***Translation***

*The following is a translation of China's* Cybersecurity Law, *as amended in October 2025. The law lays out the cybersecurity responsibilities of network service providers, app developers, and other users of computer networks, and sets fines and other civil penalties for violations. The most notable 2025 amendments to the* Cybersecurity Law, *originally passed in 2016, add language about state support for AI, in terms of using AI technology to bolster existing cybersecurity practices and to improve the security of AI programs themselves.*

**Title**
Cybersecurity Law of the People's Republic of China
中华人民共和国网络安全法

**Author**
Standing Committee of the 14th National People's Congress (第十四届全国人民代表大会常务委员会)

**Source**
National People's Congress (NPC) website, October 28, 2025.

*This translation incorporates the October 2025 amendments to the* Cybersecurity Law *into the text of the November 2016 original version of the* Cybersecurity Law.
*The original and archived Chinese source text of the 2016* Cybersecurity Law *are available online at, respectively:*
http://www.npc.gov.cn/zgrdw/npc/xinwen/2016-11/07/content_2001605.htm; *and*
https://perma.cc/7DQH-CY5Z
*The original and archived Chinese source text of the 2025 amendments are available online at, respectively:*
http://www.npc.gov.cn/npc///c2/c30834/202510/t20251028_449048.html; *and*
https://perma.cc/WS7D-884A
*U.S. $1 ≈ 6.8 Chinese Yuan Renminbi (RMB), as of April 14, 2026.*

| **Translation Date** | **Translator** | **Editor** |
|---|---|---|
| April 14, 2026 | Etcetera Language Group, Inc. | Ben Murphy, CSET Translation Manager |

# Cybersecurity Law of the People's Republic of China

**(Adopted at the 24th Meeting of the Standing Committee of the 12th National People's Congress on November 7, 2016.[1] Amended at the 18th Meeting of the Standing Committee of the 14th National People's Congress on October 28, 2025.)**

[1] Translator's note: This translation is of the amended 2025 version of the *Cybersecurity Law*. An English translation of the original 2016 version of the *Cybersecurity Law* is available online at:

## Table of Contents



## Chapter I General Provisions

**Article 1** This Law is formulated to ensure cybersecurity; safeguard cyberspace sovereignty and national security as well as the public interest; protect the lawful rights and interests of citizens, legal persons, and other organizations; and promote the healthy development of economic and social informatization (信息化).

**Article 2** This Law applies to the construction, operation, maintenance, and use of networks within the People's Republic of China,[2] as well as the supervision and administration of cybersecurity.

**Article 3** Cybersecurity work upholds the leadership of the Chinese Communist Party, implements the holistic approach to national security (总体国家安全观), does overall planning for development and security, and advances the construction of China into a cyber powerhouse.[3]

---

https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/.

[2] Translator's note: The Chinese word 境内 jìngnèi, translated throughout as "within the People's Republic of China (PRC)," literally means "inside the borders [of mainland China]." China considers Hong Kong, Macao, and Taiwan to be part of China but not to be "within the PRC."

[3] Translator's note: Alternate English translations for the Chinese term wǎngluò qiángguó (网络强国)—here translated as "cyber powerhouse"—include "cyber superpower," "network powerhouse," "network superpower," and so on. For a more thorough discussion in English of the meaning of the term wǎngluò qiángguó, see: https://www.newamerica.org/cybersecurity-initiative/digichina/blog/lexicon-wangluo-qiangguo/.

**Article 4** The state adheres to giving equal emphasis to cybersecurity and informatization development, follows the directives of active utilization, scientific development, law-based management, and ensuring security; advances the construction of network infrastructure and interconnectivity; encourages innovation and application of network technologies; supports the cultivation of cybersecurity talent; establishes and improves the cybersecurity assurance system; and enhances cybersecurity protection capabilities.

**Article 5** The state formulates and continuously improves the national cybersecurity strategy, clarifies the basic requirements and primary objectives for safeguarding cybersecurity, and proposes cybersecurity policies, work tasks, and measures for key areas.

**Article 6** The state adopts measures to monitor, prevent, and address cybersecurity risks and threats originating from within and outside[4] the People's Republic of China; protects critical information infrastructure from attacks, intrusions, interference, and destruction; punishes cyber-related illegal and criminal activities in accordance with the law; and safeguards cyberspace security and order.

**Article 7** The state advocates honest, trustworthy, healthy, and civilized online conduct; promotes the dissemination of the socialist core values concept (社会主义核心价值观); adopts measures to raise cybersecurity awareness and capacity across society as a whole; and fosters a favorable environment in which the whole society jointly participates in promoting cybersecurity.

**Article 8** The state actively conducts international exchanges and cooperation in areas including cyberspace governance, research and development of network technologies and standards setting, and combating cyber-related illegal and criminal activities; promotes the building of a peaceful, secure, open, and cooperative cyberspace; and establishes a multilateral, democratic, and transparent cyberspace governance system.

