Featured Article

AI Compliance Observations in China, the EU, and the United States

Stuart Russell, an AI expert, famously posed the "Gorilla Problem": When humans create a species with intelligence far surpassing their own, will they find themselves dominated, as gorillas are?[1]

To mitigate the various crises arising from Artificial Intelligence (AI), legislators worldwide are actively developing solutions. A global competitive landscape is forming, led by the United States, China, and the European Union. According to data released by Stanford HAI, these three major jurisdictions possess the vast majority of frontier models globally.[2] Given the differences in technological development and legal systems across these jurisdictions, distinctive governance paradigms have emerged.

To better understand the compliance boundaries in the AI sector, this article reviews and interprets AI compliance requirements across these jurisdictions, providing a reference for AI industry participants.

1 Stuart Russell, Human Compatible: Artificial Intelligence and the Problem of Control, at 132 (2019).

2 Stanford Univ. Inst. for Human-Centered AI, Artificial Intelligence Index Report 2025, at 4 (2025).

I. China

With the formal publication of the *Measures for the Labeling of Artificial Intelligence-Generated and Synthesized Content* on March 14, 2025, China completed another key component of the regulatory framework for its AI industry.[3] China adopts a model of **vertical stratification and horizontal categorization**, relying on superior legislation to issue specific administrative regulations targeting concrete applications such as algorithm recommendations, deep synthesis, and generative AI, thereby establishing a closed-loop governance system from data sources to content terminals.

(I) Foundational Legislation

The *Cybersecurity Law*, the *Data Security Law* (DSL), and the *Personal Information Protection Law* (PIPL) collectively form the overarching legislative design in China's cyber law domain.[4]

1. **The *Cybersecurity Law* (CSL)** The *Cybersecurity Law* underwent its first revision in nearly a decade in December 2025 (hereinafter referred to as "the Amendment"), focusing on adjusting legal liability while accommodating technological trends such as AI.[5] The Amendment introduced a specific "AI provision" encompassing four core elements:

First, strengthening foundational support: clarifying that the state supports fundamental AI theory research and the development of core technologies, such as algorithms. This support aligns with policies such as the "AI +" action plan, aiming to enhance model capabilities, advance core technologies, and foster high-value application scenarios.

Second, clarifying resource supply: promoting the construction of training

3 *See Notice of the Cyberspace Administration of China on Issuing the Measures for the Labeling of Artificial Intelligence Generated and Synthesized Content*, (Mar. 14, 2025), available at https://www.cac.gov.cn/2025-03/14/c_1743654684782215.htm.

4 *Cybersecurity Law of the People's Republic of China* (promulgated by the Standing Comm. Nat'l People's Cong., Nov. 7, 2016, effective June 1, 2017) (P.R.C.). *Hereinafter* CSL.

Data Security Law of the People's Republic of China (promulgated by the Standing Comm. Nat'l People's Cong., Sept. 1, 2021, effective Sept. 1, 2021) (P.R.C.).. *Hereinafter* DSL.

Personal Information Protection Law of the People's Republic of China (promulgated by the Standing Comm. Nat'l People's Cong., Aug. 20, 2021, effective Nov. 1, 2021) (P.R.C.). *Hereinafter* PIPL.

5 *Decision of the Standing Committee of the National People's Congress on Revising the Cybersecurity Law of the People's Republic of China* (promulgated by the Standing Comm. Nat'l People's Cong., Oct. 28, 2025), *available at* http://www.npc.gov.cn/npc/c2/c30834/202510/t20251028_449048.html (last visited Dec. 9, 2025).

data resources and computing power infrastructure. This strategy not only affirms the legality of compliance-based processing of training data but also treats training data as critical infrastructure, thereby providing legal guidance for resolving data compliance challenges specific to generative AI.

Third, establishing ethical standards: elevating previously scattered ethical requirements to legal obligations, emphasizing security assurance capabilities in compliance, and establishing an **"ethics-first" governance tone**.

Fourth, perfecting risk governance: establishing a governance path to strengthen risk monitoring, assessment, and security supervision.

