Cybersecurity Law of People's Republic of China (2025 Amendment)[1]

Authority: **Standing Committee of the National People's Congress**

Document number: No. 61

Promulgation Date: October 28, 2025

Effective Date: January 1, 2026

(Adopted at the 24th Session of the Standing Committee of the Twelfth National People's Congress on November 7, 2016, and amended in accordance with the *Decision of the Standing Committee of the Fourteenth National People's Congress on Amending the Cybersecurity Law of the People's Republic of China* adopted at the 18th Session on October 28, 2025)

Table of Contents

[1]Translated by Health Law Asia – Pharmaceutical, Medical Device, and Cosmetics Law

Chapter I: General Provisions

Article 1

In order to safeguard cyberspace security, uphold the sovereignty of cyberspace, protect national security and the public interest, safeguard the legitimate rights and interests of citizens, legal persons, and other organizations, and to promote the healthy development of informatization in the economy and society, this Law is hereby enacted.

Article 2

This Law shall apply to the construction, operation, maintenance, and use of networks within the territory of the People's Republic of China, as well as to the supervision and administration of cybersecurity.

Article 3

Cybersecurity work shall adhere to the leadership of the Communist Party of China, implement the overall national security concept, coordinate development and security, and promote the building of a strong cyber nation.

Article 4

The State shall attach equal importance to cybersecurity and informatization development, adhere to the principles of active utilization, scientific development, legal governance, and security assurance, promote the construction of network infrastructure and interoperability, encourage innovation and application of network technologies, support the cultivation of cybersecurity talent, establish and improve the cybersecurity protection system, and enhance the capacity for cybersecurity protection.

Article 5

The State shall formulate and continuously improve a cybersecurity strategy, clarify the basic requirements and primary objectives for ensuring cybersecurity, and put forward policies, tasks, and measures for key areas of cybersecurity.

Article 6

The State shall adopt measures to monitor, defend against, and respond to cybersecurity risks and threats originating both within and outside the territory of the People's Republic of China, protect critical information infrastructure from attacks, intrusions, interference, and damage, punish cybersecurity-related illegal and criminal activities in accordance with the law, and maintain the security and order of cyberspace.

Article 7

The State advocates honest, trustworthy, and civilized conduct online, promotes the dissemination of the core socialist values, adopts measures to raise the overall awareness and level of cybersecurity across society, and fosters a favorable social environment in which all members of society participate in promoting cybersecurity.

Article 8

The State shall actively engage in international exchanges and cooperation in cyberspace governance, network technology research and development, standard-setting, and combating cybercrime, promote the building of a peaceful, secure, open, and cooperative cyberspace, and establish a multilateral, democratic, and transparent network governance system.

Article 9

The State's cyberspace administration authorities are responsible for the overall coordination of cybersecurity work and related supervision and management. The competent telecommunications authorities under the State Council, the public security organs, and other relevant agencies shall, within the scope of their respective responsibilities and in accordance with this Law and other applicable laws and administrative regulations, carry out cybersecurity protection and supervision. The cybersecurity protection and supervision duties of relevant departments of local people's governments at or above the county level shall be determined in accordance with relevant national regulations.

Article 10

Network operators, in the conduct of business and service activities, shall comply with laws and administrative regulations, respect social morality, observe business ethics, act honestly and in good faith, fulfil obligations to protect cybersecurity, accept government and social supervision, and bear social responsibilities.

Article 11

Those who construct, operate networks, or provide services via networks shall, in accordance with the provisions of laws, administrative regulations, and mandatory national standards, adopt technical 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, confidentiality, and availability of network data.

Article 12

Network-related industry organizations shall, in accordance with their articles of association, strengthen industry self-discipline, formulate codes of conduct for cybersecurity, guide their members in enhancing network security protection, improve overall cybersecurity levels, and promote the healthy development of the industry.

Article 13

The State shall protect the lawful rights of citizens, legal persons, and other organizations to use networks, promote widespread network access, enhance the quality of network services, provide safe and convenient network services to society, and ensure the lawful and orderly free flow of network information.