**Article 9** The national cyberspace affairs (网信) departments are responsible for overall coordination of cybersecurity work and related supervision and administration. The State Council main oversight departments (主管部门) for telecommunications, public security departments, and other relevant agencies, in accordance with this Law and relevant laws and administrative regulations, are responsible for cybersecurity protection as well as supervision and administration

[4] Translator's note: The Chinese word 境外 jìngwài, translated throughout as "outside the People's Republic of China," literally means "outside the borders [of mainland China]." The term encompasses not just foreign countries but also Hong Kong, Macao, and Taiwan.

within the scope of their respective duties.

The cybersecurity protection, supervision, and administration responsibilities of the relevant departments of local people's governments at or above the county level shall be determined in accordance with relevant national provisions.

**Article 10** When conducting business and service activities, network operators must comply with laws and administrative regulations; respect social morality; observe business ethics; be honest and trustworthy; fulfill cybersecurity protection obligations; accept supervision by the government and society; and shoulder their responsibility to society.

**Article 11** Those who construct or operate networks, or provide services through networks, shall, in accordance with the provisions of laws and administrative regulations and the mandatory requirements of national standards, adopt technical measures and other necessary measures to ensure cybersecurity and stable operation, effectively respond to cybersecurity incidents, prevent cyber-related illegal and criminal activities, and safeguard the integrity, secrecy, and availability of network data.

**Article 12** Network-related industry organizations shall, in accordance with their charters, strengthen industry self-discipline, formulate codes of conduct for cybersecurity, guide their members in strengthening cybersecurity protection, raise the level of cybersecurity protection, and promote the healthy development of the industry.

**Article 13** The state protects the right of citizens, legal persons, and other organizations to use networks in accordance with law; promotes the widespread availability of network access; enhances the level of network services; provides society with safe and convenient network services; and ensures the lawful, orderly, and free flow of network information.

Any individual or organization using networks shall abide by the Constitution and laws, observe public order, and respect social morality; shall not endanger cybersecurity; and shall not use networks to engage in activities that endanger the nation's security, reputation, or interests, including inciting subversion of state power or overthrow of the socialist system, inciting separatism or damaging national unity, advocating terrorism or extremism, advocating ethnic hatred or ethnic discrimination, disseminating information involving violence, obscenity, or pornography, fabricating or disseminating false information to disrupt economic order or social order, or infringing upon the reputation, privacy, intellectual property rights, or other lawful rights and interests of others.

**Article 14** The state supports the research, development, and utilization of

network products and services conducive to the healthy growth of minors, punishes in accordance with law activities that use networks to harm the physical or mental health of minors, and provides minors with a safe and healthy online environment.

**Article 15** Any individual or organization has the right to report acts endangering cybersecurity to cyberspace affairs, telecommunications, public security, and other relevant departments. Departments receiving such reports shall promptly handle them in accordance with law. Where the matter does not fall within their responsibilities, they shall promptly transfer it to the department with the authority to handle it.

Relevant departments shall keep secret relevant information on the whistleblower (举报人) and protect the whistleblower's lawful rights and interests.

## Chapter II Support and Promotion of Cybersecurity

**Article 16** The state establishes and improves the cybersecurity standards system. The State Council main oversight department for standardization administration and other relevant departments of the State Council shall, in accordance with their respective responsibilities, organize the formulation and timely revision of national standards and industry standards relating to cybersecurity management as well as the security of network products, services, and operations.

The state supports enterprises, research institutions, institutions of higher learning, and network-related industry organizations in participating in the formulation of national cybersecurity standards and industry standards.

**Article 17** The State Council and the people's governments of provinces, autonomous regions, and province-level municipalities shall engage in overall planning; increase investment, support key cybersecurity technology industries and projects; support the research, development, and application of cybersecurity technologies; promote secure and trustworthy network products and services; protect intellectual property rights for network technologies; and support enterprises, research institutions, and institutions of higher learning in participating in national cybersecurity technology innovation projects.

**Article 18** The state advances the construction of a society-oriented[5] cybersecurity services system and encourages relevant enterprises and institutions to carry out cybersecurity certification, testing, risk assessment, and other security

[5] Translator's note: The phrase "society-oriented" (社会化) typically refers to public services that are at least partially provided by non-government entities, such as corporations or community groups.

services.

**Article 19** The state encourages the development of technologies for the protection and utilization of network data, promotes the opening up (开放) of public data resources, and advances technological innovation and economic and social development.

**Article 20** The state supports basic theoretical research in artificial intelligence (AI) and the research and development of key technologies such as algorithms; advances the construction of infrastructure such as training data resources and computing power (compute); improves AI ethical norms; strengthens risk monitoring and assessment as well as security supervision; and promotes the application and healthy development of AI.

The state supports innovative approaches to cybersecurity management and the application of AI and other new technologies to enhance cybersecurity protection capabilities.

