative power in AI governance and China, representative to the rise of Global South and as a merging power in AI governance—are rolling out their context-contingent regulations.

The literature on AI governance has increasingly grappled with its ethical, legal, and normative ambiguities. Orwat *et al*. (2024) highlight the fundamental vagueness embedded in AI norms, while Ruschemeier (2023) exposes the legal headaches posed by the EU's AI Act. At the same time, Laux (2024) raises the issue of human oversight—or the lack thereof—within this regulatory framework. The broader concern over AI and democratic legitimacy also looms large, with Coeckelbergh (2024) and Tambiama (2019) diagnosing a "democracy deficit" in AI governance. Meanwhile, Racine *et al*. (2024) push the concept of "living ethics," questioning whether AI ethics can ever be more than a corporate PR exercise, a concern echoed in Van Maanen's (2022) critique of "ethics washing." Beyond the EU's struggles, there's also the matter of AI as a geopolitical tool. Ekdal and Manners (2021) frame the EU's approach as one of "normative power," exporting its governance model as if AI ethics were just another piece of the Brussels effect. But AI doesn't just live in the realm of abstract norms—it transforms economies and societies in ways that are anything but neutral. Kim *et al*. (2025) examine its role in education, while Emery-Xu *et al*. (2024) analyze AI's military and security implications. In the economic domain, Sahebi and Formosa (2024) explore how AI is reshaping labor markets in low- to middle-income countries, with disruptive effects that cut across traditional development models. Then there's the big picture: AI as a political instrument in global governance. Xue (2024) lays out five core challenges to regulating AI at the international level, while Yan and Zhang (2024) provide a comparative analysis of how the EU and the US structure their AI governance regimes—differing not just in policy provisions but in how much influence private corporations wield over the process.

Taken together, these studies reflect a growing recognition of AI's ethical, political, and social ramifications, but they still miss something crucial: the deep-seated political and ideological fractures that make any global AI governance framework inherently fragile. The elephant in the room isn't just regulatory divergence—it's the fact that major powers approach AI from fundamentally different value systems. Without a case-by-case analysis of these cross-cultural and political fault lines, attempts to govern AI globally are likely to remain an exercise in wishful thinking

Nowhere is this divergence clearer than in the AI governance models of China and the EU. The article raises the question: how profoundly these two models differ and what this means for global collaboration? Our findings show that these two actors don't just regulate AI differently—they operate from fundamentally distinct political cultures and economies that shape how they see the role of AI in society. The EU's approach, rooted in rule of law, human rights, and democratic oversight, contrasts sharply with China's model, which prioritizes social stability, national security, and technological sovereignty. This fundamental difference isn't just an academic observation—it has real consequences for regulatory coordination and the interoperability of AI products between the EU and China. Rather than moving toward a unified global framework, the future of AI governance will likely depend on whether these systems can find points of compatibility rather than pursuing outright convergence. We argue that cooperation is only possible when governance models acknowledge and adapt to these underlying structural differences, rather than assuming a one-size-fits-all approach.

This study is based on a comprehensive, multi-source analysis of Chinese AI policies, government-issued strategies, masterplans, think tank reports, and press releases from 2017 to 2023. To ensure a robust examination, these sources are supplemented with scholarly and corporate publications that assess AI governance trajectories. Additionally, the study systematically analyzes European AI regulations from 2016 to 2024, with a particular focus on the European Parliament's 459-page Artificial Intelligence Act (legislative resolution of 13 June 2024). The paper is structured as follows: Section two explores how political culture and political economy shape AI regulation in the EU and China. Section three and four compares their departure points and their regulatory approaches, highlighting key differences in the light of political culture and political economy framework. The conclusion summarizes findings and assesses the potential for cooperation through regulatory compatibility rather than unification.

2. Theoretical Framework: Political Culture, Political Economy and Their Policy Nexus

The article takes the hybrid of political culture and political economy approach to analysing the EU's and China's AI regulations, which we believe are historically contingent and culturally bound outcomes. Political culture, a concept dating back to Almond and Verba (1963), explains how collective values, norms, and attitudes define the limits of state power and authority. Lucian Pye and Mary Pye (1985) argued that political development is highly sensitive to cultural variations, making it impossible to separate politics from culture. This cultural embeddedness extends to democracy itself. The "Singapore school" (Tan, 2012; Charteris, 2002; Chia, 2011) highlights Confucian principles, which prioritize hierarchy and stability over egalitarianism, challenging Western democratic assumptions. This perspective explains why Asia's governance models diverge from liberal norms.

The notion of Normative Power Europe (NPE) is that the EU is an 'ideational' actor characterized by common principles and acting to diffuse norms within international relations. Ian Manners (2002) defines this as the way the EU is able to spread its core norms and values beyond its own borders. The European narratives set out as normative pillars that are constitutive of the European identity, as illustrated by the Treaty of Lisbon itself that legitimize as follows:

"The Union's action on the international scene shall be guided by the principles which have inspired its own creation, development and enlargement, and which it seeks to advance in the wider world: democracy, the rule of law, the universality and indivisibility of human rights and fundamental freedoms, respect for human dignity, the principles of equality and solidarity, and respect for the principles of the

United Nations Charter and international law."(European Union, 2012).

In essence, EU, perceived as a normative power, instead of relying on a traditional "hard" power like military or economic coercion, hinges on its capacity to shape international norm, values and standards through example-setting and diplomacy. From the perspective of EU policymakers, the legitimacy of fast-paced AI development is consolidated through the reassurance of the empowerment to European citizens as enactors of human-centric change, rather than as passive subjects in the current of AI technological innovation. This seeks to renew the relationship between representatives and citizens, rejuvenating the cornerstone of democratic principles beyond mere vote polling (Ekdal and Manners, 2021). Following the global roles of civilian power (Carr, 1962) and military power (Bull, 1982), the EU perceives itself as being founded on benevolent norms and fundamental principles such as democracy, human rights, anti-discrimination, solidarity, and the rule of law.

Political culture and its embeddedness in the political economy play a defining role in shaping the market-development project. Europe, steeped in democratic norms, leans toward a neoliberal capitalist model whereas the state is bestowed with legitimacy to clear the regulatory and administrative barriers for private actors (such as providing a level playing field), educate private actors on historical norms and punish them when faced with breeding social-ills (such as the European Commission's antitrust rulings), and, at the very best, set up economic incentives and guarantees (such as derisking tools) to lure private actors to be drawn in the policy-endorsed economic sectors, ultimately leaving private actors to be the main driver of the economy (Gabor, 2023). The European political economy has never functioned as a macro-level national planner in the way China does, where economic planning is carried out through subnational municipal governments.

By contrast, China, bestowed upon a distinctive set of political and cultural values—a combination of Confucianism as both philosophy and state orthodoxy—formulates its draft of AI governance with different sets of considerations and focuses. As a state orthodoxy, Confucianism regards the government or the highest political authority as the true instrument in guiding the conduct of the society. Rooted in a legacy of centralized authority, the Confucianist norms emphasizes social harmony which uphold hierarchy, meritocracy, and collective well-being. The aim of Confucian orthodoxy was the well-organized society provided by the moral guidance of a Confucian-informed government. The social and political relevance and strength Confucianism, not to mention its longevity, is due to this coexistence of political philosophy with social harmony, making the state appear as the natural extension from one's family (Kwang-Ok, 1988). In contrast to Western history, the power of the Chinese state has not been seriously challenged by rivals (aristocracies, churches, capitals, merchants, etc.).The Chinese views on the state are very different from those of the West in the way that the state is seen not only as the defender of the Chinese civilization but also as the patriarch, the head of family (Li, 2016).