The Amendment significantly revised the legal liability provisions for network operational security and Critical Information Infrastructure (CII) security, reflecting a legislative spirit of **"combining strictness and leniency, and applying precision policies".** This revision systematically strengthened network operational security responsibilities, including significantly raising the upper limit on fines, imposing penalties on senior personnel, and introducing enforcement measures better suited to the mobile internet era, such as the shutdown of applications. While penalties were increased, a safe harbor is provided. The Amendment aligns with the *Administrative Penalty Law* by expanding the circumstances under which penalties may be waived or reduced (e.g., by voluntarily eliminating or mitigating the harmful consequences of illegal acts), thereby incentivizing enterprises to establish proactive compliance systems and evidence-based emergency **response mechanisms**.

2. **The *Data Security Law* (DSL)** established **"data classification and grading"** and **"cross-border transfer management"** systems to safeguard national data sovereignty and complete lifecycle security. Given that generative AI relies heavily on large datasets for training, the DSL provides the legal foundation for data element governance in AI. Its core requirements compel AI enterprises to establish data classification and grading protection systems, rigorously identify, and strictly control Important Data and Core Data within their training datasets. Concurrently, it mandates that enterprises implement comprehensive lifecycle data security management (acquisition, storage, processing, disposal), ensure the use of legal data sources and compliant processing procedures, and set strict security assessment and approval redlines **for cross-border data transfers** involved in AI model development or service exports.

The *Regulations on Network Data Security Management* further established a comprehensive compliance

framework that covers data acquisition, model training, and AI application services.[6] **At the source**, it mandates that generative AI services strengthen training data security management and strictly prohibit automated scraping used for illegal intrusion or interference with network operations. **At the application level, it grants users the right to refuse/opt out and to delete user tags, thereby** breaking the cycle of mandatory algorithmic content pushing. **At the regulatory level**, it draws a clear line against large online platforms that use algorithms to deceive or engage in unreasonable differential treatment (Big Data discrimination), thereby confirming that data processors must build technological applications on a foundation of data security, lawful sourcing, fairness, and transparency.

3. **The *Personal Information Protection Law* (PIPL)** is dedicated to protecting personal information rights, establishing the **notice-consent principle**, and requiring **separate consent** for sensitive personal information. However, generative AI may involve scraping large volumes of personal information during training, a process that is often automated and technically difficult to distinguish between general and sensitive information, posing challenges for technical compliance with the law.

(II) Administrative Regulations

1. **Targeting Algorithm Recommendation Technology: *The Administrative Provisions on Algorithm Recommendation for Internet Information Services (2022).*** [7] These provisions are China's first specific departmental rules on algorithmic recommendation technology, jointly issued by the Cyberspace Administration of China and three other departments. It aims to integrate technology applications into a legal framework through **graded, classified management and an algorithmic filing system**. It establishes the service provider's **principal legal responsibility**, strictly prohibiting the use of algorithms to induce addiction, manipulate rankings, engage in monopolistic behavior, or utilize **Big Data discrimination.** Simultaneously, it mandates breaking the algorithmic black box by granting users the **right to be informed** and the **right to refuse/opt-out**, particularly to reinforce the protection of minors, older persons, and workers. The promulgation of these provisions marked a shift in China's internet governance

6 *Regulations on Network Data Security Management* (promulgated by the Cyberspace Admin. of China, et al., effective Jan. 1, 2025) (P.R.C.). *Hereinafter* Data Security Regulations.

7 *Administrative Provisions on Algorithm Recommendation for Internet Information Services* (promulgated by the Cyberspace Admin. of China, et al., effective Mar. 1, 2022) (P.R.C.). *Hereinafter* Algorithm Recommendation Provisions.

from simple content regulation to algorithmic governance.

2. **Targeting Deep Synthesis Technology: *The Administrative Provisions on Deep Synthesis for Internet Information Services (2023).***[8] These regulations are specialized rules for deep synthesis, aiming for transparent and controllable technology applications across the value chain. They mandate that service providers implement **real-name authentication** and content review, requiring **prominent labeling** of AI-generated and synthesized content to prevent public confusion. They set a **separate consent** threshold for processing biometric information, such as facial and voice data, and establish a **dual-access mechanism for algorithm filing and security assessment,** thereby mitigating the risks of forgery, fraud, and data security breaches associated with AI technology.