**Article 21** People's governments at all levels and their relevant departments shall organize the regular launching of cybersecurity propaganda and education activities, and guide and urge relevant work units (单位) to carry out cybersecurity propaganda and education work.

Mass media shall conduct targeted cybersecurity propaganda and education activities directed toward society.

**Article 22** The state provides support to enterprises, institutions of higher learning, vocational schools, and other education and training institutions in conducting cybersecurity-related education and training, adopts multiple approaches to cultivate cybersecurity talent, and promotes exchanges among cybersecurity talent.

## Chapter III Network Operations Security

### Section 1 General Regulations

**Article 23** The state implements the ranked cybersecurity protection system.[6]

[6] Translator's note: China's "ranked cybersecurity protection system" (网络安全等级保护制度) divides cybersecurity threats, and the corresponding degree of cyber defense needed against these attacks, into five ranks or levels. Rank 1 attacks, if successful, harm the rights and interests of individuals and organizations, but do not threaten national security, social order, or the public interest. Successful rank 2 attacks cause severe or exceptionally severe harm to the rights and interests of individuals and organizations, or threaten social order and the public interest, but do not threaten national security. Successful rank 3 attacks severely threaten social order and the public interest, or threaten national

Network operators shall, in accordance with the requirements of the ranked cybersecurity protection system, perform the following cybersecurity protection obligations to ensure that networks are protected from interference, damage, or unauthorized access, and to prevent network data from being leaked, stolen, or tampered with:

(a) Establish internal cybersecurity management systems and operating procedures, designate persons responsible for cybersecurity, and implement cybersecurity protection responsibility systems;

(b) Adopt technical measures to prevent computer viruses and cyberattacks, network intrusions, and other acts endangering cybersecurity;

(c) Adopt technical measures to monitor and record network operational status and cybersecurity incidents, and retain relevant network logs for no fewer than six months in accordance with regulations;

(d) Adopt measures such as data categorization, backups of important data, and encryption;

(e) Other obligations prescribed by laws and administrative regulations.

**Article 24** Network products and services shall comply with the mandatory requirements of relevant national standards. Providers of network products and services shall not install malicious programs; when they discover that their network products or services contain security defects, vulnerabilities, or other risks, they shall immediately take remedial measures and, in accordance with regulations, promptly inform users and report the issue to the relevant main oversight departments.

Providers of network products and services shall continuously provide security maintenance for their products and services and shall not terminate the provision of security maintenance within the prescribed period or the period agreed upon by the parties.

Where network products or services have functions for collecting user information, their providers shall clearly inform users and obtain their consent; where personal information of users is involved, they shall also comply with this Law and relevant laws and administrative regulations concerning personal information protection.

**Article 25** Key network equipment and specialized cybersecurity products

---

security. Successful rank 4 attacks threaten social order and the public interest to an exceptionally severe degree, or severely threaten national security. Successful rank 5 attacks threaten national security to an exceptionally severe degree.

shall, in accordance with the mandatory requirements of relevant national standards, undergo security certification by qualified institutions or pass security testing before they may be sold or provided. National cyberspace affairs departments, together with relevant departments of the State Council, shall formulate and publish catalogues of key network equipment and specialized cybersecurity products, and promote mutual recognition of security certification and security testing results to avoid repetitive certification and testing.

**Article 26** Where network operators handle network access for users and provide domain name registration services, handle network access procedures for landline telephones, mobile phones, and similar services, or provide users with services such as information publication or instant messaging, they shall, when concluding agreements with users or confirming the provision of services, require users to provide their true identity information. Where users do not provide true identity information, network operators shall not provide the relevant services.

The state implements a trusted online identity strategy (网络可信身份战略), supports the research and development of secure and convenient electronic identity authentication technologies, and promotes mutual recognition among different electronic identity authentication systems.

**Article 27** Network operators shall formulate emergency response plans for cybersecurity incidents and promptly address security risks such as system vulnerabilities, computer viruses, cyberattacks, and network intrusions. When incidents endangering cybersecurity occur, they shall immediately activate emergency response plans, adopt corresponding remedial measures, and report the matter to the relevant main oversight departments in accordance with regulations.

**Article 28** Entities conducting cybersecurity certification, testing, risk assessment, and other such activities, or releasing to the public cybersecurity information about matters such as system vulnerabilities, computer viruses, cyberattacks, or network intrusions, shall comply with relevant national regulations.

**Article 29** No individual or organization shall engage in activities endangering cybersecurity such as illegally intruding into others' networks, interfering with the normal functioning of others' networks, or stealing network data; shall not provide programs or tools specifically used to carry out activities endangering cybersecurity, such as network intrusion, interference with normal network functioning or protective measures, or theft of network data; and, where they know that others are engaging in activities endangering cybersecurity, shall not provide technical support, advertising promotion, payment settlement, or other assistance.

**Article 30** Network operators shall provide technical support and assistance to public security agencies and national security agencies for activities carried out in accordance with law to safeguard national security and investigate crimes.