Extended to the economic and development realms, the state's "natural authority" is seen as the "guardian role" of economic development in the cultural consciousness of Chinese people and as the "development agent" in shaping China's economic directions and performance. In contrast to European neoliberal economic system, Chinese neo-developmentalist system sees economic development as the over-arching objective of the state, intertwined with national security, political sovereignty and long-term economic sustainability. This approach diverges from classical developmentalism, which shields domestic actors from global competition through mercantilist policies. Instead, China adopts a hybrid neo-developmentalist strategy: deploying developmentalist tools to engage in the industrial upgrading of the chosen sectors along the lines of the countries comparative advantages and shield emerging sectors

from overseas acquisitions. Simultaneously, it embraces neoliberal integration within global production networks, leveraging latecomer advantages to tap into its latent competitive advantages, which later feeds back to the industrial policy design of the next targets. This dynamic interaction between state-led planning and global market participation continuously reshapes China's industrial policy.

The neo-developmental Chinese state is a macro national planner with its evolving industrial policy emphasising different sectors at different times, contingent on evolving comparative advantages within the global neoliberal order. Ultimately, in this new development thinking, Chinese state is the main driver of market project which embeds business enterprises within a broader framework of state-driven planning, ultimately seeking to leapfrog advanced Western and Asian incumbents (Ban, 2013; Thurbon *et al*., 2023; Wade, 2018).

3. Two Different Sets of Departure Points to AI Regulation

The AI regulations of the EU and China are not merely technocratic adjustments but are deeply rooted in their distinct political cultures and economic frameworks. Grounded in this broader literature, this article proposes two theoretical foundations that underpin their respective AI governance strategies. In line with our comparative analysis, we identify the key driving forces behind their regulatory approaches: the EU's framework is anchored in the normative dimensions of AI, emphasizing ethical considerations and democratic values, while China's approach prioritizes the technical dimensions, viewing AI as a strategic tool for economic development. In essence, the EU's regulatory model embodies the principles of "democracy" in AI governance, whereas China's model is driven by the imperative of "development" which reflects "technocracy" in AI adoption and regulation.

3.1. The normative elements of EU's AI governance

The most notable development of AI principles that attempt to elevate the EU as a normative power to govern AI technologies, wishing to achieve the same extraterritorial "Brussels-effect" as its GDPR, is its "trustworthy" and "human-centric" approach. This ambition is exemplified by two significant 2019 deliverables—*Ethics Guidelines for Trustworthy AI and Policy and Investment Recommendations for Trustworthy AI in* 2019—written by the High-level Expert Group on AI (AI HLEG) (2019a, 2019b) set up by the European Commission in 2018. HLEG-AI does see the use of AI systems closely tied to democracy, which can be understood as an "umbrella concept" on which other normative dimensions depend and are connected to.

To Europe, an underlying narrative is that AI application seems to be interpreted as a potential threat to democratic mechanism.

"The use of AI systems should be given careful consideration, particularly in situations relating to the democratic processes, including not only political decision-making but also electoral contexts (e.g. when AI systems amplify fake news, segregate the electorate, facilitate totalitarian behaviour, etc.)". (AI HLEG, 2019a)

The human-centric approach emphasizes that AI should assist people in making informed decisions without removing their self-determination. Human oversight must remain the final arbiter (European Parliament, 2024) ensuring that AI systems are used responsibly. For example, a physician should still make the final diagnosis, despite AI assistance. This approach aligns with the OECD's human-centric values, and the EU has defined seven core principles:

Human Agency and Oversight underscores that human should always have the possibility ultimately

to over-ride a decision made by a system (AI HLEG, 2019a), meaning that AI should always retain a space for external feedback from diverse stakeholders, including affected individuals, community leaders, and advocacy groups. During the lifecycle of developing and deploying an AI system, the demographical landscape may undergo substantial changes, altering the context in which the system was originally designed and, consequently, the training data may become outdated or fail to accurately represent current realities. Given that AI systems evolve over time, constant monitoring and updating are necessary to address potential risks and keep the system relevant. Providers must be held accountable for system modifications if adverse effects arise.

Technical Robustness and Safety focuses on creating secure, reliable AI systems to prevent cyber-attacks and misuse. Developers must anticipate vulnerabilities and apply safeguards through rigorous testing such as penetration scanning and adversarial testing. Collaboration with cybersecurity experts is vital to ensure AI system safety during the design phase.

Privacy and Data Protection addresses the need for high-quality data that reflects community diversity, preventing biases that marginalize certain groups (MIT Technology Review, 2023). AI systems must safeguard personal data by ensuring it is collected, stored, processed, and shared securely and responsibly. Proper data handling is key to maintaining trust and preventing discrimination based on characteristics like ethnicity, gender, or sexuality.

Transparency demands clarity in AI's development, interaction with humans, and the outcomes of its decisions. First, AI building processes must be documented and traceable (European Research Service Parliament, 2019). Second, users must be informed when interacting with AI (European Law Institute, 2022) . Third, the decision-making processes must be understandable. Users should be able to seek clarification and appeal decisions, particularly in high-stakes situations affecting their well-being.

Diversity, Non-discrimination, and Fairness address the need to prevent built-in bias in AI algorithms. Even non-explicit bias in algorithmic models can harm vulnerable populations. Additionally, balancing model accuracy and robustness is critical. Highly accurate models might fail when applied to new, unseen data, so ensuring generalizability across different environments and data distributions is essential for fairness.

Societal and Environmental Well-being ensures that AI systems contribute positively to individuals' and society's physical and mental health. The development and deployment of AI should aim to promote the common good, considering long-term societal impacts.

Accountability stresses the need for mechanisms to ensure responsibility in AI systems. Regulatory bodies must oversee AI's adherence to ethical standards, conducting independent audits and impact evaluations. Non-compliance could result in sanctions, ranging from fines to legal action, fostering trust and mitigating risks.

In essence, these seven core principles of the EU serve as a tangible embodiment of democracy in the adoption and regulation of AI technology. Not constrained in its own judiciary, EU is poised to effectively become the world's AI police, creating binding rules on transparency, ethics, and more (European Union Agency for Law Enforcement Cooperation, 2024). However, even though the EU attempts to dominate AI ethical standards through the enactment of the Artificial Intelligence Act and other measures, some argues that its lack of technological strength greatly weakens its voice (Yan and Zhang, 2024) .

3.2. The technical components of Chinese AI governance

To China, the underlying narrative is that AI seems to be interpreted as a potential opportunity to economic growth and positive instruments to social life of citizens. In the 2025 Government Work Report,

the 'AI+' project is mentioned multiple times, with its official definition clarified as follows:

"Continuously promoting the 'AI+' initiative, better integrating digital technology with manufacturing and market advantages, supporting the widespread application of large-scale models, vigorously developing new generation intelligent terminals such as intelligent connected new energy vehicles, artificial intelligence smartphones and computers, intelligent robots, and intelligent manufacturing equipment."

Computing power, Algorithms, and Data (CAD) is perceived as the three core technical components of AI in China (Jiang *et al*., 2020). As noted by Byte Bridge (2021), "The algorithm, computing power, and data are the three basic elements of the development of artificial intelligence. Just as a triangle needs three sides to stabilize its shape, artificial intelligence will also need all three elements to perfect itself." CAD underscores the fundamental components that drive advancements and effectiveness in artificial intelligence. In the following, we have compared China, Europe and the US (as a shadow case) on each of CAD.

