Key Points of China's Cybersecurity Law Amendments

By Xun Yang | Echo Li | Roy Zheng

On October 28, 2025, the Decision of the Standing Committee of the National People's Congress on Amending the Cybersecurity Law was adopted at the 18th session of the 14th Standing Committee of the National People's Congress, and the amendments will come into effect on January 1, 2026. This is the first revision of the Cybersecurity Law, the foundational legislation in cybersecurity, which has been in effect since June 1, 2017. The amendments aim to address the new requirements and challenges at the cybersecurity frontier.

This article will briefly introduce the main revisions of the Cybersecurity Law.

1. Framework for the Healthy Development of Artificial Intelligence

Artificial intelligence, as a strategic technology, is leading a new round of technological revolution and industrial transformation. In particular, with the breakthrough innovations in recent years in the fields of language large models, multimodal large models, artificial intelligence agents, and embodied intelligence, artificial intelligence is profoundly changing human production and lifestyle. However, it should also be noted that the rapid development of artificial intelligence technology has brought new opportunities and challenges to national security, cybersecurity, and social governance.

To respond to the needs of artificial intelligence governance and promote development, the revised Cybersecurity Law has added Article 20, which stipulates that "China supports the research of basic theories of artificial intelligence and the development of key technologies such as algorithms, promotes

如果您需要本出版物的中文本,
请联系:

Publication@llinkslaw. com

For more Llinks publications,
please contact:

Publication@llinkslaw.com

the construction of infrastructure for training data resources and computing power, improves ethical norms for artificial intelligence, strengthens risk monitoring, assessment, and security supervision, and promotes the application and healthy development of artificial intelligence." This article, from a broad perspective, clarifies China's strategic stance and development direction for artificial intelligence, promoting a shift in artificial intelligence governance from fragmented oversight to systematic regulation.

This addition not only proposes general principles for cybersecurity governance under the rapid development of artificial intelligence but also marks the progress in China's cybersecurity governance, from the pure emphasis on security protection to seeking security in development. It can be seen that in the future construction and enforcement of Cybersecurity Law, there will be more considerations related to artificial intelligence.

2. Enhancing the Integration of Laws

Since the promulgation of the Cybersecurity Law, China has continuously consolidated the legal foundation of cyberspace and has successively promulgated laws and regulations, such as the Data Security Law and the Personal Information Protection Law, to regulate data processing activities, ensure data security, promote the development and utilization of data, and protect personal information rights and interests. These legislations have further detailed the specific requirements for data processing and personal information protection (such as cross-border data transmission) and penalties, based on the foundation of the Cybersecurity Law.

To improve the alignment between the Cybersecurity Law and other laws and regulations, the revised Cybersecurity Law has added Paragraph 2 to Article 42, stipulating that “The network operators processing personal information shall comply with the provisions of this Law and other laws and administrative regulations such as the PRC’s Civil Code and the Personal Information Protection Law.” This article cites the penalties for illegal acts such as infringing personal information rights and interests and illegal cross-border data transmission to the corresponding laws and regulations, to unify legal responsibilities and strengthen the coherence and consistency of the legal system.

3. New Legal Liability for the Illegal Sale or Provision of Network Key Equipment and Cybersecurity-specific Products

The previous version of the Cybersecurity Law proposed a network key equipment security certification and security testing system in Article 23, stipulating that "The Network key equipment and cybersecurity-specific products shall be certified as qualified by qualified institutions in accordance with the mandatory requirements of relevant national standards for security certification or meet the requirements of security testing before they can be sold or provided." However, the previous version of the Cybersecurity Law did not establish the corresponding penalty clauses for this article.

In the field of cybersecurity, network key equipment and cybersecurity-specific products (such as firewalls) play an important role in ensuring the reliability and security of network operations. Since the implementation of the Cybersecurity Law, China's network key equipment security certification and security testing system has been continuously improved. In particular, in 2023, the Cyberspace Administration of China, the Ministry of Public Security, the Ministry of Industry and Information Technology, the Certification and Accreditation Administration, and other ministries successively issued the "Announcement on Adjusting the Management of Cybersecurity-specific Products" and the "Directory of Network Key Equipment and Cybersecurity-specific Products," further implementing China's network key equipment and cybersecurity-specific product certification and testing system.

This revision of the Cybersecurity Law adds the penalty clauses for the "illegal sale or provision of network key equipment and cybersecurity-specific products." Article 63 of the revised version stipulates that "In violation of Article 25 of this Law, those who sell or provide network key equipment and cybersecurity-specific products that have not been safety certified, safety tested, or have failed safety certification or do not meet the requirements of safety testing, shall be ordered by the relevant competent authorities to stop selling or providing, be given a warning, and have their illegal gains confiscated; if there are no illegal gains or the illegal gains are less than 100,000 RMB, a fine of more than 20,000 RMB but less than 100,000 RMB shall be imposed; if the illegal gains are more than 100,000 RMB, a fine of one to five times the amount of illegal gains shall be imposed; in serious cases, the relevant business may be ordered to suspend operations, be ordered to suspend business for rectification, have its relevant license revoked, or have its business license revoked. Where other laws and administrative regulations have other provisions, such provisions shall apply."

