# Strictest Amendment to China's Cybersecurity Law In Effect

February 26, 2026 Liza Mark, Maisy Chang

PRACTICES Privacy and Cybersecurity, China, International

On Oct. 28, 2025, the Standing Committee of the National People's Congress adopted the 2025 Amendment of the Cybersecurity Law of the People's Republic of China (hereinafter referred to as "**2025 Cybersecurity Law**" or "**the 2025 Amendment**"). The Cybersecurity Law of the People's Republic of China was first adopted on Nov. 7, 2016. After this latest revision, together with the Data Security Law of the People's Republic of China (hereinafter referred to as "**Data Security Law**", promulgated on June 10, 2021 and effective on Sept. 1, 2021) and the Personal Information Protection Law of the People's Republic of China (hereinafter referred to as "**Personal Information Protection Law**", promulgated on Aug. 20, 2021 and effective on Nov. 1, 2021), the three laws now form the core legal regulation for China's cyberspace and data governance.

The 2025 Cybersecurity Law took effect on Jan. 1, 2026. The 2025 Amendment turns out to be the strictest amendment on the regulation of Cybersecurity and also demonstrates the Chinese government's strong desire to energetically develop the artificial intelligence ("**AI**") industry.

## Key Takeaways:

- **AI Policy Support with Built-in Risk Governance:** The 2025 Amendment adds a special provision for AI, affirming China's support for the AI industry, but requiring that operators – including foreign operators – consider and deploy risk control mechanisms in the whole life-cycle for AI development.
- **Higher Fines and Broader Personal Liability:** Penalties increase significantly across violation tiers, with fines up to RMB 10 million for particularly serious violations and up to RMB 1 million for directly responsible person(s)-in-charge and other directly responsible persons. This materially increases exposure for local management of multinational entities.
- **Service Shutdown Authority as a Critical Enforcement Tool:** Regulators are authorized to order takedowns of websites or apps, creating acute operational and revenue risk; incident response and business continuity plans should account for potential service disruption orders.
- **Supply Chain Security Reviews and Lifecycle Obligations:** Critical Information Infrastructure Operators ("CIIOs") remain primary obligors for strict security reviews of procurements affecting critical infrastructure. In other words, if CIIOs are conducting business that involves critical infrastructure, then its supply chain will also be under strict security review. Network product and service providers are required to cooperate and ensure lifecycle security and compliance. Foreign vendors and cloud/managed service providers should expect more rigorous due diligence and contract requirements by the CIIOs.
- **Wider Impact Across Internet-dependent Businesses:** Expansion of these supply chain security review and lifecycle obligations substantially increases the number of parties

affected. Foreign businesses relying on internet services should proactively reassess vendor risk management, technical baselines and compliance documentation.

As compared to the 2016 original Cybersecurity Law, the 2025 Cybersecurity Law clearly shows a change in the regulatory attitude from the government and reflects the ongoing support for the development of AI industry in China. Key changes are detailed in the below four aspects:

## I. Special Provisions on Artificial Intelligence

To address the cybersecurity challenges brought by the development of new technologies such as artificial intelligence and to emphasize government support of the industry, the revised law adds special and framework regulatory provisions for AI.

Article 20, a newly added clause, clearly states: "The state supports basic theoretical research on artificial intelligence and the research and development of key technologies such as algorithms, promotes the construction of infrastructure such as training data resources and computing power, improves AI ethical norms, strengthens risk monitoring, assessment and safety supervision, and promotes the application and healthy development of artificial intelligence. The state supports innovating cybersecurity management methods and applying new technologies such as artificial intelligence to improve the level of cybersecurity protection."

This provision reflects China's regulatory philosophy of "promoting development through regulation and ensuring development through security" in the field of AI. It encourages technological innovation and emphasizes risk control. With the released direct regulation like the *Interim Measures for the Administration of Generative AI Services* (the first Administrative Regulation governing generative AI service and security management, promulgated on July 10, 2023), *Measures for Labelling AI-Generated or Composed Content* (promulgated on Dec. 25, 2025, mandating clear identification and labeling of AI-generated or composed content) and indirect laws like the Data Security Law and Personal Information Protection Law, we anticipate more laws or regulations on AI regulation will be promulgated with the rapid development of this industry.

## II. Substantially Increased Legal Penalties for Infractions

The 2025 Cybersecurity Law significantly increases the legal penalties for infractions:

- **Substantially Upgraded Fines, Expanded Responsible Persons and Death Threat**

The 2025 Amendment refines the penalty standards for different types of cybersecurity violations and significantly raises the fine in every level of violation. For serious violations that cause major cybersecurity risks, the fine is up to RMB 10 million. For directly responsible persons-in-charge and other directly responsible persons, the upper limit of fines increased from a maximum of RMB 50 thousand to RMB 1 million.