Computing Power refers to the hardware and infrastructure required to process massive datasets and execute complex AI algorithms efficiently. As of June 2024, China's total computing power has reached 246 EFLOPS, with intelligent computing power accounting for approximately 30% (76 EFLOPS)[1]. China's computing resources support 70% of AI training and 95% of inference tasks domestically, driven by the rapid expansion of intelligent computing infrastructure and the widespread adoption of large-scale AI models. The Guizhou Guian Supercomputing Center, for example, provides computational support for film rendering and AI model training through the "East Data West Computing" project. Additionally, the DeepSeek-R1 AI model has been deployed across multiple key computing hubs. By the end of 2023, China rank the second in terms of computing power scale, accounting for 26% of the global scale (CAICT, 2024).

By the end of 2023, the United States had a total computing power of 291.2 EFLOPS (FP32), accounting for 32% of the global total and ranking first in the world (CAICT, 2024). If the current annual growth rate of 40% continues, U.S. computing power is expected to surpass 400 EFLOPS by 2024. The country remains dominant in AI chips, particularly with NVIDIA GPUs, widely used for AI training, and investments by cloud providers like AWS and Microsoft. NVIDIA held a 95% market share in the data center GPU market in 2023[2]. Since NVIDIA is U.S.-based, this could be interpreted as the U.S. holding a near-monopoly in server GPU supply (NVIDIA's dominance may approximate U.S. share).

Europe has not publicly disclosed its total computing power, but estimates suggest it accounts for approximately 15%-20% of the global total, based on the 910 EFLOPS recorded worldwide in 2023. However, its development of intelligent computing power lags behind and remains heavily dependent on U.S. chips and technology ecosystems. To strengthen its position, the European Union has introduced the EU Chips Act, planning to invest €43 billion to increase Europe's share of advanced semiconductor production to 20% of the global market by 2030, while also promoting quantum computing and green data center construction (European Chips Act, 2023). However, due to limited domestic chip production, Europe remains highly reliant on external computing resources to meet its AI training and inference demands.

---

[1] At the recent "2024 China Computing Power Conference Opening Ceremony", Zhao Zhiguo, Chief Engineer of the Ministry of Industry and Information Technology, mentioned in his speech that China's total number of operational computing center racks has exceeded 8.3 million standard racks, with a total computing power reaching 246 EFLOPS, placing the country among the world leaders.

[2] https://x.com/Beth_Kindig/status/1695141490513899625.

Table 1
Overview of computing power in China, Europe and the US.

Dimension	China	Europe	United States
Total computing power	246 EFLOPS (June 2024)	136 EFLOPS (estimated)	291.2 EFLOPS (2023)
Computing power in global proportion	26% (as of 2023)	15-20% (as of 2023)	32% (as of 2023)
AI support capacity	Support 70% training and 95% inference tasks domestically	Mainly localized applications (dependent on external compute)	Supply more than 50% global training demand[3]
Policy investment	East Data West Computing project ($55.2 billion)	European Chips Act ($46.87 billion)	Chips and Science Act ($52.7 billion)

Algorithms are the backbone of AI, driving how systems learn from data and make decisions or predictions. They power key tasks like image recognition, natural language processing, and autonomous driving. Advancing algorithms—especially in areas like optimization, machine learning, and cryptography—is at the core of AI innovation, with plenty of policies worldwide focused on pushing the boundaries in both theory and application.

In 2024, U.S.-based institutions produced 40 notable AI models, compared to China's 15 and Europe's three (Stanford HAI, 2025). While the U.S. maintains its lead in quantity, Chinese models have rapidly closed the quality gap: performance differences on major benchmarks such as MMLU. China's rapid progress in natural language processing (NLP) is reflected in the rise of Chinese open-source large language models (LLMs), with companies like Alibaba's Qwen 1.5 and startups like Zhipu AI and DeepSeek making significant strides in the field. It's clear the AI race is no longer just a one-player game.

However, related to algorithmic theory and design, China continues to lead in AI publications and patents, with the US following with a smaller volume of filings than China but a higher proportion of granted patents. The EU and UK lag far behind both China and the U.S., highlighting slower growth in AI patenting activity. China dominates, accounting for 61.1% of global AI patent origins in 2022, far outpacing the U.S. (20.9%). While Europe lags behind, with only 1.17 thousand patents granted in 2022, China continues to lead with 35.31 thousand patents granted, highlighting its rapid growth in AI patent activity (Stanford HAI, 2025).

Data is the fuel that drives AI systems. AI data centers are not merely storage facilities but critical enablers of technological evolution. Cloud computing platforms (e.g., Microsoft Azure, AWS, Alibaba Cloud) and hyperscale data centers also play a vital role in AI infrastructure. Hyperscale data centers, owned by single companies, are becoming the epicenter of AI-driven tasks. These facilities offer significantly higher cloud computing capacity than traditional data centers and are crucial for AI applications. Major players in hyperscale data centers include Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP), and Alibaba, with AWS having the largest number of data center sites globally.

According to ABI research[4], the number of hyperscale data centers is expected to grow from 523 in 2024 to 738 by 2030. Shown in Fig. 1, European companies are less prominent in hyperscale data center

[3] https://www.grandviewresearch.com/industry-analysis/data-center-gpu-market-report
[4] https://www.abiresearch.com/blog/data-centers-by-region-size-company

ownership, with Google operating hyperscale data centers in several European countries like Denmark, Belgium, and the Netherlands. This also reflects the broader trend of digital infrastructure localization in response to increasing AI adoption. Countries like Germany, China, and Saudi Arabia are constructing local data centers to assert control over digital sovereignty and manage AI-related risks more effectively.

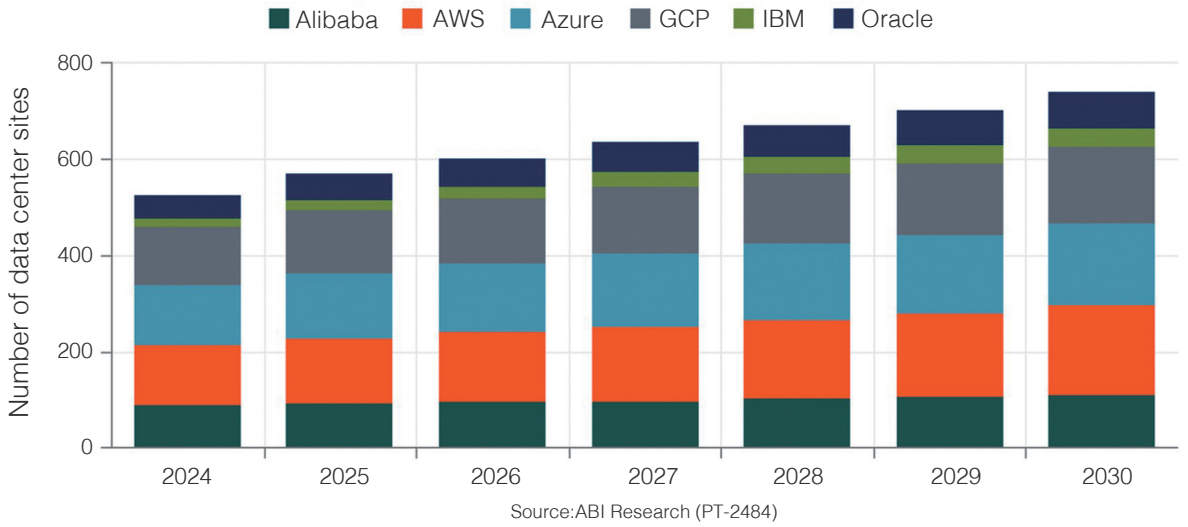

Fig. 1. Number of hyperscale data centers by company, 2024.