Any individual or organization using networks shall comply with the Constitution and laws, observe public order, respect social ethics, and shall not: endanger network security; use networks to endanger national security, honor, or interests; incite subversion of state power or overthrow the socialist system; incite national division or undermine national unity; promote terrorism, extremism, ethnic hatred, or ethnic discrimination; disseminate violent or pornographic information; fabricate or spread false information that disrupts economic or social order; or infringe upon the reputation, privacy, intellectual property, or other lawful rights and interests of others.

Article 14

The State shall support the research and development of network products and services conducive to the healthy growth of minors, punish, in accordance with the law, activities that endanger the physical or mental health of minors via networks, and provide a safe and healthy network environment for minors.

Article 15

Any individual or organization shall have the right to report acts that endanger cybersecurity to the competent authorities, including the Cyberspace Administration, telecommunications authorities, or public security organs.

Authorities receiving such reports shall, in a timely manner, handle them in accordance with the law; if the matter does not fall within their jurisdiction, it shall be promptly transferred to the competent authority for handling. Relevant authorities shall keep the information of the informant confidential and safeguard the lawful rights and interests of the informant.

Chapter II: Cybersecurity Support and Promotion

Article 16

The State shall establish and improve a cybersecurity standards system. The standardization administration department of the State Council and other relevant departments of the State Council shall, within the scope of their respective duties, organize the formulation and timely revision of national standards and industry standards concerning cybersecurity management, as well as the security of network products, services, and operations.

The State supports enterprises, research institutions, institutions of higher education, and industry organizations related to cyberspace in participating in the formulation of national and industry cybersecurity standards.

Article 17

The State Council and the people's governments of provinces, autonomous regions, and municipalities directly under the Central Government shall make coordinated plans, increase investment, and support key cybersecurity technology industries and projects. They shall support the research, development, and application of cybersecurity technologies; promote secure and trustworthy network products and services; protect intellectual property rights in network technologies; and support enterprises, research institutions, and institutions of higher education in participating in national cybersecurity technology innovation projects.

Article 18

The State promotes the development of a socialized cybersecurity service system and encourages relevant enterprises and institutions to carry out cybersecurity certification, testing, risk assessment, and other security-related services.

Article 19

The State encourages the development of technologies for the protection and utilization of network data security, promotes the opening and sharing of public data resources, and advances technological innovation as well as economic and social development.

Article 20

The State supports research into the fundamental theories of artificial intelligence and the research and development of key technologies such as algorithms. It promotes the development of foundational infrastructure, including training data resources and computing power; improves ethical norms for artificial intelligence; strengthens risk monitoring, assessment, and security supervision; and promotes the application and sound development of artificial intelligence. The State supports innovative approaches to cybersecurity management and the use of new technologies, such as artificial intelligence, to enhance the level of cybersecurity protection.

Article 21

People's governments at all levels and their relevant departments shall organize the regular conduct of cybersecurity publicity and education activities, and shall guide and supervise relevant entities in carrying out cybersecurity publicity and education work. Mass media outlets shall conduct targeted cybersecurity publicity and education activities for the public.

Article 22

The State supports enterprises and institutions of higher education, vocational schools, and other education and training institutions in carrying out cybersecurity-related education and training, adopts diversified measures to cultivate cybersecurity professionals, and promotes exchanges of cybersecurity talent.

Chapter III: Network Operations Security

Section 1: General Provisions

Article 23

The State implements a cybersecurity multi-level protection scheme. Network operators shall, in accordance with the requirements of the cybersecurity multi-level protection scheme, perform the following security protection obligations to ensure that networks are protected from interference, damage, or unauthorized access, and to prevent the leakage, theft, or tampering of network data:

1-Establish internal security management systems and operating procedures, designate persons responsible for cybersecurity, and implement cybersecurity protection responsibilities;

2-Adopt technical measures to prevent computer viruses, cyberattacks, network intrusions, and other acts that endanger cybersecurity;

3-Adopt technical measures to monitor and record network operation status and cybersecurity incidents, and retain relevant network logs for not less than six months in accordance with regulations;

4-Adopt measures such as data classification, backup of important data, and encryption;

5-Other obligations as 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. Where security defects, vulnerabilities, or other risks are discovered in their network products or services, providers shall immediately take remedial measures, promptly notify users in accordance with regulations, and report to the relevant competent authorities.