According to Article 61, for operators of critical information infrastructure who fail to fulfill cybersecurity protection obligations and cause serious consequences such as large-scale data leakage or partial loss of functionality of critical information infrastructure, the competent authorities shall impose a fine of not less than RMB 500,000 but not more than RMB 2 million and a fine of not less than RMB 50,000 but not more than RMB 200,000 on the directly responsible persons-in-charge and other directly responsible persons. If the main functions of critical information infrastructure are lost and other particularly serious consequences endangering cybersecurity are

caused, a fine of not less than RMB 2 million but not more than RMB 10 million shall be imposed, and a fine of not less than RMB 200,000 but not more than RMB 1 million shall be imposed on the directly responsible persons-in-charge and other directly responsible persons.

In addition, the 2025 Amendment also added an emergency power by authorizing the regulatory department to shut down the website or apps when the illegal acts cause severe consequences like massive data leakage. This emergency power could be the most effective deterrent for the operators by creating acute operational and revenue risk. Incident response and business continuity plans should account for potential service disruption orders.

- **The Safe Harbor Mechanism**

To encourage active preventative behavior for any misconduct under the 2025 Cybersecurity Law, the 2025 Amendment established a “safe harbor mechanism” by adding Article 73, which directly connects with the PRC Administrative Penalty Law. This mechanism plays a crucial role in balancing the rigidity of regulatory sanctions and the flexibility of compliance incentives. Specifically, Article 73 of the 2025 Cybersecurity Law stipulates that "where a violation of the provisions of this Law is committed but there are circumstances for mitigation, reduction or exemption from administrative punishment as stipulated in the Administrative Penalty Law of the People's Republic of China, the punishment shall be mitigated, reduced or exempted in accordance with the relevant provisions."

We would like to emphasize that the safe harbor under Article 73 is not an absolute "immunity umbrella". Its application is subject to the specific identification criteria stipulated in the Administrative Penalty Law and the administrative penalty discretion standards to be formulated by competent regulatory authorities. In addition, Article 73 draws a line to distinguish the entity/persons actively preventing or correcting any misconduct and those who turn a blind eye to the misconducts. Therefore, it is of crucial importance that operators involved with cybersecurity concerns start to form internal rules and keep records for implementing the risk-control measures to preserve future mitigation credits.

## III. Expanded Legal Liabilities in Supply Chain Security Review

The 2025 Amendment has further refined the regulatory framework for supply chain security in cyber and network industry. With Article 37 (obligation to conduct security reviews for procurement activities) and Article 67 (legal liability for violations), supplemented by relevant provisions in Article 24 (safety requirements for network products and services) and Article 25 (safety certification of key network equipment), the 2025 Amendment establishes a multi-tiered supply chain security review obligation system that integrates "prior review, in-process supervision and post-event accountability".

This supply chain security review obligation under the 2025 Cybersecurity Law adopts a "focused coverage plus extended supervision" model. The primary obligors are CIIOs, which are required to perform strict security review obligations for procurement activities involving critical information infrastructure, covering core network equipment, important communication products, high-performance computers and servers, cloud computing services and other products and services that have an important impact on cybersecurity. Secondly, network product and service providers are obligated to cooperate with the security review and ensure the security and compliance of their products and services throughout the life cycle.

The expansion of security obligations into the supply chain substantially increases the scope of coverage of the 2025 Cybersecurity Law. Industries based on or involving internet service need to be aware and actively correcting any potential risks in operation and future development due to the heightened obligations under the 2025 Cybersecurity Law. Cloud/managed service providers and network products vendors to CIIOs in China should expect more rigorous due diligence and contract requirements after the 2025 Amendment and need to pay more attention as to future detailed guidance on relevant regulatory requirements.

## IV. Enhancing the Regulation of Cross-Border Cybersecurity Threats

In response to the increasingly complex cross-border cybersecurity situation, the 2025 Cybersecurity Law also upgrades the punitive measures for cross-border cybersecurity threats. The revised Article 77 stipulates: "Any foreign institution, organization or individual who engages in any activity that endangers the cybersecurity of the People's Republic of China shall be held legally liable; where serious consequences are caused, the public security authority under the State Council and relevant authorities may decide to take measures such as freezing assets or other necessary sanctions against such institution, organization or individual."

This provision strengthens China's ability to respond to cross-border cybersecurity threats and provides a strong legal guarantee for safeguarding national cyber sovereignty and security. Foreign companies in China needs to be more cautious when dealing with cross-border cybersecurity issues.

In light of the 2025 Cybersecurity Law, multinational companies with operations in China should take immediate and proactive steps to reassess and strengthen their cybersecurity compliance frameworks. Foreign vendors, cloud service providers and other network product service providers should anticipate more rigorous due diligence requirements and prepare for enhanced contractual obligations when serving CIIOs under the expanded supply chain security review framework. Multinational companies deploying AI technologies in China should align their AI governance with lifecycle risk control methods and ensure compliance with both the 2025 Cybersecurity Law and related AI-specific regulations. Finally, taking advantage of the newly introduced "safe harbor mechanism" under Article 73, companies should establish robust internal compliance rules, maintain detailed records of risk-control measures and demonstrate active efforts to prevent and correct any misconduct, which may serve as a basis for future mitigation, reduction or exemption from administrative penalties. Given the increasingly complex cross-border cybersecurity regulatory environment, foreign companies in China must exercise heightened caution in handling cross-border cybersecurity matters and it is necessary to maintain close attention to legislative and regulatory developments in the relevant fields.