Data Annotation and Labeling play a crucial role in AI training, particularly for machine learning algorithms. The quality, quantity, and diversity of labeled data are critical for improving AI model performance and accuracy (Mohammed *et al.*, 2025). For example, autonomous driving systems require annotated data representing various driving scenarios to train AI. The growing demand for annotated data has led to the rise of specialized data labeling services, with companies like Appen leading the market. This trend will continue as AI development expands into more sophisticated and specialized domains. As AI development continues to expand into more sophisticated and specialized domains, the role of data annotation and management will remain central to technological progress.

4. Comparative Analysis of AI Regulation Approaches in the EU and China

4.1. Rights-focused risk-differentiated in the EU

Since 2016, the European Union (EU) has been working on a regulatory framework for artificial intelligence (AI). In April 2021, the European Commission proposed the AI Act, which represents the first comprehensive AI regulation by a major global regulator. The release of ChatGPT in November 2022 further accelerated this effort, culminating in the European Parliament's approval of the Act in June 2023 (European Parliament, 2024). By March 2024, the legislative resolution on the AI Act was adopted, with the EU's 27 member states unanimously endorsing it in December 2024. This makes the AI Act the first proposed AI-specific bill in the world, placing the EU in a pioneering position.

The AI act categorizes different AI applications through a risk-based approach, banning unacceptable uses of AI, regulating those that pose a high risk and encourages adopting codes of conduct for those

applications that are of limited- or no risk at all (European Commission, 2021). The EU's regulatory approach aims to prevent AI from potential risk of infringing upon fundamental rights clearly exhibiting a rights-focused approach to risk control, which contrasts sharply with China's security-focused approach to risk control, as further detailed in the section.

The regulation's core objective is to ensure that AI systems do not pose a threat to people's safety, livelihoods, and rights. It outlines practices that are prohibited due to their unacceptable risk to human rights. These include AI systems that manipulate individuals' behavior or impair decision-making, exploit vulnerable groups (e.g., individuals with disabilities), or engage in biometric categorization that infers sensitive attributes like race or political opinions (see Article 5 in Chapter II (European Parliament, 2024). Notably, the Act forbids general-purpose social scoring by public authorities, which would give differential treatment to individuals based on their social behaviors or personal characteristics. A crucial point here is that the AI Act limits the use of such scoring across unrelated social settings. "General-purpose" means that the social scores cannot be used across different settings, subjecting individuals to differential treatment in other un-related contexts. As the Act stipulates that it is forbidden that the use of the treatment "in social contexts that are unrelated to the contexts in which the data was originally generated or collected" (European Parliament, 2024, p 182) and the use of treatment "that is unjustified or disproportionate to their social behaviours or its gravity (European Parliament, 2024, pp 182)."Hence, financial credit scoring by private entities may still be allowed if transparent and non-discriminatory, meaning that the generated financial treatment should be proportionate and not crossed over to other social settings.

The regulation also prohibits certain AI practices, such as AI systems predicting crime likelihood based on profiling without objective facts, collecting facial images for surveillance databases without consent, or using 'real-time' biometric identification in public spaces for law enforcement, except in limited cases where such use is deemed essential for public safety. Real-time biometric identification is considered particularly intrusive to individuals' rights, as it could lead to feelings of constant surveillance and deter the exercise of fundamental freedoms like freedom of assembly (European Commission, 2021). However, the Act does allow for exemptions under specific conditions, such as 1) preventing imminent threats to life such as terrist attack, 2) targeted searching for potential crime victims such as missing children, 3) or locating suspects during criminal investigations (Veale and Borgesius, 2021).

Table 2
Examples of prohibited AI activities.

Type	Example
Exploiting vulnerable groups (Type 2)	An AI-driven financial advisory platform targets elderly individuals with limited financial literacy, providing misleading advice or pressuring them into risky investments.
General-purpose social scoring (Type 4)	A company uses AI to analyze social media activity and assign social scores, which affect hiring decisions. Candidates with lower scores may face discrimination, regardless of their qualifications.
Predictive policing (Type 5)	AI systems used by police predict crime likelihood based on demographic characteristics, leading to unfair targeting and increased surveillance of certain groups without evidence of criminal activity. This can result in discrimination and violations of privacy and civil liberties.
Real-time' remote biometric identification (Type 8)	Involves 'real-time' remote biometric identification, capturing, comparing, and identifying biometric data without significant delay, unlike 'post-time' systems. Post-remote systems, though high-risk, are not considered unacceptable risks by the EU and must be used proportionately, targeting specific individuals, locations, and times with legally acquired footage.

Regarding high-risk AI systems, these are defined as systems that have a significant impact on individuals' lives or on decision-making in areas such as safety, employment, healthcare, and access to essential services. Examples include AI systems used in employment or worker management, law enforcement, healthcare, and critical infrastructure. Article 6 of the AI Act classifies high-risk systems into two categories: (1) systems that serve as safety components in products governed by EU health and safety regulations (such as aviation or medical devices), and (2) systems deployed in specific areas like education, public services, law enforcement, and migration.

High-risk AI systems must comply with several requirements. Providers must register these systems in an EU-wide database before market release and ensure their systems are tested in real-world conditions. The AI Act mandates that Member States set up AI regulatory sandboxes to facilitate testing, especially for small and medium-sized enterprises (SMEs) and startups, which will be prioritized for access to these sandboxes. The Commission will provide technical support to help establish and operate these sandboxes.

Furthermore, providers of high-risk AI systems must conduct conformity assessments to ensure compliance with the AI Act. Some systems, especially those related to non-banned biometrics, must undergo third-party conformity assessments by a notified body, a private sector certification firm designated by an EU member state. The European Parliament justifies limiting third-party assessments to biometrics, citing the expertise of certifiers in product safety and the distinct risks involved. These assessments focus on testing systems for risks like bias, model drift, and security vulnerabilities.

Take Nice, who aims to be a model of "safe city" in France, for example. During the Carnival of Nice (from February 16th to March 2nd 2019), the real-time facial recognition test was deployed on various scenarios such as a child lost in the crowd or locating a "person of interest", which is excluded in prohibited AI type as it is public safety for a large event. This technology is developed by the Israeli company Any Vision comparing the sample pictures with the faces recorded by the surveillance devices at the entrance to the carnival. In this case, Any Vision should have conducted a third-party conformity assessment by a notified body. Controversially, and it still applies today, it is difficult to obtain the consent of all the participants in the Carnival, as required the General Data Protection Regulation (GDPR). It creates legal uncertainty in this area that warrants further legal clarity.

The regulation also emphasizes transparency. AI providers must ensure that AI systems generating synthetic content like deepfakes clearly indicate that the content is artificially generated. Providers must label AI-generated content with machine-readable markers, allowing automated systems to identify the content's artificial origin. This disclosure requirement is particularly important to avoid deception and ensure that users can distinguish between real and AI-generated content. Providers of general-purpose AI (GPAI) models must include clear instructions for use, enabling downstream users to understand the model's capabilities, limitations, and appropriate application. The European Parliament (2024, p 283) stipulates that "providers of AI systems, including GPAI systems, generating synthetic audio, image, video or text content, shall ensure the outputs of the AI system are marked in a machine-readable format and detectable as artificially generated or manipulated."