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

Where network products or services have functions for collecting user information, the provider shall explicitly inform users and obtain their consent. Where personal information of users is involved, the provider shall also comply with the provisions on personal information protection under this Law and other relevant laws and administrative regulations.

Article 25

Critical network equipment and specialized network security products shall, in accordance with the mandatory requirements of relevant national standards, obtain security certification from qualified institutions or pass security testing before they may be sold or provided. The national cyberspace administration authority, in conjunction with the relevant departments of the State Council, shall formulate and publish a catalogue of critical network equipment and specialized network security products, and shall promote mutual recognition of security certification and security testing results, so as to avoid duplicate certification and testing.

Article 26

Where a network operator handles network access services, domain name registration services, procedures for fixed-line or mobile telephone network access, or provides information publishing, instant messaging, or other services to users, it shall require users to provide their true identity information when entering into an agreement with users or confirming the provision of services. Where a user fails to provide true identity information, the network operator shall not provide the relevant services.

The State shall implement a trusted digital identity strategy, support the research and development of secure and convenient electronic identity authentication technologies, and promote mutual recognition among different electronic identity authentication systems.

Article 27

Network operators shall formulate emergency response plans for cybersecurity incidents, promptly address security risks such as system vulnerabilities, computer viruses, cyberattacks, and network intrusions, and, upon the occurrence of an incident endangering network security, immediately activate the emergency response plan, adopt appropriate remedial measures, and report the incident to the relevant competent authorities in accordance with the applicable regulations.

Article 28

Entities conducting activities such as cybersecurity certification, testing, or risk assessment, or releasing to the public cybersecurity information relating to system vulnerabilities, computer viruses, cyberattacks, or network intrusions, shall comply with the relevant provisions of the State.

Article 29

No individual or organization shall engage in activities that endanger cybersecurity, including but not limited to illegally intruding into the networks of others, interfering with the normal functioning of networks, or stealing network data. No individual or organization shall provide programs or tools specifically designed for activities that endanger cybersecurity, such as network intrusion, interference with normal network functions or protective measures, or theft of network data. Where an individual or organization is aware that another party is engaging in activities that endanger cybersecurity, it shall not provide technical support, advertising or promotional services, payment or settlement services, or any other assistance thereto.

Article 30

Network operators shall provide technical support and assistance to public security authorities and national security authorities in accordance with the law in their efforts to safeguard national security and investigate criminal activities.

Article 31

The State supports cooperation among network operators in areas such as the collection, analysis, notification, and emergency response relating to cybersecurity information, so as to enhance the cybersecurity protection capabilities of network operators. Relevant industry organizations shall establish and improve cybersecurity protection standards and coordination mechanisms within their respective industries, strengthen the 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 the cyberspace administration authorities and other relevant departments in the performance of their cybersecurity protection duties shall be used solely for the purposes of safeguarding cybersecurity and shall not be used for any other purposes.

Section 2: Operational Security of Critical Information Infrastructure

Article 33

The State shall, on the basis of the cybersecurity multi-level protection scheme, implement enhanced protection for critical information infrastructure in important industries and sectors such as public communications and information services, energy, transportation, water conservancy, finance, public services, and e-government, as well as other critical information infrastructure which, if destroyed, rendered dysfunctional, or subject to data leakage, may seriously endanger national security, the national economy and people's livelihood, 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, the departments responsible for the security protection of critical information infrastructure shall separately formulate and organize the implementation of security plans for critical information infrastructure within their respective industries and fields, and shall guide and supervise the operational security protection of critical information infrastructure.

Article 35

The construction of critical information infrastructure shall ensure that such infrastructure possesses the capabilities necessary to support stable and continuous business operations, and shall ensure that security technical measures are planned, constructed, and put into use simultaneously with the infrastructure.

Article 36

In addition to the provisions of Article 23 of this Law, operators of critical information infrastructure shall also perform the following security protection obligations:

1-Establish dedicated security management bodies and designate responsible security management personnel, and conduct security background checks on such personnel and on personnel in key positions;

2-Regularly provide cybersecurity education, technical training, and skills assessments to employees;

3-Conduct disaster recovery backups for important systems and databases;

4-Formulate emergency response plans for cybersecurity incidents and conduct regular drills;

5-Fulfill other obligations as prescribed by laws and administrative regulations.