**Article 31** The state supports cooperation among network operators in areas such as the collection, analysis, and notification of cybersecurity information and emergency response, to enhance network operators' security assurance capabilities.

Relevant industry organizations shall establish and improve cybersecurity protection norms and collaboration mechanisms within their respective industries, strengthen analysis and assessment of cybersecurity risks, regularly issue risk alerts to their members, and support and assist members in responding to cybersecurity risks.

**Article 32** Information obtained by cyberspace affairs departments and relevant departments in the course of performing cybersecurity protection responsibilities shall be used solely for the needs of safeguarding cybersecurity and shall not be used for any other purposes.

### Section 2 Operations Security for Critical Information Infrastructure

**Article 33** On the basis of the ranked cybersecurity protection system, the state implements prioritized protection for critical information infrastructure in important industries and fields such as public telecommunications and information services, energy, transportation, water conservancy, finance, public services, and e-government, as well as other critical information infrastructure that, in the event of damage, loss of functionality, or data leakage, may severely endanger national security, China's ruling stratagem (国计), the people's livelihoods (民生), or the public interest. The specific scope of critical information infrastructure and the measures for its security protection shall be formulated by the State Council.

The state encourages network operators other than operators of critical information infrastructure to voluntarily participate in the critical information infrastructure protection system.

**Article 34** In accordance with the division of responsibilities prescribed by the State Council, departments responsible for the security protection of critical information infrastructure shall separately formulate and organize the implementation of critical information infrastructure security plans for their respective industries and fields, and guide and supervise security protection work for the operation of critical information infrastructure.

**Article 35** The construction of critical information infrastructure shall ensure that it possesses performance capable of supporting stable and continuous operations,

and shall ensure that security technical measures are planned, constructed, and put into use simultaneously.

**Article 36** In addition to the provisions of Article 21 of this Law, operators of critical information infrastructure shall also perform the following cybersecurity protection obligations:

(a) Establish specialized security management bodies, designate persons responsible for security management, and conduct security background checks on such persons and on other personnel holding critical positions;

(b) Regularly conduct cybersecurity education, technical training, and skills assessments for personnel;

(c) Carry out disaster recovery backups for important systems and databases;

(d) Formulate emergency response plans for cybersecurity incidents and conduct regular drills;

(e) Other obligations prescribed by laws and administrative regulations.

**Article 37** Where operators of critical information infrastructure procure network products or services that may affect national security, they shall undergo a national security review organized by the national cyberspace affairs departments together with relevant departments of the State Council.

**Article 38** Where operators of critical information infrastructure procure network products or services, they shall, in accordance with regulations, conclude security and secrecy protection (保密) agreements with the providers, clearly specifying security and secrecy protection obligations and responsibilities.

**Article 39** Personal information and important data collected or generated by operators of critical information infrastructure during operations within the People's Republic of China shall be stored within the PRC. Where it is truly necessary to provide such data outside the PRC due to business needs, a security assessment shall be conducted in accordance with the measures formulated by the national cyberspace affairs departments together with relevant departments of the State Council; where laws or administrative regulations provide otherwise, such provisions shall apply.

**Article 40** Operators of critical information infrastructure shall, either independently or by entrusting the work to cybersecurity service institutions, conduct at least one testing and assessment of the security of their networks and potential risks per year, and shall submit the testing and assessment results and improvement measures to the departments responsible for the security protection of critical information infrastructure.

**Article 41** The national cyberspace affairs departments shall coordinate with relevant departments to adopt the following measures for the security protection of critical information infrastructure:

(a) Conduct spot checks and testing of security risks relating to critical information infrastructure, propose improvement measures, and, where necessary, entrust cybersecurity service institutions to conduct testing and assessment of existing network security risks;

(b) Regularly organize cybersecurity emergency response drills for operators of critical information infrastructure to enhance their capacity to respond to cybersecurity incidents and their ability to coordinate and cooperate;

(c) Promote the sharing of cybersecurity information among relevant departments, operators of critical information infrastructure, and relevant research institutions and cybersecurity service institutions;

(d) Provide technical support and assistance for emergency response to cybersecurity incidents and the restoration of network functions.

## Chapter IV Network Information Security

**Article 42** Network operators shall strictly protect the secrecy of the user information they collect and shall establish and improve user information protection systems.

Where network operators process personal information, they shall comply with the provisions of this Law and relevant laws and administrative regulations, including the *Civil Code of the People's Republic of China* and the *Personal Information Protection Law of the People's Republic of China*.[7]

**Article 43** Where network operators collect or use personal information, they shall follow the principles of lawfulness, legitimacy, and necessity; publicly disclose rules for the collection and use of personal information; clearly indicate the purposes, methods, and scope of said collection and use; and obtain the consent of the individuals concerned.