High-risk AI systems must adhere to strict **technical documentation** requirements by Articles 9 and 11. The documentation must include design specifications, input/output modalities, system architecture, model licensing, and the track record of relevant changes (see European Parliament, 2024, p 432). The purpose is to ensure transparency, traceability, and accountability throughout the lifecycle of the AI system. The technical documentation should also include cybersecurity measures to prevent

data poisoning, adversarial attacks, and other vulnerabilities. These systems must demonstrate resilience against errors and ensure robust data governance, including secure management of training, validation, and testing data. According to the European Parliament (2024, p 215), "high-risk AI systems must demonstrate resilience against errors, faults, or inconsistencies, especially in interactions with people or other systems." This includes technical redundancy solutions like backups and fail-safes. Documentation should address AI-specific vulnerabilities, such as data poisoning, model poisoning, adversarial examples, model evasion, confidentiality breaches, and inherent model flaws. Additionally, they should address inputs intentionally crafted to induce errors in the AI model, namely adversarial examples or model evasion, as well as confidentiality breaches or inherent flaws within the model.

In addition to these technical and transparency requirements, the AI Act introduces quality management systems, as outlined in Article 17, that AI providers must establish. These systems include monitoring the performance of AI systems post-market, reporting incidents, and ensuring that data used for AI training and testing is relevant, accurate, and complete, with meticulous **record-keeping of events (logs)** to identify risks and significant modifications. Providers must also establish risk management protocols to evaluate and mitigate identified risks. The risk management process is continuous and iterative, using system logs to detect and address issues like data quality, model drift, bias, and security vulnerabilities early.

Table 3
Summary of main requirements for providers of high-risk AI systems.

Number	Requirement types	Main content
1	Registration in EU database	AI systems must be registered in the EU database, including their status (e.g., on the market, recalled), operating logic, and impact assessments for high-risk AI systems.
2	Technical documentation (Article 11)	Providers must submit system details, including the provider's name, the system's purpose, hardware version, design specifications, and optimization goals.
3	Quality management systems (Article 17)	Establish a post-market monitoring system, incident reporting, data management procedures, and technical standards to ensure the system meets regulatory requirements.
4	Risk management (Article 9)	AI systems must undergo real-world testing to identify, mitigate, and control risks effectively.
5	Data governance (Article 10)	Data collection and origin must be documented. Training, validation, and testing data should be relevant, accurate, and complete, with any gaps or shortcomings identified.
6	Cybersecurity (Article 15)	AI systems must meet cybersecurity standards to prevent risks such as data poisoning, adversarial attacks, and exploitation of vulnerabilities in digital assets or underlying infrastructure.
7	Transparency to deployers (Article 13)	Providers must include clear instructions for use and mark AI-generated content (e.g., using watermarks or text overlays) to indicate its artificial nature for transparency.

Not only are they targeted at providers of AI systems, but several articles also specify obligations along the entire AI value chain, including those of providers, importers, and distributors. All of these fall within the regulatory scope.

AI systems categorized as presenting "limited risk", such as those interacting with humans (e.g.,

chatbots and some forms of deepfakes), are subject to lighter transparency obligations. Developers and deployers of such systems are mandated to ensure that end-users are informed of their interaction with AI. With regards to AI systems deemed as "minimal risk", they pose little to no risk to users' safety, rights, or freedoms. Examples include AI features in video games, spam filters, and basic recommendation algorithms. These systems are largely unregulated under the current framework due to their low-risk nature. Although compliance is voluntary for minimal risk AI systems, providers are encouraged to implement measures such as transparency in AI decision-making, user notifications, and robust data protection practices.

The AI Act also sets out penalties for non-compliance. The European Parliament mandates administrative fines for specific infringements and ensures that whistleblowers are protected under EU law. The European Parliament mandates that "the upper limits for setting the administrative fines for certain specific infringements should be laid down" (2024, p151) and "Persons acting as whistleblowers on the infringements of this Regulation should be protected under the Union law." (2024, p153).

To sum up. the EU's rights-focused, risk-differentiated approaches, as embodied in the Artificial Intelligence Act, is deeply rooted in its political culture of Normative Power Europe (NPE) and its neoliberal capitalist political economy. This normative commitment translates into AI governance that prioritizes individual empowerment and human-centric innovation, ensuring citizens are active enactors of change rather than passive subjects of technological disruption (Ekdal and Manners, 2021). The risk-differentiated approach—categorizing AI systems into unacceptable, high, limited, and minimal risk—reflects this by banning practices that violate fundamental rights (e.g., social scoring) and imposing stringent oversight on high-risk applications to safeguard dignity, equality, and anti-discrimination principles. In the EU's neoliberal framework, the state facilitates a level playing field for private actors, as described by Gabor (2023), by setting regulatory standards, enforcing compliance (e.g., antitrust rulings), and offering incentives like derisking tools to align market-driven AI development with democratic values. Unlike China's macro-level planning, the EU's regulatory state avoids direct economic control, instead shaping AI markets through normative guardrails that reinforce its identity as a global standard-setter.

4.2. Security-focused sector-differentiated regulation in China

The EU takes a rights-focused, risk-differentiated approach to AI regulation, while China's policy framework can be seen as a security and development-focused, sector-differentiated approach. In China, cybersecurity and vertical technical standardization are key priorities, as shown in its regulatory efforts since 2017. The State Council's Development Plan for the New Generation of Artificial Intelligence envisioned China as a global AI innovation center by 2023, but a comprehensive AI-specific regulation has yet to be enacted (For more information on the list of AI regulations, please refer to Appendix).

China's approach to AI policy is shaped by priorities that differ from Europe's rights-centered regulation. The Cyberspace Administration of China (CAC) , one of the influential policy agents in the field of AI, addresses AI primarily in the context of online information provision, with regulations such as Regulations on *the Management of Network Audio and Video Information Service* (CAC, 2019a) and Regulations on *Ecological Governance of Network Information Content* (CAC, 2019b). These mandates require security assessments for AI systems using technologies like deep learning, algorithmic recommendations, and virtual reality, especially those with public opinion attributes or social mobilization capabilities. The aim is to prevent AI-assisted dissemination of harmful content that threatens national security or unity. It

mandates online information providers to conduct **security assessment report** if they meet two criteria: (1) they use new AI technologies like deep learning, algorithmic recommendation technology, virtual reality, and deep synthesis, to provide feed information in audio or video forms; (2) they have public opinion attributes or social mobilization capabilities. Appearing very alarmingly, the agency seeks to prevent the AI technology-assisted dissemination of media information that jeopardizes national security, state secrets, and national unity, incites discrimination against groups or regions, or promotes vulgar content with clear policy priorities.

Fuelled by the blockbuster release of ChatGPT in November 2022, CAC (2022) subsequently issued *Administrative Provisions on Deep Integration of Internet Information Services and (2023)Interim Measures for the Management of Generative Artificial Intelligence Services*, mandating deep synthesis service providers must clearly mark generated or edited content to inform the public of the nature of the deep synthesis outcomes, and must maintain event logs.

The uptake of these administrative measures by CAC, focused on integrating AI technology into online information provision—classified in Europe as either "high risk" or "limited risk"—clearly underscores the centrality of political stability and digital sovereignty in China's policy agenda. Alongside these measures, emphasis on data annotation, high-quality labeled data, and secure data storage reflects a distinctive approach: while Europe primarily views data through the lens of privacy, China regards it as a pillar of sovereignty, security, and political stability.