Article 37

Where the procurement of network products and services by operators of critical information infrastructure may affect national security, such procurement shall be subject to a national security review organized by the national cyberspace administration authority in conjunction with the relevant departments of the State Council.

Article 38

When procuring network products and services, operators of critical information infrastructure shall, in accordance with the relevant regulations, enter into security and confidentiality agreements with the providers, clearly specifying the security and confidentiality obligations and liabilities of the parties.

Article 39

Personal information and important data collected or generated by operators of critical information infrastructure during operations within the territory of the People's Republic of China shall be stored within the territory of the People's Republic of China. Where it is truly necessary to provide such information or data overseas due to business requirements, a security assessment shall be conducted in accordance with the measures formulated by the national cyberspace administration authority in conjunction with the relevant departments of the State Council; where laws or administrative regulations provide otherwise, such provisions shall prevail.

Article 40

Operators of critical information infrastructure shall, either independently or by engaging cybersecurity service institutions, conduct at least one inspection and assessment each year of the security of their networks and the potential risks therein, and shall submit the results of such inspection and assessment, together with improvement measures, to the relevant departments responsible for the security protection of critical information infrastructure.

Article 41

The national cyberspace administration authority shall coordinate the relevant departments in adopting the following measures for the security protection of critical information infrastructure:

1-Conduct spot inspections and testing of security risks of critical information infrastructure, propose improvement measures, and, where necessary, entrust cybersecurity service institutions to conduct inspections and assessments of existing network security risks;

2-Regularly organize cybersecurity emergency response drills for operators of critical information infrastructure, in order to enhance their capacity to respond to cybersecurity incidents and to improve coordination and cooperation;

3-Promote the sharing of cybersecurity information among relevant departments, operators of critical information infrastructure, and relevant research institutions and cybersecurity service institutions;

4-Provide technical support and assistance for emergency response to cybersecurity incidents and for the restoration of network functions.

Chapter IV: Network Information Security

Article 42

Network operators shall keep strictly confidential the user information they collect and shall establish and improve a system for the protection of user information.

When handling personal information, network operators shall comply with the provisions of this Law, the *Civil Code of the People's Republic of China*, the *Personal Information Protection Law of the People's Republic of China*, and other applicable laws and administrative regulations.

Article 43

Network operators shall, in collecting and using personal information, abide by the principles of legality, legitimacy, and necessity; shall make public the rules for collecting and using information; and shall clearly inform the data subjects of the purpose, method, and scope of the collection and use, and obtain their consent.

Network operators shall not collect personal information that is unrelated to the services they provide, shall not collect or use personal information in violation of laws, administrative regulations, or the terms agreed with the user, and shall process any personal information they retain in accordance with legal requirements and the agreements made with the user.

Article 45

Where an individual discovers that a network operator has collected or used their personal information in violation of laws, administrative regulations, or the agreements between the parties, the individual shall have the right to require the network operator to delete such personal information; where the individual discovers that the personal information collected or stored by the network operator is inaccurate, the individual shall have the right to require the network operator to correct it. Network operators shall take measures to delete or correct such information.

Article 46

No individual or organization shall steal or obtain personal information through other unlawful means, nor shall they illegally sell or illegally provide personal information to others.

Article 47

Departments and personnel who, in accordance with law, are responsible for network security supervision and management shall strictly maintain the confidentiality of personal information, privacy, and trade secrets that they become aware of in the course of performing their duties, and shall not disclose, sell, or unlawfully provide such information to others.

Article 48

All individuals and organizations shall be responsible for their conduct on the network. They shall not establish websites, communication groups, or other platforms for the purpose of committing fraud, instructing others in the commission of crimes, producing or selling prohibited or controlled items, or engaging in other illegal activities. They shall not use the network to publish information related to committing fraud, producing or selling prohibited or controlled items, or other illegal activities.

Article 49

Network operators shall strengthen the management of information posted by their users. Upon discovering information that is prohibited from being published or transmitted under laws or administrative regulations, network operators shall immediately stop the transmission of such information, take measures to remove or otherwise dispose of it, prevent its dissemination, preserve relevant records, and report the matter to the competent authorities.

Article 50

Electronic information sent and application software provided by any individual or organization shall not contain malicious programs, nor shall they include information prohibited from being published or transmitted under laws or administrative regulations.