3. **Targeting Large Models: *The Interim Measures for the Management of Generative Artificial Intelligence Services (2023).*** [9] These interim measures are specialized regulations for generative AI services, establishing a regulatory tone that **emphasizes both development and security** and employs an **inclusive and prudent regulatory approach.** It primarily regulates generative AI services provided to the public in China, building a comprehensive compliance system from **source data governance** (requiring lawful training data, respect for IP, and privacy) to **algorithmic process supervision** (anti-discrimination, algorithm filing) and **terminal service standards** (content labeling, anti-addiction, personal information protection). A core requirement is that service providers bear dual legal responsibilities as **online information content producers** and **personal information processors**. Services with public opinion attributes or social mobilization capabilities must satisfy the algorithm filing and security assessment.

4. **Targeting Labeling: *The Measures for the Labeling of Artificial Intelligence Generated and Synthesized Content (2025).*** [10] These Measures are key supporting rules for China's AI content governance. They mandate a **dual, explicit and implicit, labeling system**: service providers must add user-perceptible, **prominent identification** to text, audio/video, and virtual scenes,

8 *Administrative Provisions on Deep Synthesis for Internet Information Services* (promulgated by the Cyberspace Admin. of China, et al., effective Jan. 10, 2023)(P.R.C.). *Hereinafter* Deep Synthesis Provisions.

9 *Interim Measures for the Management of Generative Artificial Intelligence Services* (promulgated by the Cyberspace Admin. of China, et al., effective Aug. 15, 2023) (P.R.C.). *Hereinafter* Generative AI Measures.

10 *Measures for the Labeling of Artificial Intelligence Generated and Synthesized Content* (promulgated by the Cyberspace Admin. of China, et al., effective Sept. 1, 2025) (P.R.C.). *Hereinafter* Labeling Measures.

while simultaneously embedding **file metadata** containing production elements. The core logic is to create a closed-loop accountability chain: upstream generators are responsible for **labeling,** downstream **content dissemination platforms** are responsible for **verification and notification** (distinguishing between confirmed AI, user-declared, and suspected AI content), application stores are accountable for **on-shelf review/approval,** and end-users are strictly prohibited from maliciously tampering with the identification marks. The regulation also permits users to obtain content without explicit labels, provided that the provider **retains logs for at least six months**. These measures aim to thoroughly address the social risk posed by confusion between human- and machine-generated digital content by combining technical standards and management norms.

(III) Judicial Guidance: "Lenient Entry, Strict Exit" Institutional Supply

While legislative and administrative bodies set red lines, China's judicial system is exploring a more pragmatic **"lenient entry, strict exit"** rationale to address the tension between **massive data demand** and **excessive authorization costs** associated with the legality of training data.

The Intellectual Property Court of the Supreme People's Court, in its official article titled *Legal Risks and Institutional Supply for AI Training Data,*[11] explicitly states the necessity of establishing a *sui generis* reasonable-use system for data input while maintaining strict controls over the output of content. Regarding the legality of **input data,** it proposes a comprehensive fair use system that covers intellectual property, personal information, and enterprise data, drawing on the three-step test adopted by the US and the EU. In the context of personal information, implied consent applies to non-sensitive personal information, while explicit consent is required for sensitive personal information.

This approach emphasizes strict control over **output content**, compelling enterprises to enhance their technical governance capabilities (e.g., filtering mechanisms, alignment training) rather than stifling data acquisition. This article suggests that future judicial decisions in China may prioritize the **"how the data was used"** and **"what result was generated"** over simply whether the data was scraped.

Overall, China has established a regulatory system that is **"vertically stratified, horizontally categorized, and covers the entire chain", forming** a

11 Qi Lei (亓蕾), Judge, The Supreme People's Court Intellectual Property Court, *Legal Risks and Institutional Supply for AI Training Data* (Dec. 4, 2025), *available at* https://mp.weixin.qq.com/s/x6fZcFx7DUrM_2T_EH592w.

China Solution centered on **security and control,** aiming to delineate a clear pathway for industrialization while mitigating risks.

