Cybersecurity Law of the People's Republic of China

(The Standing Committee of the Twelfth National People's Congress, November 7, 2016)

The Committee adopted the resolution at its 24th meeting on October 28, 2025.

The 18th meeting of the Standing Committee of the 14th National People's Congress on the "Regarding

(Amended by the Decision to Amend the Cybersecurity Law of the People's Republic of China)

Table of contents

Chapter 1 General Provisions

Chapter Two: Cybersecurity Support and Promotion

Chapter 3 Network Operation Security

Section 1 General Provisions

Section 2 Operational Security of Critical Information Infrastructure

Chapter 4 Network Information Security

Chapter 5 Monitoring, Early Warning and Emergency Response

Chapter Six Legal Liability

Chapter Seven Supplementary Provisions

Chapter 1 General Provisions

Article 1. In order to safeguard cybersecurity and protect cyberspace sovereignty and national security,

To protect the public interest, safeguard the legitimate rights and interests of citizens, legal persons and other organizations, and promote economic development.

This law is formulated to promote the healthy development of information technology in the economy and society.

Article 2. The construction, operation, maintenance, and use of the network within the territory of the People's Republic of China.

This law applies to the supervision and management of networks and network security.

Article 3 Cybersecurity work adheres to the leadership of the Communist Party of China and implements the overall national strategy.

A national security perspective, balancing development and security, and advancing the construction of a cyber power.

Article 4 The State adheres to the principle of giving equal importance to cybersecurity and informatization development, and follows the principle of actively benefiting the people.

Advance network infrastructure development based on the principles of scientific development, law-based management, and ensuring security.

Construction and interconnection, encouragement of network technology innovation and application, and support for the cultivation of cybersecurity talent.

Talent, establishing and improving the cybersecurity protection system, and enhancing cybersecurity protection capabilities.

Article 5 The State formulates and continuously improves its cybersecurity strategy, and clearly defines the responsibilities for protecting the network.

The document outlines the basic requirements and main objectives of cybersecurity, and proposes cybersecurity policies and work plans for key areas.

Tasks and measures.

Article 6 The State shall take measures to monitor, defend against, and deal with threats originating from the People's Republic of China

Cybersecurity risks and threats both within and outside the Republic, protecting critical information infrastructure from harm.

To combat attacks, intrusions, interference, and sabotage, and to punish cybercrimes in accordance with the law, we must safeguard [the rights and interests of cybersecurity].

Cyberspace security and order.

Article 7 The State advocates honest, trustworthy, healthy, and civilized online behavior and promotes the dissemination of...

Promote core socialist values and take measures to raise public awareness of cybersecurity.

This will create a favorable environment for the whole society to participate in and promote cybersecurity.

Article 8 The State actively engages in cyberspace governance, network technology research and development, and standards.

To promote international exchange and cooperation in areas such as formulating and combating cybercrime, and to advance the building of a community with a shared future for mankind.

A peaceful, secure, open, and cooperative cyberspace; establishing a multilateral, democratic, and transparent cyberspace.

Network governance system.

Article 9 The State Cyberspace Administration is responsible for coordinating cybersecurity work and related matters.

Supervision and management. The State Council's telecommunications regulatory authority, public security department, and other relevant authorities.

In accordance with this law and relevant laws and administrative regulations, each party shall be responsible within its respective scope of duties.

Cybersecurity protection and supervision.

Cybersecurity protection and supervision by relevant departments of local people's governments at or above the county level

The responsibilities are determined in accordance with relevant national regulations.

Article 10 Network operators must comply with laws and regulations when conducting business and service activities.

Administrative regulations, respect for social morality, adherence to business ethics, honesty and trustworthiness, and fulfillment of network obligations.

They have a duty to ensure safety and protection, accept supervision from the government and society, and assume social responsibility.

Article 11 The construction, operation, or provision of services through the network shall be carried out in accordance with

In accordance with the provisions of laws, administrative regulations, and the mandatory requirements of national standards, technical measures shall be adopted.

Implement and take other necessary measures to ensure network security and stable operation, and effectively respond to network security threats.

The entire process involves preventing cybercrime and safeguarding the integrity and confidentiality of network data.

Sex and availability.

Article 12. Network-related industry organizations shall, in accordance with their charters, strengthen industry self-regulation and formulate...