Providers of electronic information sending services and application software download services shall fulfill their obligations for security management. If they become aware that their users engage in any of the conduct described in the preceding paragraph, they shall immediately cease providing services, take measures to remove or otherwise dispose of the content, preserve relevant records, and report the matter to the competent authorities.

Article 51

Network operators shall establish systems for complaints and reporting regarding network information security, publicize the methods for filing complaints or reports, and promptly accept and handle complaints and reports concerning network information security.

Network operators shall cooperate with supervision and inspections lawfully conducted by the Cyberspace Administration or other relevant authorities.

Article 52

The national cyberspace administration and relevant departments, in accordance with the law, shall perform supervisory and administrative duties regarding network information security. Upon discovering information whose publication or transmission is prohibited by laws or administrative regulations, they shall require network operators to cease transmission and take measures such as removal, while preserving relevant records. In the case of such information originating from outside the territory of the People's Republic of China, the relevant institutions shall be notified to adopt technical and other necessary measures to block its dissemination.

Chapter V: Monitoring, Early Warning, and Emergency Response

Article 53

The State shall establish a system for cybersecurity monitoring, early warning, and information notification. The national cyberspace administration shall coordinate relevant departments to strengthen the collection, analysis, and dissemination of cybersecurity information, and shall, in accordance with regulations, uniformly issue cybersecurity monitoring and early warning information.

Article 54

Departments responsible for the protection of critical information infrastructure shall establish and improve cybersecurity monitoring, early warning, and information notification systems within their respective industries or domains, and shall submit cybersecurity monitoring and early warning information in accordance with regulations.

Article 55

The national cyberspace administration shall coordinate relevant departments to establish and improve mechanisms for cybersecurity risk assessment and emergency response, formulate emergency response plans for cybersecurity incidents, and conduct regular drills. Departments responsible for the protection of critical information infrastructure shall formulate emergency response plans for cybersecurity incidents within their respective industries or domains, and conduct regular drills. Cybersecurity incident emergency response plans shall classify incidents based on factors such as the severity of harm and scope of impact, and shall stipulate corresponding emergency response measures.

Article 56

When the risk of a cybersecurity incident increases, the relevant departments of the people's government at or above the provincial level shall, in accordance with prescribed authority and procedures, and based on the characteristics of the cybersecurity risk and the potential harm it may cause, take the following measures:

1-Require relevant departments, institutions, and personnel to promptly collect and report pertinent information and strengthen monitoring of cybersecurity risks;

2-Organize relevant departments, institutions, and professional personnel to analyze and evaluate cybersecurity risk information, and to forecast the likelihood of incidents, the scope of impact, and the severity of harm;

3-Issue cybersecurity risk warnings to the public and publish measures to avoid or mitigate harm.

Article 57

In the event of a cybersecurity incident, the emergency response plan for cybersecurity incidents shall be immediately activated. The incident shall be investigated and assessed, and network operators shall be required to adopt technical and other necessary measures to eliminate security hazards, prevent the expansion of harm, and promptly issue warnings to the public as appropriate.

Article 58

When exercising supervisory and administrative responsibilities for cybersecurity, relevant departments of the people's government at or above the provincial level, upon discovering a network with significant security risks or upon the occurrence of a security incident, may, in accordance with prescribed authority and procedures, conduct consultations with the legal

representatives or principal responsible persons of the network operator. Network operators shall, as required, take corrective measures and eliminate potential hazards.

Article 59

In the event that a cybersecurity incident causes an emergency or a production safety accident, handling shall be carried out in accordance with the relevant provisions of the Law of the People's Republic of China on Emergency Response and the Law of the People's Republic of China on Production Safety, as well as other applicable laws and administrative regulations.

Article 60

For the purpose of safeguarding national security and public order, and addressing major sudden social security incidents, the State Council may, by decision or approval, authorize the imposition of temporary measures restricting network communications within designated areas.

Chapter VI: Legal Liability

Article 61

1-Where a network operator fails to perform the network security protection obligations prescribed in Articles 23 or 27 of this Law, the relevant competent authority shall order rectification and issue a warning. A fine of RMB 10,000 to 50,000 may be imposed; if the operator refuses to rectify or causes consequences that endanger network security, a fine of RMB 50,000 to 500,000 may be imposed. The directly responsible supervisory personnel and other directly responsible personnel may be fined RMB 10,000 to 100,000.