II. The European Union

The European Union, as a global regulatory leader, was the first to introduce the **EU Artificial Intelligence Act (AI Act)**.[12] The AI Act follows the principle of **risk classification,** dividing systems into Unacceptable Risk, High Risk, Limited Risk, and Minimal Risk.[13] The Act begins by setting **red lines** (Article 5), prohibiting practices that pose unacceptable risks, such as **subliminal manipulation, social scoring, and real-time remote biometric identification in publicly accessible spaces**.[14] Violators face **fines up to €35 million or 7% of global annual turnover**.[15]

For **High-Risk AI** systems used in fields such as infrastructure, employment, and justice, enterprises must fulfill full-lifecycle compliance obligations similar to those for product certification.[16] Notably, **transparency requirements under Article 13** and the **Human-in-the-loop mechanism under Article 14** mandate the preservation of the human right to intervene in algorithmic decision-making.[17] Furthermore, Chapter V establishes coordinating rules for **General-Purpose AI Models (GPAI)**, especially those with **systemic risk**, defining classification standards and imposing documentation, information, and assessment obligations on model providers.[18]

At the data element level, the **General Data Protection Regulation (GDPR)** and the **Data Act** establish the boundaries for privacy protection and industrial data sharing.[19] At the platform level, the **Digital Services Act (DSA)** and the **Digital Markets Act (DMA)** impose pervasive supervision over algorithmic recommendation transparency and monopolistic behavior by technology giants.[20] Furthermore, the revised **Product Liability Directive (PLD)** formally incorporates AI software into the definition of product, establishing the principle of **strict liability**.[21] These regulations interlock with the AI Act to form the EU's full-lifecycle governance system for AI, covering development, operation, and compensation.

12 *Regulation (EU) 2024/1689 of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence* (EU AI Act), 2024 O.J. (L 2024/1046) 38. *Hereinafter* EU AI Act.

13 Id. tit. III

14 Id. art. 5

15 Id. art. 99

16 *See generally* EU AI Act, tit. III

17 *Id.* arts. 13-14.

18 *Id.* tit. V

19 GDPR art. 5; Data Act art. 3.

20 DSA art. 25; DMA art. 5.

21 PLD art. 1 (as revised).

III. The United States

On December 11, 2025, President Trump signed an Executive Order to establish a **minimally burdensome** national standard for artificial intelligence, rather than 50 discordant State standards. The Order argues that the current fragmented regulatory landscape increases compliance burdens, compels companies to embed ideological bias within models, and impinges on interstate commerce.[22]

The Order directs the **Department of Justice** to litigate against state AI laws that conflict with the policy and authorizes the **Department of Commerce** to suspend federal funding to states enforcing overly burdensome AI regulations. It explicitly criticizes the **Colorado AI Act**, arguing that its provisions prohibiting algorithmic discrimination effectively compel models to alter truthful outputs. Given that the **constitutionality** of the Order will face fierce legal challenges from **State Attorneys General**, state laws **remain effective** until a formal court ruling is issued.

Consequently, the primary challenge in U.S. AI compliance has shifted from the high costs of fragmented state standards to a direct conflict between federal and state rules. The federal government now not only permits companies to disregard state laws but, through procurement clauses, explicitly prohibits practices that were previously considered compliant. Companies are now trapped in a compliance double bind: measures taken to comply with California, Colorado, or EU laws—such as algorithmic bias audits and anti-discrimination impact assessments-may violate federal requirements, thereby disqualifying them from federal procurement bidding.[23]

Given the uncertainty of litigation outcomes, it is recommended that enterprises **not dismantle their existing compliance frameworks** to avoid potential retroactive enforcement by state governments. Companies should maintain a highest-common-denominator strategy when preparing for version forking: foundation model training, data governance, and safety testing should still benchmark against the EU *AI Act* and California standards. However, a **dynamic alignment architecture** should be implemented at the inference layer to address diverging compliance requirements. Additionally, although the

22 *Eliminating State Law Obstruction of National Artificial Intelligence Policy*, The White House, https://www.whitehouse.gov/presidential-actions/2025/07/preventing-woke-ai-in-the-federal-government/, Published: Dec. 11, 2025, Accessed: Dec. 16, 2025.

23 *Executive Order on Preventing Woke AI in the Federal Government*, The White House, https://www.whitehouse.gov/presidential-actions/2025/07/preventing-woke-ai-in-the-federal-government/, Published: July 23, 2025, Accessed: Dec. 16, 2025. This Order establishes rules excluding "Woke AI" from the scope of federal government procurement.

federal government is pursuing deregulation, the Federal Trade Commission's authority to prosecute fraud remains intact; therefore, it is advisable to meticulously document algorithmic decision-making processes to prepare for potential state-level legal challenges.