Network operators shall not collect personal information unrelated to the services they provide; shall not collect or use personal information in violation of the provisions of laws or administrative regulations or the agreements between the parties; and shall process the personal information they retain in accordance with the provisions of laws

[7] Translator's note: An archived version of China's official English translation of the *Personal Information Protection Law* is available online at: https://perma.cc/6E6E-HNMY.

and administrative regulations and their agreements with users.

**Article 44** Network operators shall not disclose, tamper with, or damage the personal information they collect; without the consent of the individuals concerned, they shall not provide personal information to others, except where such information has been processed so that it cannot be used to identify specific individuals and such that personally identifiable information cannot be restored from it.

Network operators shall adopt technical measures and other necessary measures to ensure the security of the personal information they collect and to prevent information leakage, damage, or loss. Where personal information leakage, damage, or loss occurs or may have occurred, they shall immediately adopt remedial measures and, in accordance with regulations, promptly inform users and report to the relevant main oversight departments.

**Article 45** Where individuals discover that a network operator has collected or used their personal information in violation of the provisions of laws or administrative regulations or the agreement between the parties, they have the right to request that the network operator delete their personal information; where individuals discover that the personal information collected or stored by a network operator is inaccurate, they have the right to request that the network operator make corrections. Network operators shall take measures to delete or correct such information.

**Article 46** No individual or organization shall steal personal information or obtain it by other illegal means, nor shall they illegally sell personal information or illegally provide it to others.

**Article 47** Departments that, in accordance with law, bear responsibilities for cybersecurity supervision and administration, and their staff members, shall strictly protect the secrecy of any personal information, private information, or trade secrets that they become aware of in the course of performing their duties, and shall not disclose, sell, or illegally provide such information to others.

**Article 48** Every individual or organization shall be responsible for their conduct in using networks and shall not establish websites or communication groups for the purpose of carrying out fraud, teaching criminal methods, or producing or selling prohibited or controlled items, or other illegal or criminal activities; nor shall they use networks to publish information relating to the carrying out of fraud, the production or sale of prohibited or controlled items, or other illegal or criminal activities.

**Article 49** Network operators shall strengthen the management of information published by their users. When they discover information that laws or administrative

regulations prohibit from being published or transmitted, they shall immediately stop the transmission of such information, adopt measures such as deletion to dispose of it, prevent the information from spreading, preserve relevant records, and report the matter to the relevant main oversight departments.

**Article 50** Electronic information sent, and application software provided, by any individual or organization shall not contain malicious programs and shall not contain information that laws or administrative regulations prohibit from being published or transmitted.

Providers of electronic information transmission services and providers of application software download services shall perform security management obligations. Where they know that their users have engaged in the acts specified in the preceding paragraph, they shall stop providing services, adopt measures such as deletion to dispose of the information, preserve relevant records, and report the matter to the relevant main oversight departments.

**Article 51** Network operators shall establish mechanisms for complaints and reports concerning network information security, publicize information such as complaint and reporting channels, and promptly accept and handle complaints and reports related to network information security.

Network operators shall cooperate with supervision and inspections lawfully carried out by cyberspace affairs departments and relevant departments.

**Article 52** The national cyberspace affairs departments and relevant departments shall, in accordance with law, perform network information security supervision and administration responsibilities. Where they discover information that laws or administrative regulations prohibit from being released or transmitted, they shall require network operators to stop transmission, adopt measures such as deletion to dispose of the information, and preserve relevant records; where such information originates from outside the People's Republic of China, they shall notify relevant institutions to adopt technical measures and other necessary measures to block its dissemination.

## Chapter V Monitoring, Early Warning, and Emergency Response

**Article 53** The state establishes systems for cybersecurity monitoring and early warning and for information notification. The national cyberspace affairs departments shall coordinate with relevant departments to strengthen cybersecurity information collection, analysis, and notification work, and shall, in accordance with regulations, uniformly release cybersecurity monitoring and early-warning information.

**Article 54** Departments responsible for the security protection of critical information infrastructure shall establish and improve cybersecurity monitoring, early-warning, and information notification systems for their respective industries and fields, and shall, in accordance with regulations, submit cybersecurity monitoring and early-warning information.

**Article 55** The national cyberspace affairs departments shall coordinate with relevant departments to establish and improve cybersecurity risk assessment and emergency response mechanisms, formulate emergency response plans for cybersecurity incidents, and regularly organize drills.

Departments responsible for the security protection of critical information infrastructure shall formulate cybersecurity incident emergency response plans for their respective industries and fields and regularly organize drills.

Cybersecurity incident emergency response plans shall grade cybersecurity incidents based on factors such as the degree of harm after an incident occurs and the scope of impact, and shall specify corresponding emergency response measures.

**Article 56** When the risk of cybersecurity incidents increases, the relevant departments of people's governments at or above the provincial level shall, in accordance with the prescribed authorities and procedures and based on the characteristics of the cybersecurity risks and the potential harm they may cause, adopt the following measures:

(a) Require relevant departments, institutions, and personnel to promptly collect and report relevant information, and strengthen monitoring of cybersecurity risks;

(b) Organize relevant departments, institutions, and professional personnel to analyze and assess cybersecurity risk information, and to predict the likelihood of an incident occurring, the scope of impact, and the degree of harm;

(c) Issue cybersecurity risk warnings to the public and announce measures to avoid or mitigate harm.