Establish cybersecurity code of conduct to guide members in strengthening cybersecurity protection and improving cybersecurity awareness.

Achieving comprehensive protection and promoting the healthy development of the industry.

Article 13 The State protects the lawful use of the Internet by citizens, legal persons and other organizations.

Rights, promoting universal internet access, improving network service levels, and providing a safe and secure society.

Convenient network services ensure the lawful, orderly, and free flow of network information.

Any individual or organization using the internet must abide by the constitution and laws, and observe public order.

Respect social morality, do not endanger cybersecurity, and do not use the internet to engage in activities that harm the country.

Security, honor, and interests; inciting subversion of state power and overthrow of the socialist system;

Actions that split the country, undermine national unity, promote terrorism and extremism, and advocate democracy

Promoting ethnic hatred and discrimination, spreading violent and pornographic information, and fabricating and disseminating false information.

Information that disrupts economic and social order, or infringes upon the reputation, privacy, or knowledge of others.

Activities related to property rights and other legitimate rights and interests.

Article 14 The State supports research and development that is beneficial to the healthy growth of minors.

Internet products and services, punishing those who use the internet to harm the physical and mental health of minors in accordance with the law.

The activities aim to provide a safe and healthy online environment for minors.

Article 15 Any individual or organization has the right to report acts that endanger cybersecurity.

Reports can be made to departments such as the Cyberspace Administration, telecommunications authorities, and public security bureaus. The receiving department should promptly take action in accordance with the law.

If a matter is not within the responsibilities of this department, it should be promptly transferred to the department with the authority to handle it.

Relevant departments should keep the information of whistleblowers confidential and protect their rights.

Legitimate rights and interests.

Chapter Two: Cybersecurity Support and Promotion

Article 16 The State shall establish and improve a cybersecurity standards system. (State Council Standards)

The relevant administrative departments and other relevant departments of the State Council shall, in accordance with their respective responsibilities, organize and formulate...

Formulate and revise relevant provisions on network security management and the security of network products, services and operations as appropriate.

ÿ4ÿ

National standards and industry standards.

The state supports enterprises, research institutions, universities, and internet-related industry organizations to participate.

In conjunction with the formulation of national and industry standards for cybersecurity.

Article 17 The State Council and the people's governments of provinces, autonomous regions and municipalities directly under the Central Government shall make overall plans

Plan, increase investment, support key cybersecurity technology industries and projects, and support network security.

Research, development, and application of security technologies; promotion of secure and reliable network products and services.

Protect intellectual property rights related to network technologies and support the participation of enterprises, research institutions, and universities.

National Cybersecurity Technology Innovation Project.

Article 18 The State promotes the construction of a socialized cybersecurity service system and encourages relevant entities to participate in such initiatives.

Provide cybersecurity certification, testing, and risk assessment services to relevant enterprises and institutions.

Article 19 The State encourages the development of technologies for the protection and utilization of network data security, and promotes...

Promote the opening up of public data resources to drive technological innovation and economic and social development.

Article 20 The State supports basic theoretical research and key technologies such as algorithms in artificial intelligence.

Technological research and development, advancing the construction of infrastructure such as training data resources and computing power, and improving artificial intelligence.

Intelligent ethical guidelines, strengthening risk monitoring and assessment and safety supervision, and promoting the application of artificial intelligence

Use and healthy development.

The state supports innovative approaches to cybersecurity management, utilizing new technologies such as artificial intelligence.

Improve the level of cybersecurity protection.

Article 21 People's governments at all levels and their relevant departments shall organize and carry out economic...

Regular cybersecurity awareness and education should be conducted, and relevant units should be guided and supervised to improve cybersecurity.

Publicity and education work.

Mass media should conduct targeted cybersecurity awareness campaigns to the public.

educate.

Article 22 The State supports enterprises and institutions of higher learning, vocational schools, and other educational institutions and training organizations.

Training institutions conduct cybersecurity-related education and training, and cultivate cybersecurity professionals through various means.

We need to cultivate a diverse pool of talent and promote the exchange of cybersecurity professionals.

Chapter 3 Network Operation Security

Section 1 General Provisions

Article 23 The State implements a network security classification protection system. Network operators

The following security protection obligations shall be fulfilled in accordance with the requirements of the network security classification protection system.