IV. Summary and Outlook

Facing these complex legal requirements, enterprises must adopt an approach that integrates compliance *into* development, establishing an inherent compliance system rather than attempting "development first, compliance later". First, a cross-functional AI Governance Committee should be established to coordinate the management of legal, technical, and ethical risks. Second, a **Freedom-to-Operate (FTO) search** must be conducted before product export to systematically eliminate intellectual property and other legal risks associated with the model architecture and training data. Critically, enterprises must practice **"Compliance by Design"**, building a complete compliance evidence chain from the legal basis of data collection (acquisition stage) to **bias testing** (development stage) and **labeling and traceability** (deployment stage). Simultaneously, enterprises must establish real-time user screening mechanisms to prevent unfavorable legal consequences arising from **export control and sanctions risks**, such as providing computing services to sanctioned entities.

Future core competitiveness will not be determined solely by data and computing power, but increasingly by a system's **transparency, robustness, and legal accountability**. Only under the guidance of clear and stable rules can AI truly progress steadily and successfully.

Appendix: Comparison of Core Elements in China, the EU, and US AI Regulatory Frameworks (2025)

Dimension	China	European Union	United States
Extraterritorial Scope	**Strong.** Applies to companies that provide services to individuals located in China.	**Strong.** Applies to providers placing AI systems on the EU market or whose outputs affect individuals within the EU.	**Moderate/Strong.** CA SB 53 (Frontier Model Act) applies to providers placing models on the CA market. CA SB 942 (Transparency Act)

Dimension	China	European Union	United States
			applies to AI systems accessible in California that have over 1 million monthly users.
Pre-Market Access	**Mandatory Algorithm Filing and Security Assessment:** Required for algorithm recommendation services with public opinion/mobilization capabilities, deep synthesis services, CII operators, and PII processors exceeding specified thresholds.	**Risk-based and Mandatory:** Unacceptable risk AI systems are **prohibited**. **Mandatory Conformity Assessment** for High-Risk AI before deployment. GPAI with **Systemic Risk** must notify the EU AI Office.	**State Mandatory Disclosure:** CA SB 53 requires large frontier AI developers to publish general safety frameworks and transparency reports detailing their risk management practices. Colorado law requires high-risk system deployers to implement risk management policies that incorporate the **NIST AI RMF**.
Global Common Key Compliance Actions	**1.Governance/Accountability:** Establish internal management and accountability frameworks; define roles/responsibilities; require staff AI literacy. **2. Development/Data Quality:** Define purpose/scope; ensure training/testing datasets meet quality and representativeness standards. **3. Evaluation/Testing:** Conduct forward-looking risk assessments and performance testing before deployment (e.g., accuracy, robustness, human rights impact). **4. Operation/Transparency:** Maintain transparency, ensure human explainability and intervention mechanisms, and provide timely incident response and reporting.		

Dimension	China	European Union	United States
Regional Key Compliance Actions	**China:** Complete Algorithm Filing, Security Assessment, and Ethics Review. **Dual explicit and implicit labeling** of AI-generated content	**EU:** Determine risk category. Establish technical documentation, instructions for use, and mechanisms for human oversight. Appoint an EU Authorized Representative.	**US:** Implement the **NIST AI RMF** framework (voluntary, but industry standard). NYC: Recruitment algorithms require **third-party audits and public disclosure**. CA SB 53: Report catastrophic risk assessment summaries.
Penalty Severity	**Personal Data:** Up to **¥50 million or 5%** of the previous year's turnover, plus potential business suspension/license revocation. Penalties for senior personnel may reach up to RMB ¥1 million, and fines for the company may reach up to ¥10 million.	**Unacceptable risk systems:** up to €35 million or 7% of global annual turnover. **High-risk systems:** up to **€15 million or 3%**. **GDPR Personal Data:** Up to **€20 million or 4%** of global turnover.	**FTC Enforcement:** The FTC may impose fines and sanctions for UDAP violations, including requiring the destruction of noncompliant algorithms. **State Fines:** CA Frontier Model violations up to **$1 million** per violation. **Federal Criminal:** TAKE IT DOWN Act imposes fines and imprisonment up to **3 years** for offenses involving minors.

The "Featured article" is not equal to legal opinions.

If you need special legal opinions, please consult our professional consultants and lawyers.

Email address : ltbj@lungtin.com Website www.lungtin.com

For more information, please contact the author of this article.

ZHOU, Ziqi

Attorney at Law

Ms. Zhou Ziqi specializes in handling legal affairs related to intellectual property rights, and has rich experience in patent invalidation, patent infringement, and technical secret infringement litigation.