**Article 57** When a cybersecurity incident occurs, emergency response plans for cybersecurity incidents shall be immediately activated; the incident shall be investigated and assessed; network operators shall be required to adopt technical measures and other necessary measures to eliminate hidden dangers to security and prevent the expansion of harm; and warning information relevant to the public shall be promptly released.

**Article 58** Where the relevant departments of people's governments at or

above the provincial level, in the course of performing cybersecurity supervision and administration responsibilities, discover that a network poses relatively significant security risks or that a security incident has occurred, they may, in accordance with the prescribed authorities and procedures, conduct interviews with the legal representative or principal person in charge of the network operator. Network operators shall take measures in accordance with the requirements, carry out rectification, and eliminate hidden dangers.

**Article 59** Where sudden public security incidents (突发事件) or production safety accidents occur as a result of cybersecurity incidents, they shall be handled in accordance with the provisions of relevant laws and administrative regulations, including the *Sudden Public Security Incident Response Law of the People's Republic of China* (中华人民共和国突发事件应对法) and the *Law of the People's Republic of China on Work Safety*.

**Article 60** Where necessary to safeguard national security and social and public order, or to address major sudden societal security incidents, and upon decision or approval by the State Council, temporary measures such as restrictions on network communications may be adopted in specified regions.

## Chapter VI Legal Liability

**Article 61** Where network operators fail to perform the cybersecurity protection obligations prescribed in Articles 23 and 27 of this Law, the relevant main oversight departments shall order rectification, issue a warning, and may impose a fine of Chinese Yuan Renminbi (RMB) 10,000–50,000; where rectification is refused or where consequences such as harm to cybersecurity are caused, a fine of RMB 50,000–500,000 shall be imposed, and a fine of RMB 10,000–100,000 shall be imposed on the directly responsible persons in charge and other directly responsible personnel.

Where operators of critical information infrastructure fail to perform the cybersecurity protection obligations prescribed in Articles 35, 36, 38, and 40 of this Law, the relevant main oversight departments shall order rectification, issue a warning, and may impose a fine of RMB 50,000–100,000; where rectification is refused or where consequences such as harm to cybersecurity are caused, a fine of RMB 100,000–1,000,000 shall be imposed, and a fine of RMB 10,000–100,000 shall be imposed on the directly responsible persons in charge and other directly responsible personnel.

Where the acts described in the preceding two paragraphs result in severe consequences endangering cybersecurity, such as large-scale data leakage or partial

loss of functionality of critical information infrastructure, the relevant main oversight departments shall impose a fine of RMB 500,000–2,000,000, and a fine of RMB 50,000–200,000 shall be imposed on the directly responsible persons in charge and other directly responsible personnel; where such acts result in exceptionally severe consequences endangering cybersecurity, such as the loss of primary functions of critical information infrastructure, a fine of RMB 2,000,000–10,000,000 shall be imposed, and a fine of RMB 200,000–1,000,000 shall be imposed on the directly responsible persons in charge and other directly responsible personnel.

**Article 62** Where any of the following acts is committed in violation of the provisions of the first and second paragraphs of Article 24 or the first paragraph of Article 50 of this Law, the relevant main oversight departments shall order rectification and issue a warning; where rectification is refused or where consequences such as harm to cybersecurity are caused, a fine of RMB 50,000–500,000 shall be imposed, and a fine of RMB 10,000–100,000 shall be imposed on the directly responsible persons in charge:

(a) Installing malicious programs;

(b) Failing to immediately adopt remedial measures for security defects, vulnerabilities, or other risks in its products or services, or failing to promptly inform users and report to the relevant main oversight departments in accordance with regulations;

(c) Unauthorized termination of the provision of security maintenance for its products or services.

Where the acts specified in items (1) or (2) of the preceding paragraph result in the consequences specified in the third paragraph of Article 61 of this Law, penalties shall be imposed in accordance with that paragraph.

**Article 63** Where, in violation of the provisions of Article 25 of this Law, key network equipment or specialized cybersecurity products are sold or provided without having undergone security certification or security testing, or where security certification is unqualified or security testing fails to meet requirements, the relevant main oversight departments shall order cessation of sale or provision, issue a warning, and confiscate any illegal gains; where there are no illegal gains or where illegal gains are less than RMB 100,000, a fine of RMB 20,000–100,000 shall additionally be imposed; where illegal gains are RMB 100,000 or more, a fine of one to five times the amount of the illegal gains shall additionally be imposed; where the circumstances are severe, the relevant main oversight departments may also order suspension of relevant business, suspension of operations for rectification, revocation of relevant business permits, or revocation of the operating license (营业执照). Where laws or

administrative regulations provide otherwise, such provisions shall apply.