We advise companies involved in selling and providing related products to ensure their products undergo the required certification and testing. This is especially important for foreign cybersecurity equipment manufacturers or cybersecurity equipment importers in China, who should comply with certification and testing requirements to guarantee that the cybersecurity equipment listed in the directory has completed the necessary safety certification and testing before being provided or sold.

4. Improving the Cybersecurity Penalty Mechanism

The revision responds to the development of cybersecurity technology and systematically improves the chapter on legal liabilities. It broadens both the types and amounts of penalties for unlawful actions and refines the tiered penalty system. Additionally, it introduces provisions for reduced, mitigated, or waived penalties in certain cases, thereby creating a more precise and scientifically grounded legal liability framework.

(1) Refining the Penalty Mechanism for Non-Compliance with Cybersecurity Protection Obligations

Adjusting the Penalty Methods and Amounts

For example, according to Article 61 of the revised Cybersecurity Law, for network operators who fail to fulfill their network operation security protection obligations in accordance with the law, the basic penalty is changed from "a warning" to "a warning, with a fine of more than 10,000 RMB but less than 50,000 RMB." If they still refuse to correct or cause cybersecurity accidents and other consequences, the maximum and minimum limits of the fine have both been increased fivefold. For operators of critical information infrastructure, the basic penalty is changed from "a warning" to "a warning, with a fine of more than 50,000 RMB but less than 100,000 RMB." This marks the cancellation of the "first warning" principle by the revised Cybersecurity Law, and the competent authorities may directly impose fines for illegal acts.

Adding Penalty Clauses for Serious Consequences and Particularly Serious Consequences

Paragraph 3 of Article 61 of the revised Cybersecurity Law has added penalty clauses for "causing a large amount of data leakage, partial loss of function of critical information infrastructure" and "loss of main functions of critical information infrastructure and other particularly serious harm to cybersecurity consequences." The maximum fine for enterprises can be up to 10 million RMB, and the maximum fine for relevant responsible personnel can be up to 1 million RMB.

Expanding Penalties to More Individuals

Article 61 of the revised Cybersecurity Law broadens the range of individuals subject to penalties from "directly responsible managers" to include "directly responsible managers and other directly responsible personnel." This means that, besides managers, those responsible for security, technology, and other related roles may also be fined.

(2) Adding Penalty Methods for Specific Illegal Acts

For example, for network operators who fail to fulfill their real-name registration obligations (Article 64 of the revised version), who illegally conduct cybersecurity certification, monitoring, risk assessment, and illegally publish system vulnerabilities (Article 65 of the revised version), new penalties such as shutting down applications (i.e., Apps) have been added to adapt to the development of mobile Internet.

(3) Increasing the Penalty for Information Security

Article 69 of the revised Cybersecurity Law has increased the minimum and maximum limits of fines for network operators who fail to handle illegal information and added the penalty of shutting down applications.

(4) Adjusting Penalties Related to Critical Information Infrastructure

Article 67 of the revised Cybersecurity Law has adjusted the penalties for operators of critical information infrastructure who use network products or services that have not been reviewed for security or have not passed the security review, adding the provision of "ordering to correct within a time limit and eliminating the impact on national security."

(5) Adding Situations for Lighter, Mitigated, and Waived Penalties

Article 73 has been added to the revised Cybersecurity Law, stipulating that "In violation of the provisions of this Law, if there are circumstances for lighter, mitigated, or waived penalties as stipulated in the PRC's Administrative Penalty Law, penalties shall be imposed in accordance with its provisions."

(6) Expanding the Sanctions Against Foreign Entities

Article 77 of the revised Cybersecurity Law has expanded the scope of sanctions and legal liabilities against foreign entities from those "engaging in activities that endanger the security of China's critical information infrastructure" to "engaging in activities that endanger China's cybersecurity." This further expands the scope of sanctions and widens the toolbox in the field of cybersecurity.

If you would like to know more information about the subjects covered in this publication, please contact:

Xun Yang
+86 21 3135 8799
xun.yang@llinkslaw.com

SHANGHAI
19F, ONE LUJIAZUI
68 Yin Cheng Road Middle
Shanghai 200120 P.R.China
T: +86 21 3135 8666
F: +86 21 3135 8600

BEIJING
30F, Central Tower, China Overseas Plaza, 8 Guanghuadongli,
Chaoyang District
Beijing 100020 P.R.China
T: +86 10 5081 3888
F: +86 10 5081 3866

SHENZHEN
18F, China Resources Tower
2666 Keyuan South Road,
Nanshan District
Shenzhen 518063 P.R.China
T: +86 755 3391 7666
F: +86 755 3391 7668

HONG KONG
Room 3201, 32/F, Alexandra House
18 Chater Road
Central, Hong Kong
T: +852 2592 1978
F: +852 2868 0883

LONDON
1/F, 3 More London Riverside
London SE1 2RE
United Kingdom
T: +44 (0)20 3283 4337
D: +44 (0)20 3283 4323

www.llinkslaw.com

Wechat: LlinksLaw

WE LINK LOCAL LEGAL INTELLIGENCE WITH THE WORLD