Protect the network from interference, sabotage, or unauthorized access, and prevent network data leakage.

Exposure or theft/tampering:

(a) Establish internal security management systems and operating procedures, and define network security responsibilities.

Responsible persons should implement network security protection responsibilities;

(ii) Take measures to prevent computer viruses, network attacks, network intrusions, and other threats to the network.

Technical measures for network security behavior;

(iii) Adopting technologies to monitor and record network operation status and network security incidents.

Measures shall be taken, and relevant network logs shall be retained for no less than six months as required;

(iv) Take measures such as data classification, backup of important data, and encryption;

(v) Other obligations stipulated by laws and administrative regulations.

Article 24 Network products and services shall comply with the mandatory standards of relevant national standards.

ÿ6ÿ

Sexual requirements. Providers of network products and services must not install malicious programs; if they discover that their network...

When network products or services have security flaws, vulnerabilities, or other risks, remedial measures should be taken immediately.

Measures should be taken to promptly inform users and report to relevant authorities in accordance with regulations.

Providers of network products and services shall continuously provide security for their products and services.

Maintenance; security maintenance shall not be terminated within the prescribed period or the period agreed upon by the parties.

Providers of network products and services that have the function of collecting user information shall, in accordance with the relevant regulations, disclose such information to the relevant authorities.

The user has given explicit consent; where user personal information is involved, this law and relevant regulations shall also be followed.

Relevant laws and administrative regulations regarding the protection of personal information.

Article 22 Key network equipment and dedicated network security products shall be in accordance with

The mandatory requirements of relevant national standards shall be subject to safety certification by qualified institutions or

Products can only be sold or provided after passing safety inspections. The State Internet Information Office, in conjunction with...

Relevant departments of the State Council shall formulate and publish a list of key network equipment and dedicated network security products.

Record and promote mutual recognition of security certification and security testing results to avoid duplicate certification and testing.

Article 26 Network operators shall provide users with network access and domain name registration services.

Services include handling network access procedures for landline and mobile phones, or providing information to users.

Services such as publishing and instant messaging, when signing an agreement with users or confirming the provision of services,

Users should be required to provide their real identity information. If a user fails to provide their real identity information,

Network operators are prohibited from providing related services to them.

The state implements a network trusted identity strategy and supports research and development of secure and convenient electronic identity systems.

Electronic identity authentication technology promotes mutual recognition between different electronic identity authentication methods.

Article 27 Network operators shall formulate emergency response plans for network security incidents.

Promptly address security risks such as system vulnerabilities, computer viruses, network attacks, and network intrusions.

Risk; In the event of an incident endangering cybersecurity, immediately activate the emergency response plan and take appropriate measures.

Appropriate remedial measures should be taken, and a report should be submitted to the relevant competent authorities in accordance with regulations.

Article 28. Conducting activities such as cybersecurity certification, testing, and risk assessment.

Release information to the public regarding system vulnerabilities, computer viruses, network attacks, and network intrusions.

Security information shall comply with relevant national regulations.

Article 29 No individual or organization may engage in illegally intruding into another person's network.

Activities that endanger network security, such as interfering with the normal functioning of others' networks or stealing network data;

It is prohibited to provide equipment specifically designed for intruding into networks, interfering with normal network functions, and infringing upon protective measures.

Programs and tools used to steal network data or engage in activities that endanger cybersecurity; knowingly allowing others to engage in such activities.

Those who engage in activities that endanger cybersecurity shall not be provided with technical support, advertising, or other assistance.

Assistance with payment settlement, etc.

Article 30 Network operators shall provide services to public security organs and national security organs in accordance with the law.

Provide technical support and assistance for activities to safeguard national security and investigate crimes.

Article 31 The State supports cooperation among network operators in the collection of network security information.

Collaborate on data collection, analysis, reporting, and emergency response to improve network operators' capabilities.

Security capabilities.

Relevant industry organizations should establish and improve their industry-specific cybersecurity protection standards and collaboration mechanisms.

Establish a mechanism to strengthen the analysis and assessment of cybersecurity risks and regularly provide risk warnings to members.

It indicates that it supports and assists members in addressing cybersecurity risks.