**Article 64** Where a network operator violates the provisions of the first paragraph of Article 26 of this Law by failing to require users to provide true identity information, or by providing relevant services to users who do not provide true identity information, the relevant main oversight departments shall order rectification; where rectification is refused or the circumstances are serious, a fine of RMB 50,000–500,000 shall be imposed, and the relevant main oversight departments may also order suspension of relevant business, suspension of operations for rectification, closure of websites or applications, revocation of relevant business permits, or revocation of the operating license; a fine of RMB 10,000–100,000 shall be imposed on the directly responsible persons in charge and other directly responsible personnel.

**Article 65** Where the provisions of Article 28 of this Law are violated in conducting cybersecurity certification, testing, risk assessment, or other such activities, or in releasing to the public cybersecurity information such as system vulnerabilities, computer viruses, cyberattacks, or network intrusions, the relevant main oversight departments shall order rectification and issue a warning, and may impose a fine of RMB 10,000–100,000; where rectification is refused or the circumstances are serious, a fine of RMB 100,000–1,000,000 shall be imposed, and the relevant main oversight departments may also order suspension of relevant business, suspension of operations for rectification, closure of websites or applications, revocation of relevant business permits, or revocation of the operating license; a fine of RMB 10,000–100,000 shall be imposed on the directly responsible persons in charge and other directly responsible personnel.

Where the acts described in the preceding paragraph result in the consequences specified in the third paragraph of Article 61 of this Law, penalties shall be imposed in accordance with that paragraph.

**Article 66** Where, in violation of the provisions of Article 29 of this Law, a person engages in activities endangering cybersecurity, provides programs or tools specifically used to carry out activities endangering cybersecurity, or provides technical support, advertising promotion, payment settlement, or other assistance for others to engage in activities endangering cybersecurity, and such conduct does not constitute a crime, the public security authorities shall confiscate any illegal gains and impose detention of up to five days, and may concurrently impose a fine of RMB 50,000–500,000; where the circumstances are relatively serious, detention of five to fifteen days shall be imposed, and a fine of RMB 100,000–1,000,000 may concurrently be imposed.

Where a work unit commits any of the acts specified in the preceding paragraph,

the public security authorities shall confiscate any illegal gains and impose a fine of RMB 100,000–1,000,000, and shall impose penalties on the directly responsible persons in charge and other directly responsible personnel in accordance with the provisions of the preceding paragraph.

Where people who violate the provisions of Article 29 of this Law are subject to social order (治安) management penalties, they shall be prohibited from working in cybersecurity management and key network operation positions for five years; where such persons are subject to criminal penalties, they shall be prohibited for life from working in cybersecurity management and key network operation positions.

**Article 67** Where operators of critical information infrastructure violate the provisions of Article 37 of this Law by using network products or services that have not undergone a security review or that have failed a security review, the relevant main oversight departments shall order rectification within a prescribed time limit, cessation of use, and elimination of impacts on national security, and also shall impose a fine of one to ten times the procurement amount; a fine of RMB 10,000–100,000 shall be imposed on the directly responsible persons in charge and other directly responsible personnel.

**Article 68** Where, in violation of the provisions of Article 48 of this Law, a person establishes websites or communication groups for the purpose of carrying out illegal or criminal activities, or uses networks to publish information relating to the carrying out of illegal or criminal activities, and such conduct does not constitute a crime, public security agencies shall impose detention of up to five days, and may also impose a fine of RMB 10,000–100,000; where the circumstances are relatively serious, detention of five to fifteen days shall be imposed, and a fine of RMB 50,000–500,000 may also be imposed. Websites or communication groups used to carry out illegal or criminal activities shall be closed.

Where a work unit commits any of the acts specified in the preceding paragraph, the public security authorities shall impose a fine of RMB 100,000–500,000, and shall impose penalties on the directly responsible persons in charge and other directly responsible personnel in accordance with the provisions of the preceding paragraph.

**Article 69** Where a network operator violates the provisions of Article 49 of this Law by failing to stop transmission of information that laws or administrative regulations prohibit from being published or transmitted, failing to adopt disposal measures such as deletion, failing to preserve relevant records, or failing to report to the relevant main oversight departments; or where a network operator violates the provisions of Article 52 of this Law by failing to comply with the requirements of the relevant departments to stop transmission of information that laws or administrative

regulations prohibit from being published or transmitted, failure to adopt disposal measures such as deletion, and failure to preserve relevant records, the relevant main oversight departments shall order rectification, issue a warning, and circulate a notice of criticism, and may impose a fine of RMB 50,000–500,000; where rectification is refused or the circumstances are serious, a fine of RMB 500,000–2,000,000 shall be imposed, and the relevant main oversight departments may also order suspension of relevant business, suspension of operations for rectification, closure of websites or applications, revocation of relevant business permits, or revocation of the operating license; a fine of RMB 50,000–200,000 shall be imposed on the directly responsible persons in charge and other directly responsible personnel.