Another policy agent— National Information Security Standardization Technical Committee (NISSTC)—addresses AI systems on the terms of technical standardisation and security. As revealed in the release of multiple documents such as *White Paper on Artificial Intelligence Security Standardization (2019) and Network Security Standard Practice Guide* (2021), "security risk" has been framed as the top priority and has been categorised into five types of risk based on CAD acronym: (1) Algorithm Model Security Risks; (2) Data Security and Privacy Protection Risks; (3) Data Storage, Sharing, and Transmission Security Risks; 4) Infrastructure Security Risks; 5) Application Security Risks.

Data labelling and annotation, particularly concerning generative AI, is a key area of focus in China's AI governance. NISSTC (2024) released *Basic security requirements for generative artificial intelligence services*, which include conducting **a security assessment report** on (1) input data security, which address the data resources in relation to privacy rights, fair and unbiased representation, its compliance with intellectual property rights, relevant to industry like art, literacy, film, and, most importantly, **data annotation** to identify 31 types of risks (detailed in the Appendix 1); (2) output data security, which evaluates the generative output against test questions addressing 31 types of risks; and (3) maintaining a refusal output database, whose database identifies content to avoid, such as material related to religion, culture, and national security. This focus on securing data reflects China's view of data as a pillar of sovereignty and political stability, contrasting with Europe's privacy-focused approach.

The *Guidelines for the Construction of the National New Generation Artificial Intelligence Standard System* (Standardization Administration of China *et al*., 2020) consolidated that the term "security" is often found used together with "standard" or "standardization" as a solution to mitigate the security risk. Worth noting, the security standards have covered six types: (1) Basic AI Security Standards, concerning international security terminology and principles; (2) Data, Algorithms, and Model Security Standards, concerning data integrity, model trustworthiness; (3) AI Technology System Security Standards, concerning AI infrastructure security; (4) AI Security Management and Service Standards, concerning AI supply chain security; (5) AI Security Testing and Evaluation Standards, concerning standardising the standards and (6) AI Product and

Application Security Standards, concerning end-user application security.

In line with these policies, CAC has implemented an algorithm filing system for generative AI services with public opinion attributes or social mobilization capabilities, as evidenced by *the Interim Measures for the Management of Generative Artificial Intelligence Services* (CAC *et al*., 2023). As of May 2025, CAC had approved 211 generative AI products, underscoring the importance of regulation in this space (CAC, 2025). Generative AI providers are required to submit detailed reports, including information about their algorithms and their intended purposes, to ensure alignment with national security interests (Gao and Yan, 2025).

Table 4
Summary of requirements for providers of Generative AI

Number	Requirement types	Main content
1	Security assessment report	Includes input data security check, output data security test, and refusal output database for content related to sensitive topics.
2	Algorithm filing system	Requires provider's name, system purpose, hardware version, design specifications, and system optimization details.

In addition to security concerns, neo-developmentalist China's AI policy emphasizes industrial development. Unlike the EU, which regulates AI across a wide range of applications, China focuses on embedding AI within specific industries like manufacturing, raw materials, and critical infrastructure. This sector-differentiated approach is designed to drive economic productivity and growth.

While China has yet to enact a comprehensive "Artificial Intelligence Law" akin to the EU AI Act, its industry associations, private telecom giants and enterprises, surprisingly, take a bottom-up approach to set the scene. *Artificial Intelligence Endogenous Security White Paper* spearheaded by China Unicom and other industrial associations (2024) is a comprehensive industrial document that explores the concept of endogenous security in the context of artificial intelligence (AI). Endogenous security refers to the inherent safety and robustness of AI systems, ensuring they are secure by design and can operate reliably in various environments that are inherently secure and resilient to external threats. Unlike the European approach to risk mitigation, which focuses on addressing built-in risks inherent to the model itself, the Chinese industrial guidelines aim to mitigate risks that arise from external factors and pressures. In other words, while Europe is busy tinkering with the engine, China's out there reinforcing the walls.

Interestingly, *Artificial Intelligence Demonstration Law 2.0 (Expert Suggestion Draft)* (Institute of Law *et al*., 2024) and *Artificial Intelligence Law (Scholar's Suggestion Draft)* (Institute of Data Law *et al*., 2024) are the most two European-minded documents written by the Chinese academics of notable universities, underscoring algorithmic transparency, data protection and accountability mechanism to both AI developers and AI providers. Moreover, they, in line with the Chinese guidelines, proposed Sector-Specific specifications for high-impact sectors such as healthcare, biometric verification, autonomous driving, finance, and criminal justice.

To sum up, China's security-focused, sector-differentiated AI regulation emerges from its political culture of Confucianist state orthodoxy and its neo-developmentalist political economy, which prioritize centralized authority and national strategic goals. Confucian norms, emphasizing hierarchy, social harmony, and collective well-being, position the state as a patriarchal guardian of society, extending its moral and developmental authority into AI governance (Kwang-Ok, 1988; Li, 2016). This cultural embeddedness manifests in regulations like the 2023 Interim Measures for Generative AI, which mandate

security assessments, algorithm filing, and data sovereignty to ensure AI aligns with social stability and national security objectives. The neo-developmentalist strategy, as outlined by Ban (2013) and Thurbon *et al*. (2023), integrates state-led industrial planning with global market participation, targeting AI as a sector for technological leapfrogging and geopolitical competitiveness. Unlike the EU's universal risk model, China's sector-specific approach tailors regulations to strategic industries, shielding emerging AI applications from external threats while embedding them within state-driven frameworks. This hybrid model reflects the state's role as the primary driver of economic and technological development, contrasting with the EU's market-driven, rights-centric paradigm.

5. Conclusion: EU-China AI Collaboration Through Pragmatic Adaptation rather than Harmonization

The paper identifies two distinct approaches to AI governance: the EU's rights-focused, risk-differentiated approach and China's security-focused, sector-differentiated approach. These approaches reflect their respective political cultures, with the EU prioritizing human rights and transparency, while China focuses on national security and digital sovereignty. As detailed in Table 5, the findings highlight three key differences: (1) the Regulatory Philosophy: The EU focuses on the embodiments of democracy which prioritises rights protection, while China focuses on security and technological competitiveness which translates into Computing power, Algorithms, and Data (CAD); (2) Focus and Approach: The EU uses a universal risk model, while China tailors regulations by sector; (3) Key Characteristics: The EU mandates accountability and explainability, while China emphasises data labelling, content control and Cybersecurity measures.

Table 5
Summary of key characteristics of AI regulations in the EU and China.

	The regulatory philosophy	**Focus and approach**	**Key characteristics**
China	Computing power, Algorithms, and Data (CAD)	Emphasis on security risks and security standards	Data labelling and data annotation to ensure alignment with national security, social harmony, and political integrity.
		Guidelines that seek to keep external risks at bay	Cybersecurity measures that span over the lifecycle of AI system.
		Strict content regulation to prevent misinformation and social disharmony and disability	Security assessment report and algorithmic filing system if the service providers of AI tools have public opinion attributes or social mobilization capabilities.
The EU	Human Rights and Ethics	Emphasis on the degree of right violations of AI	Technical documentation that covers cybersecurity measures and system design.
		Guidelines that seek to keep built-in risks at bay	Quality management documentation that covers data governance, record-keeping of events (logs).
		Strict transparency and explainability on the system design and the generated outcomes	AI regulatory sandboxes to provide guidance on real-world testing and validation to ensure systems operate safely before market release. SMEs are given priority access to these sandboxes.

The EU, perennial champion of human rights, transparency, and bureaucratic oversight as a normative power, treats AI like a potential existential risk to individual rights. The EU's regulatory model is classic Brussels-effect: a meticulous, risk-based approach that categorizes AI based on its potential to trample on civil liberties. High-risk AI systems—think hiring algorithms, facial recognition, and automated legal decision-making—get the regulatory equivalent of a full-body scan. If a company wants to deploy one of these systems, it needs to jump through a series of administrative hoops, proving compliance with rigorous standards on data governance, risk management, and technical documentation.