Article 32. Cyberspace administration departments and relevant departments, in fulfilling their responsibilities for cybersecurity protection,

Information obtained during this process may only be used for the purpose of maintaining network security and may not be used for any other purpose.

use.

ÿ8ÿ

Section 2 Operational Security of Critical Information Infrastructure

Article 33 The State provides for public communication and information services, energy, transportation, and water.

Important industries and fields such as interest, finance, public services, and e-government, as well as other...

If damaged, rendered inoperable, or if data is leaked, it could seriously endanger national security.

Critical information infrastructure vital to the national economy, people's livelihood, and public interest is subject to cybersecurity level protection.

Based on the existing system, key protection measures will be implemented. The specific scope of critical information infrastructure and...

The security protection measures shall be formulated by the State Council.

The state encourages network operators other than those involved in critical information infrastructure to voluntarily participate in the relevant...

Key information infrastructure protection system.

Article 34. In accordance with the division of responsibilities stipulated by the State Council, those responsible for key information infrastructure...

The relevant departments responsible for infrastructure safety protection shall formulate and organize the implementation of relevant plans and regulations for their respective industries and fields.

Critical information infrastructure security planning, guidance and supervision of critical information infrastructure operations

To carry out safety protection work.

Article 35 The construction of critical information infrastructure shall ensure that it has the support

Ensuring stable and continuous operation of services, and guaranteeing that security measures are planned and implemented concurrently.

Construction should be carried out step by step and used simultaneously.

Article 36 Except as provided in Article 23 of this Law, critical information infrastructure

The operator of the facility shall also fulfill the following safety protection obligations:

(i) Establish a dedicated safety management organization and appoint a safety management officer, and hold the responsible officer accountable.

Conduct security background checks on responsible persons and key personnel;

(ii) Regularly provide cybersecurity education, technical training, and skills training to employees.

Assessment;

(iii) Perform disaster recovery backups for important systems and databases;

(iv) Develop emergency response plans for cybersecurity incidents and conduct regular drills;

(v) Other obligations stipulated by laws and administrative regulations.

Article 37 Operators of critical information infrastructure shall procure network products and

Services that may affect national security should be handled through the State Internet Information Office in conjunction with the State Council.

National security review organized by relevant departments.

Article 38. Operators of critical information infrastructure shall procure network products and

For services, a security and confidentiality agreement should be signed with the provider in accordance with regulations, clearly defining security and protection responsibilities.

Confidentiality obligations and responsibilities.

Article 39 Operators of critical information infrastructure in the People's Republic of China

Personal information and important data collected and generated during operations within the country should be stored within the country.

If it is truly necessary to provide information to overseas entities for business purposes, it should be done in accordance with the requirements of the State Internet Information Office in conjunction with relevant national departments.

Safety assessments shall be conducted in accordance with the procedures formulated by the relevant departments of the State Council; where laws and administrative regulations provide otherwise.

It is determined according to its regulations.

Article 40 Operators of critical information infrastructure shall, either independently or by entrusting others,

Cybersecurity service providers assess the security of their networks and potential risks at least annually.

Conduct an evaluation and report the evaluation results and improvement measures to the relevant responsible party.

The department responsible for the security protection of critical information infrastructure.

Article 41 The State Internet Information Office shall coordinate relevant departments to address key issues.

The following measures are taken to protect the security of information infrastructure:

(i) Conduct spot checks and tests on the security risks of critical information infrastructure and propose solutions.

Improvement measures may be implemented, and if necessary, a cybersecurity service organization may be commissioned to assess network security issues.

Risk detection and assessment;

(ii) Regularly organize network security drills for operators of critical information infrastructure.

Emergency drills were conducted to improve the level of response to cybersecurity incidents and the ability to coordinate and cooperate.

(iii) Promote the relevant departments, operators of critical information infrastructure, and related parties

Cybersecurity information sharing among research institutions, cybersecurity service providers, and others;

(iv) Provide emergency response and network function restoration for cybersecurity incidents, etc.

Provide technical support and assistance.

Chapter 4 Network Information Security

Article 42 Network operators shall strictly protect the user information they collect.

Confidentiality and the establishment of a sound user information protection system.

Network operators shall comply with this law and the Basic Law of the People's Republic of China when processing personal information.

The Civil Code, the Personal Information Protection Law of the People's Republic of China, and other laws and administrative regulations

According to the regulations.