2-Where an operator of critical information infrastructure fails to perform the network security protection obligations prescribed in Articles 35, 36, 38, or 40 of this Law, the relevant competent authority shall order rectification and issue a warning. A fine of RMB 50,000 to 100,000 may be imposed; if the operator refuses to rectify or causes consequences that endanger network security, a fine of RMB 100,000 to 1,000,000 may be imposed. The directly responsible supervisory personnel and other directly responsible personnel may be fined RMB 10,000 to 100,000.

3-Where the acts described in the preceding two paragraphs result in serious consequences that endanger network security, such as large-scale data leakage or partial loss of functionality of critical information infrastructure, a fine of RMB 500,000 to 2,000,000 may be imposed on the operator, and the directly responsible supervisory personnel and other directly responsible personnel may be fined RMB 50,000 to 200,000. Where such acts result in particularly serious consequences, such as the loss of primary functions of critical information infrastructure, a fine of RMB 2,000,000 to 10,000,000 may be imposed on the operator, and the directly

responsible supervisory personnel and other directly responsible personnel may be fined RMB 200,000 to 1,000,000.

Article 62

Anyone who violates the provisions of Article 24, Paragraphs 1 and 2, or Article 50, Paragraph 1, of this Law and engages in any of the following acts shall be ordered by the competent authorities to make corrections and shall be given a warning; if the corrections are refused or the act causes consequences such as endangering network security, a fine of not less than RMB 50,000 but not more than RMB 500,000 shall be imposed, and the directly responsible supervisory personnel shall be fined not less than RMB 10,000 but not more than RMB 100,000:

1-Installing malicious programs;

2-Failing to immediately take remedial measures for security defects, vulnerabilities, or other risks in their products or services, or failing to timely inform users and report to the relevant competent authorities in accordance with the provisions;

3-Arbitrarily terminating the provision of security maintenance for their products or services.

Where the acts described in Items 1 and 2 of the preceding paragraph result in consequences as provided in Article 61, Paragraph 3, of this Law, they shall be punished in accordance with the provisions of that paragraph.

Article 63

Anyone who violates the provisions of Article 25 of this Law by selling or providing network critical equipment or network security-dedicated products that have not undergone security certification or testing, or whose security certification is unqualified or security testing does not meet requirements, shall be ordered by the competent authorities to cease such sales or provision, shall be given a warning, and shall have any illegal gains confiscated.

1-Where there are no illegal gains, or where such gains are less than RMB 100,000, a fine of not less than RMB 20,000 but not more than RMB 100,000 shall be imposed.

2-Where the illegal gains exceed RMB 100,000, a fine of not less than one time but not more than five times the illegal gains shall be imposed.

3-In cases of serious circumstances, the authorities may additionally order the suspension of the relevant business, business rectification, revocation of relevant business licenses, or revocation of the business license.

Where other laws or administrative regulations provide otherwise, such provisions shall prevail.

Article 64

Where a network operator violates the provisions of Article 26, Paragraph 1, of this Law by failing to require users to provide their true identity information, or by providing relevant services to users who do not provide true identity information, the competent authorities shall order corrections.

If corrections are refused or the circumstances are serious, a fine of not less than RMB 50,000 but not more than RMB 500,000 shall be imposed, and the authorities may additionally order the suspension of the relevant business, business rectification, closure of the website or application, revocation of relevant business licenses, or revocation of the business license.

The directly responsible supervisory personnel and other directly responsible persons shall be fined not less than RMB 10,000 but not more than RMB 100,000.

Article 65

Where the provisions of Article 28 of this Law are violated by conducting network security certification, testing, risk assessment, or by publicly disclosing information such as system vulnerabilities, computer viruses, network attacks, or network intrusions, the competent authorities shall order corrections, issue a warning, and may impose a fine of not less than RMB 10,000 but not more than RMB 100,000.

If corrections are refused or the circumstances are serious, a fine of not less than RMB 100,000 but not more than RMB 1,000,000 shall be imposed, and the authorities may additionally order the suspension of the relevant business, business rectification, closure of the website or application, revocation of relevant business licenses, or revocation of the business license.