In China, however, only generative AI providers with social mobilization abilities must prepare a security assessment report and algorithm filing documentation. For China imbedded in the Confucianist norms and neo-developmentalist mindset, AI isn't about protecting individuals—it's about securing the state. China's approach to AI governance is deeply tied to its broader political priorities: national security, social stability, and digital sovereignty. China frames risk in terms of national security, political stability, and social harmony. Data and algorithm design in China are prioritized through the lens of digital sovereignty, with regulations focused on data screening, annotation, and high-quality data sharing. Chinese regulations also place heavy oversight on online information providers and generative AI developers to maintain control over content and safeguard national interests.

Moreover, the framework is sector-specific rather than risk-based, meaning AI regulation isn't just about whether a system could violate human rights—it's about where and how it's deployed. AI tools used in critical industries, from finance to surveillance, get intense scrutiny, with tight controls over data screening and algorithmic design to ensure they serve the state's strategic interests. Chinese security-focused approach is deeply steeped in its neo-developmental philosophies, as differentiated security standards are proposed in different critical sectors, hoping to standardize security measures to drive technological stability and productivity, leading to hyper growth through AI-facilitated reindustrialization of key sectors. China's focus on the vertical application of AI—what we term "AI reindustrialization"—is central to its technological competitiveness and global leadership in AI. This approach involves deploying specialized industrial AI models across key sectors, integrating AI into every phase of development, from building productive AI infrastructures to delivering end-user applications. Each phase is subject to tailored security requirements, ensuring that AI advancements align with national priorities while addressing sector-specific risks.

To sum up, the EU burdens AI developers with layers of regulatory red tape in terms of protecting rights, while China is more interested in making sure AI serves its broader geopolitical and economic goals. The bigger picture? The EU wants AI to be an extension of its human-rights-first philosophy, wrapping it in legal and ethical constraints. China, on the other hand, sees AI as a lever for industrial and geopolitical dominance, an engine of what you might call "AI-facilitated reindustrialization." However, Europe normative power might wane due to its stifling European competitiveness, creating a landscape where homegrown AI firms struggle under compliance costs while American and Chinese firms—operating under far looser constraints—race ahead.

The regulatory disparities between the EU and China present challenges for harmonization. The world of global AI governance is a textbook case of what political scientists call "regime complexes"(Xue, 2024)—overlapping, sometimes conflicting regulatory frameworks that don't neatly stack into a single hierarchy. It's not a question of whose rules win; it's a messy tangle of competing priorities, different political economies, and bureaucratic headaches.

For Chinese AI firms trying to break into the EU market, it's a bureaucratic obstacle course. They

need to submit detailed technical documentation, pass conformity assessments, and, if they don't have an office in Europe, appoint an EU-based representative just to navigate the legal labyrinth. On the flip side, European AI firms looking to operate in China are up against an entirely different kind of regulatory beast—one that's as much about control as it is about compliance. They have to abide by China's Data Security Law (DSL) and Personal Information Protection Law (PIPL), which means storing data locally, aligning their AI systems with China's social and political frameworks, and ensuring their outputs don't clash with state-defined narratives. In short, both sides are struggling to export AI under rules designed for completely different political realities.

The EU and China's AI regulatory frameworks exert profound influence on global governance by establishing competing paradigms that other nations must navigate. The EU's model, with its emphasis on universal human rights and risk-based categorization, appeals to liberal democracies and regions seeking to align with Western normative standards. This "Brussels Effect" amplifies the EU's influence, as companies like Google or Microsoft adapt their AI systems to meet EU standards globally to avoid fragmentation (Bradford, 2020). Conversely, China's security-focused, sector-specific model resonates with authoritarian regimes and developing nations prioritizing economic development and state control. China exports this model through AI infrastructure investments in Belt and Road countries, such as Pakistan and Ethiopia, where it provides data centers, surveillance systems, and training programs tailored to local governance needs (Xinhua, 2024). This approach challenges Western norms by offering a viable and pragmatic alternative that seeks to AI capacity-building programs aimed at reducing the "digital gap" between the global South and the global North.

Could China and Europe learn from each other? We argue that particularly as AI adoption expands in critical sectors such as credit lending, healthcare, employment, and elder care in Chinese society, China should take greater reference in terms of privacy, explainability and accountability dimensions from the European AI Act. These applications directly impact citizens' access to essential services and their eligibility for institutional support, making regulatory safeguards increasingly necessary. Conversely, Europe should place greater emphasis on fostering AI competitiveness to back up its commitment to democratic values on the global stage. We argue that the EU's normative power depends on technological credibility. Without competitive AI systems, its global influence risks being overshadowed by China's neo-developmentalist advancements or U.S.

In terms of global AI governance. The EU and China could collaborate on AI capacity-building programs in Belt and Road or EU partner countries (e.g., African nations), combining China's infrastructure expertise (e.g., data centers) with EU's ethical training modules. For instance, joint projects could deploy AI for elder care in Kenya, integrating EU's risk assessments with China's security protocols. Collaboration could also focus on developing joint cybersecurity standards, a high priority for both regions. By aligning on protocols for secure AI systems, the EU and China could enhance trust and interoperability in global AI deployments. Moreover, they could negotiate a limited data-sharing framework with each other for AI research in non-sensitive sectors (e.g., in culture and music industries which can facilitate cross-border understanding of arts and aesthetics of the citizens), with mutual safeguards. The EU could relax GDPR restrictions for anonymized datasets, while China ensures compliance with its data sovereignty laws.

Acknowledgements

This work is supported by National Social Science Funds of China-NSSFC: [Grant Number 20CJY029]

and the Independent Research Fund Denmark (Grant Number 8019-00044B). We wish to thank the reviewers for their constructive and engaging input for improving the article.

Conflicts of interest

The authors declare no conflict of interest.

References

AI HLEG, 2019a. Ethics guidelines for trustworthy AI. *Publications Office of the European Union*. https://data.europa.eu/doi/10.2759/346720.

AI HLEG, 2019b. Policy and investment recommendations for trustworthy AI. Publications Office of the European Union.

Almond, G. A., & Verba, S., 1963. The Civic Culture: Political Attitudes and Democracy in Five Nations. Princeton University Press. https://www.jstor.org/stable/j.ctt183pnr2.

Ban, C., 2013. Brazil's liberal neo-developmentalism: New paradigm or edited orthodoxy? *Review of International Political Economy*, 20(2), 298–331.

Bradford, A., 2020. The Brussels Effect: How the European Union Rules the World. Oxford University Press. https://doi.org/10.1093/oso/9780190088583.001.0001, accessed 5 June 2025.

Bull, H., 1982. Civilian power Europe: A contradiction in terms? *Journal of Common Market Studies*, 21(2), 149–170.

ByteBridge, 2021. Importance of training data in different AI algorithm stage. Medium. https://becominghuman.ai/the-different-algorithm-stage-the-differentiated-demand-for-data-b25e16d230d9.

CAC, 2019a. Notice on the issuance of the "Administrative provisions on network audio-video information services". Ministry of Culture and Tourism. https://zwgk.mct.gov.cn/zfxxgkml/zcfg/gfxwj/202012/t20201204_906347.html.

CAC, 2019b. Provisions on the ecological governance of network information content. Cyberspace Administration of China. https://www.cac.gov.cn/2019-12/20/c_1578375159509309.htm.