Where the acts described in the preceding paragraph cause exceptionally severe impact or exceptionally severe consequences, the relevant main oversight departments shall impose a fine of RMB 2,000,000–10,000,000, order suspension of relevant business, suspension of operations for rectification, closure of websites or applications, revocation of relevant business permits, or revocation of the operating license; a fine of RMB 200,000–1,000,000 shall be imposed on the directly responsible persons in charge and other directly responsible personnel.

Where providers of electronic information transmission services or providers of application software download services fail to perform the security management obligations prescribed in the second paragraph of Article 50 of this Law, penalties shall be imposed in accordance with the provisions of the preceding two paragraphs.

**Article 70** Where there are violations of this Law, such violations shall, in accordance with the provisions of relevant laws and administrative regulations, be entered into credit records and publicly disclosed.

**Article 71** Where any of the following acts is committed, handling and penalties shall be imposed in accordance with the provisions of relevant laws and administrative regulations:

(a) Publishing or transmitting information that is prohibited from being published or transmitted under the second paragraph of Article 13 of this Law or under other laws or administrative regulations;

(b) Violating the provisions of the third paragraph of Article 24 or Articles 43 through 45 of this Law by infringing upon personal information rights and interests;

(c) Violations of the provisions of Article 39 of this Law by operators of critical information infrastructure who store personal information and important data outside the People's Republic of China, or provide personal information and

important data outside the PRC.

Where the provisions of Article 46 of this Law are violated by stealing personal information, obtaining personal information by other illegal means, illegally selling personal information, or illegally providing personal information to others, and such conduct does not constitute a crime, penalties shall be imposed by the public security agencies in accordance with the provisions of relevant laws and administrative regulations.

**Article 72** Where the operators of government networks for state agencies fail to perform the cybersecurity protection obligations prescribed by this Law, the corresponding higher-level agency, or the relevant agency, shall order rectification; disciplinary action shall be taken in accordance with law on the directly responsible persons in charge and other directly responsible personnel.

**Article 73** Where violations of this Law occur but circumstances exist that warrant a lighter, mitigated, or waived administrative penalty as provided in the *Law of the People's Republic of China on Administrative Penalties*, such lighter, mitigated, or waived administrative penalties shall be imposed in accordance with its provisions.

**Article 74** Where cyberspace affairs departments or relevant departments violate the provisions of Article 32 of this Law by using information obtained in the course of performing cybersecurity protection responsibilities for other purposes, disciplinary action shall be taken in accordance with law on the directly responsible persons in charge and other directly responsible personnel.

Where staff members of cyberspace affairs departments or relevant departments neglect their duties, abuse their power, or engage in favoritism or irregularities for personal gain (徇私舞弊), and such conduct does not constitute a crime, disciplinary action shall be taken in accordance with law.

**Article 75** Where violations of this Law cause harm to others, civil liability shall be borne in accordance with law.

Where violations of this Law constitute violations of social order management, social order management penalties shall be imposed in accordance with law; where such behavior constitutes a crime, criminal responsibility shall be pursued in accordance with law.

## Chapter VII Supplementary Provisions

**Article 76** The terminology below has the following meanings in this Law:

(a) "Network" refers to a system composed of computers or other information terminals and related equipment that, in accordance with certain rules and procedures, collects, stores, transmits, exchanges, and processes information.

(b) "Cybersecurity" refers to the capability to ensure that networks operate in a stable and reliable manner by adopting necessary measures to prevent attacks, intrusions, interference, destruction, illegal use, and accidents affecting networks, and to safeguard the integrity, secrecy, and availability of network data.

(c) "Network operator" refers to owners of networks, network managers, and providers of network services.

(d) "Network data" refers to various types of electronic data collected, stored, transmitted, processed, and generated through networks.

(e) "Personal information" refers to various types of information recorded electronically or by other means that can identify the personal identity of a natural person, either on its own or in combination with other information, including but not limited to a natural person's name, date of birth, identification number, personal biometric recognition information, address, and telephone number.

**Article 77** Where institutions, organizations, or individuals outside the People's Republic of China engage in activities that endanger the cybersecurity of the PRC, legal liability shall be pursued in accordance with law; where severe consequences are caused, the public security departments of the State Council and relevant departments may also decide to adopt measures such as freezing assets or other necessary sanctions against such institutions, organizations, or individuals.

**Article 78** With respect to the operational security protection of networks that store or process information involving state secrets, in addition to complying with this Law, compliance is also required with the provisions of laws and administrative regulations on secrecy protection.

**Article 79** The Central Military Commission shall separately regulate the security protection of military networks.

**Article 80** This Law shall enter into force on June 1, 2017.[8]

[8] Translator's note: The original 2016 *Cybersecurity Law* took effect June 1, 2017. The 2025 amended version of the law took effect January 1, 2026.