The directly responsible supervisory personnel and other directly responsible persons shall be fined not less than RMB 10,000 but not more than RMB 100,000.

Where the acts described in the preceding paragraph result in consequences as provided in Article 61, Paragraph 3, of this Law, they shall be punished in accordance with the provisions of that paragraph.

Article 66

Where the provisions of Article 29 of this Law are violated by engaging in activities that endanger network security, or by providing programs or tools specifically used for activities that endanger network security, or by providing technical support, advertising promotion, payment settlement, or other assistance to others engaging in activities that endanger network security, and such conduct does not constitute a criminal offense, the public security authorities

shall confiscate any illegal gains, impose detention of up to five days, and may concurrently impose a fine of not less than RMB 50,000 but not more than RMB 500,000. Where the circumstances are relatively serious, detention of not less than five days but not more than fifteen days shall be imposed, and a fine of not less than RMB 100,000 but not more than RMB 1,000,000 may concurrently be imposed.

Where an entity commits any of the acts described in the preceding paragraph, the public security authorities shall confiscate any illegal gains and impose a fine of not less than RMB 100,000 but not more than RMB 1,000,000, and the directly responsible supervisory personnel and other directly responsible persons shall be punished in accordance with the provisions of the preceding paragraph.

Where a person violates the provisions of Article 29 of this Law and is subject to public security administrative penalties, such person shall not engage in work in network security management or key positions in network operation for a period of five years; where a person is subject to criminal punishment, such person shall be permanently prohibited from engaging in work in network security management or key positions in network operation.

Article 67

Where an operator of critical information infrastructure violates the provisions of Article 37 of this Law by using network products or services that have not undergone a security review or whose security review has not been approved, the competent authority shall order correction within a specified period, cessation of use, and elimination of any impact on national security. A fine of not less than one time but not more than ten times the procurement amount shall be imposed. The directly responsible management personnel and other directly responsible persons shall be fined not less than RMB 10,000 but not more than RMB 100,000.

Article 68

Where a person violates the provisions of Article 48 of this Law by establishing websites or communication groups for the purpose of committing illegal or criminal activities, or by using the network to disseminate information related to such activities, and the act does not constitute a crime, the public security authority shall impose administrative detention of up to five days and may impose a fine of not less than RMB 10,000 but not more than RMB 100,000. If the circumstances are serious, detention of more than five days but not exceeding fifteen days may be imposed, together with a fine of not less than RMB 50,000 but not more than RMB 500,000. The websites or communication groups used for such illegal or criminal activities shall be shut down.

Where an organization commits the acts described in the preceding paragraph, the public security authority shall impose a fine of not less than RMB 100,000 but not more than RMB 500,000, and the directly responsible management personnel and other directly responsible persons shall be punished in accordance with the preceding paragraph.

Article 69

Where a network operator violates the provisions of Article 49 of this Law by failing to stop the transmission of information prohibited from being published or transmitted by laws or administrative regulations, failing to take measures to remove such information, failing to preserve relevant records, or failing to report to the relevant competent authorities; or violates the provisions of Article 52 of this Law by failing, upon the request of the relevant authorities, to stop transmission, take removal measures, or preserve relevant records of information prohibited from being published or transmitted by laws or administrative regulations, the relevant competent authority shall order correction, issue a warning, and publicize the violation. A fine of not less than RMB 50,000 but not more than RMB 500,000 may be imposed.

If the operator refuses to correct the violation or the circumstances are serious, a fine of not less than RMB 500,000 but not more than RMB 2,000,000 may be imposed, and the authority may order the suspension of related business, rectification, closure of the website or application, or revocation of relevant business licenses or business registration. The directly responsible management personnel and other directly responsible persons shall be fined not less than RMB 50,000 but not more than RMB 200,000.

Where the acts in the preceding paragraphs cause particularly serious impact or particularly serious consequences, the competent authority shall impose a fine of not less than RMB 2,000,000 but not more than RMB 10,000,000, order the suspension of related business, rectification, closure of the website or application, or revocation of relevant business licenses or business registration, and impose a fine of not less than RMB 200,000 but not more than RMB 1,000,000 on the directly responsible management personnel and other directly responsible persons.