CAC, 2022. Regulations on the management of deep synthesis in internet information services. State Council. https://www.gov.cn/zhengce/zhengceku/2022-12/12/content_5731431.htm.

CAC, 2025. Announcement of the State Internet Information Office on publishing the eleventh batch of deep synthesis service algorithm filing information. Cyberspace Administration of China. https://www.cac.gov.cn/2025-05/19/c_1749365589879703.htm.

CAC, NDRC, & MoE, *et al*., 2023. Interim measures for the management of generative artificial intelligence services. Cyberspace Administration of China. https://www.cac.gov.cn/2023-07/13/c_1690898327029107.htm.

CAICT, 2024. China comprehensive computing power index. CAICT. https://www.sgpjbg.com.cn/, https://www.sgpjbg.com.cn/.

Carr, E. H., 1962. The twenty years' crisis, 1919-1939: An introduction to the study of international relations (2nd ed.). Macmillan and Co.

Charteris, C., 2002. Democratic discourses in Indonesia, Thailand, and the Philippines. *Journal of Southeast Asian Studies*, 29, 1–15.

Chia, Y. T., 2011. The elusive goal of nation building: Asian/Confucian values and citizenship education in Singapore during the 1980s. *British Journal of Educational Studies*, 59(4), 383–402.

China Unicom, 2024. White paper on endogenous security of artificial intelligence. China Unicom. https://www.fxbaogao.com/detail/4680423.

Chinese Academy of Social Sciences, Tongji University, & People's Public Security University of China, 2024. Artificial intelligence demonstration law 2.0 (expert suggestion draft). 21st Century Business Herald.

Coeckelbergh, M., 2024. The case for global governance of AI: Arguments, counter-arguments, and challenges ahead. AI and Society, 39(6), 2867–2878.

Ekdal, D., & Manners, I., 2021. Normative power Europe and AI. JCMS: Journal of Common Market Studies, 59(3), 641–658.

Emery-Xu, N., Jordan, R., & Trager, R., 2024. International governance of advancing artificial intelligence. *AI & Society*, 39(5), 2451–2465.

European Commission, 2021. Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts. European Commission.

European Parliament, 2024. European Chips Act. European Parliament.

European Law Institute, 2022. Guiding principles for automated decision-making in the EU. European Law Institute.
European Parliament, 2024. Artificial Intelligence Act. European Parliament.
European Research Service Parliament, 2019. EU guidelines on ethics in artificial intelligence: Context and implementation.
European Parliament. https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/640163/EPRS_BRI(2019)640163_EN.pdf
European Union, 2012. Human rights and democracy. European External Action Service. https://www.eeas.europa.eu/eeas/human-rights-democracy_en.
European Union Agency for Law Enforcement Cooperation, 2024. AI and policing: The benefits and challenges of artificial intelligence for law enforcement. *Publications Office of the European Union*. https://data.europa.eu/doi/10.2813/0321023.
Gabor, D., 2023. The (European) derisking state. *Journal of European Public Policy*, 30(5), 789–812.
Gao, X., & Yan, Y., 2025. The composite regulatory governance framework for generative artificial intelligence services in China and its optimization: A mixed study based on policy texts and in-depth interviews. D IANZI ZHENGWU, 2025(05): 2-15.
Institute of Data Law, China University of Political Science and Law, & Northwest University of Political Science and Law, *et al*., 2024. Artificial intelligence law (scholar's suggestion draft). China Law Network.
Jiang, F., Jiang, Z., & Kim, K. A., 2020. Capital markets, financial institutions, and corporate finance in China. *Journal of Corporate Finance*, 63, 101309.
Kim, J., Detrick, R., & Yu, S., *et al*., 2025. Socially shared regulation of learning and artificial intelligence: Opportunities to support socially shared regulation. *Education and Information Technologies*, 30(1), 123–145.
Kwang-Ok, K., 1988. A study on the political manipulation of elite culture: Confucian culture in local level politics. *Korea Journal*, 28(11), 4–16.
Laux, J., 2024. Institutionalised distrust and human oversight of artificial intelligence: Towards a democratic design of AI governance under the European Union AI Act. *AI and Society*, 39(6), 2853–2866.
Li, X., 2016. Understanding China's economic success: "Embeddedness" with Chinese characteristics. *Asian Culture and History*, 8(2), 18–31.
Manners, I., 2002. Normative power Europe: A contradiction in terms? JCMS: Journal of Common Market Studies, 40(2), 235–258.
MIT Technology Review, 2023. Five things you need to know about the EU's new AI Act. MIT Technology Review.
Mohammed, S., Budach, L., & Feuerpfeil, M., *et al*., 2025. The effects of data quality on machine learning performance on tabular data. *Information Systems*, 132, 102549.
NISSTC, 2019. Artificial intelligence security standardization white paper. National Information Security Standardization Technical Committee.
NISSTC, 2021. Network security standard practice guide—guidelines for preventing ethical and security risks in artificial intelligence. National Information Security Standardization Technical Committee.
NISSTC, 2024. Basic security requirements for generative artificial intelligence service. National Information Security Standardization Technical Committee.
Orwat, C., Bareis, J., & Folberth, A., *et al*., 2024. Normative challenges of risk regulation of artificial intelligence. NanoEthics, 18(2), 11.
Pye, L. W., & Pye, M. W., 1985. Asian power and politics: The cultural dimensions of authority. Harvard University Press.
Racine, E., Ji, S., & Badro, V., *et al*., 2024. Living ethics: A stance and its implications in health ethics. *Medicine, Health Care, and Philosophy*, 27(2), 137–154.
Rusche, H., 2023. AI as a challenge for legal regulation: The scope of application of the Artificial Intelligence Act proposal. ERA Forum, 23(3), 361–376.
Sahebi, S., & Formosa, H., 2024. Artificial intelligence and global justice. *Minds and Machines*, 35(1), 4.
Standardization Administration of China, Cyberspace Administration of China, & NDRC, *et al*., 2020. The guidelines for the construction of the national new generation artificial intelligence standard system. State Council.
Stanford HAI, 2025. Artificial intelligence index report 2025. Stanford University Press.
State Council, 2025. The government work report.
Tambiama, M., 2020. EU guidelines on ethics in artificial intelligence: Context and implementation. European Parliament.
Tan, C., 2012. 'Our Shared Values' in Singapore: A Confucian perspective. Educational Theory, 62(4), 449-463.
Thurbon, E., Kim, S.Y., & Tan, H., *et al*., 2023. Developmental environmentalism: State ambition and creative destruction in East Asia's green energy transition. Oxford University Press.

Van Maanen, S., 2024. AI ethics, ethics washing, and the need to politicize data ethics. *Digital Society*, 3(2), 9-16.

Veale, M., & Borgesius, F. Z., 2021. Demystifying the draft EU Artificial Intelligence Act. Computer Law Review International.

Wade, R. H., 2018. The developmental state: Dead or alive? *Development and Change*, 49(2), 518–546.

Xinhua, 2024. China leads global AI cooperation as 140 nations co-sponsor UN resolution. Xinhua News Agency. https://english.news.cn/20240702/5ccf6bb8060a4979a18cd5ddeb9c2a5c/c.html.

Xue, L., 2024. Four major risks of AI spark concerns: How can global governance keep pace with the rapid advance of technology? *Tansuo Yu Zhengming*, 15(6), 8-19.

Yan, S. H., & Zhang, Y., 2024. A comparison of AI governance models in Europe and the United States: Insights and implications). *Zhanlue Juece Yanjiu*. 2024(3), 41-65.