Electronic information sending service providers and application download service providers that fail to fulfill the security management obligations under the second paragraph of Article 50 of this Law shall be punished in accordance with the preceding two paragraphs.

Article 70

Where a network operator engages in any of the following acts in violation of this Law, the competent authorities shall order correction; if the operator refuses to correct or if the circumstances are serious, a fine of not less than RMB 50,000 and not more than RMB 500,000 shall be imposed, and the directly responsible supervisory personnel and other directly responsible persons shall be fined not less than RMB 10,000 and not more than RMB 100,000:

1-Refusing or obstructing the lawful supervision and inspection conducted by relevant authorities;

2-Refusing to provide technical support and assistance to public security organs or national security organs.

Article 71

Where any of the following acts occurs, handling and punishment shall be carried out in accordance with relevant laws and administrative regulations:

1-Publishing or transmitting information prohibited by Article 13, Paragraph 2 of this Law, or by other laws and administrative regulations;

2-Violating the provisions of Paragraph 3 of Article 24 or Articles 43 through 45 of this Law, thereby infringing upon the rights and interests of personal information;

3-Violating the provisions of Article 39 of this Law, where operators of critical information infrastructure store personal information or important data overseas, or provide personal information or important data overseas.

Where personal information is stolen, obtained through other illegal means, sold illegally, or provided illegally to others in violation of Article 46 of this Law, and the conduct does not constitute a crime, the public security authorities shall impose penalties in accordance with relevant laws and administrative regulations.

Article 72

Where an act constitutes a violation of this Law, it shall be recorded in the credit information file in accordance with relevant laws and administrative regulations and made public.

Article 73

Where an act violates the provisions of this Law, but circumstances exist that, under the *Administrative Punishment Law of the People's Republic of China*, warrant mitigation, reduction, or exemption from punishment, such mitigation, reduction, or exemption shall be applied in accordance with those provisions.

Article 74

Where operators of government affairs networks of state organs fail to fulfill the network security protection obligations prescribed by this Law, their superior organs or relevant authorities shall order correction; directly responsible supervisory personnel and other directly responsible persons shall be disciplined in accordance with law.

Article 75

Where the Cyberspace Administration or relevant authorities violate Article 32 of this Law by using information obtained in the performance of network security protection duties for other purposes, directly responsible supervisory personnel and other directly responsible persons shall be disciplined in accordance with law.

Where personnel of the Cyberspace Administration or relevant authorities are negligent in the performance of duties, abuse power, or engage in favoritism or malpractice, and the conduct does not constitute a crime, they shall be disciplined in accordance with law.

Article 76

Where a violation of this Law causes harm to others, civil liability shall be borne in accordance with law.

Where a violation of this Law constitutes a public security administration offense, public security administrative penalties shall be imposed in accordance with law; where it constitutes a crime, criminal responsibility shall be pursued in accordance with law.

Article 77

Where foreign institutions, organizations, or individuals engage in activities that endanger the cybersecurity of the People's Republic of China, legal liability shall be pursued in accordance with law; where serious consequences are caused, the public security authorities of the State Council and relevant authorities may decide to take measures such as freezing property or other necessary sanctions against such institutions, organizations, or individuals.

Chapter VII: Supplementary Provisions

Article 78

The following terms used in this Law shall have the meanings indicated:

1-Network: a system composed of computers or other information terminals and related equipment that collects, stores, transmits, exchanges, and processes information according to certain rules and procedures.

2-Cybersecurity: the ability to ensure the stable and reliable operation of a network and to safeguard the integrity, confidentiality, and availability of network data by taking necessary measures to prevent attacks, intrusions, interference, destruction, illegal use, or accidental incidents affecting the network.

3-Network operator: the owner, manager, or service provider of a network.

4-Network data: various electronic data collected, stored, transmitted, processed, or generated through a network.

5-Personal information: information recorded electronically or by other means that can identify a natural person either alone or in combination with other information, including but not limited to a person's name, date of birth, identification number, biometric information, address, telephone number, and other similar data.

Article 79

The operational security protection of networks involving state secrets, in addition to complying with this Law, shall also comply with the provisions of laws and administrative regulations concerning confidentiality.

Article 80

The security protection of military networks shall be separately prescribed by the Central Military Commission.

Article 81

[Omitted]