Article 43 Network operators shall collect and use personal information in accordance with the law.

The principles of legality, legitimacy, and necessity must be upheld, and the rules for collecting and using information must be made public and clearly stated.

The purpose, method, and scope of the information, and with the consent of the person whose information is collected.

Network operators are prohibited from collecting personal information unrelated to the services they provide.

Collecting and using personal information in violation of laws, administrative regulations, and agreements between the parties.

And it shall handle its storage in accordance with the provisions of laws and administrative regulations and the agreement with users.

Personal information.

Article 44 Network operators shall not disclose, tamper with, or destroy the personal information they collect.

Personal information; personal information may not be provided to others without the consent of the person whose information was collected. However,

Except for those that have been processed in a way that makes it impossible to identify a specific individual and cannot be restored.

Network operators shall take technical measures and other necessary measures to ensure the security of their collected data.

Protecting personal information security and preventing information leakage, damage, or loss. In the event of or potential leakage of personal information.

In the event of leakage, damage, or loss of personal information, remedial measures should be taken immediately.

The relevant authorities shall promptly inform users and report to the relevant competent authorities in accordance with regulations.

Article 45. Individuals who discover violations of laws and administrative regulations by network operators shall report such violations.

If a network operator collects or uses an individual's personal information in accordance with a contract or agreement between the parties, the individual has the right to request the network operator to take appropriate action.

The user deletes their personal information; if they discover that the network operator has collected or stored their personal information in a manner that is illegal or harmful, they should take appropriate action.

If something is incorrect, the user has the right to request the network operator to correct it. The network operator should take measures.

The relevant authorities shall delete or correct the content.

Article 46 No individual or organization may steal or otherwise illegally obtain

Personal information must not be obtained illegally or illegally sold or provided to others.

Article 47 Departments legally responsible for cybersecurity supervision and management and their...

Staff members must be responsible for any personal information, privacy, and trade secrets they learn in the course of performing their duties.

It must be kept strictly confidential and must not be disclosed, sold, or illegally provided to others.

Article 48. Every individual and organization shall be responsible for their use of the Internet.

It is prohibited to establish a platform for committing fraud, teaching criminal methods, or producing or selling prohibited items.

Websites and communication groups involved in illegal activities such as selling prohibited or controlled items are prohibited from using the internet.

Posting information online that involves fraud, producing or selling prohibited or controlled items, and other illegal or unauthorized materials.

Information about his illegal and criminal activities.

Article 49 Network operators shall strengthen the management of information published by their users.

If management discovers information that is prohibited from being published or transmitted by laws and administrative regulations, it shall immediately take action.

This means stopping the transmission of the information, taking measures such as deletion to prevent its spread, and preserving it.

Record the relevant information and report it to the relevant authorities.

Article 50. Any electronic information sent by any individual or organization, or application software provided by such individual or organization...

Documents must not contain malicious programs or content prohibited by laws and administrative regulations.

The information being transmitted.

Electronic information transmission service providers and application software download service providers shall

If a company fails to fulfill its security management obligations and becomes aware that its users have engaged in the conduct described in the preceding paragraph, it shall cease providing services.

Provide services, take measures such as elimination, preserve relevant records, and report to the relevant competent authorities.

Door report.

Article 51 Network operators shall establish a system for handling network information security complaints and reports.

The system should be established to publicize information such as complaint and reporting methods, and to promptly accept and handle relevant online information.

Complaints and reports regarding information security.

Network operators should exercise their rights against the lawful supervision and inspection conducted by the Cyberspace Administration and relevant departments.

We should cooperate.

Article 52 The State Internet Information Office and relevant departments shall perform their duties in accordance with the law regarding network information.

Safety supervision and management responsibilities include discovering information that is prohibited from being published or transmitted by laws and administrative regulations.

If information is leaked, the network operator should be required to stop transmission and take measures such as deletion to protect the information.

Relevant records shall be kept; for the aforementioned information originating outside the territory of the People's Republic of China, notification shall be provided.

We are aware that relevant agencies have taken technical and other necessary measures to block the spread.

Chapter 5 Monitoring, Early Warning and Emergency Response

Article 53 The State shall establish a network security monitoring, early warning and information reporting system.

The national cyberspace administration department should coordinate with relevant departments to strengthen the collection and distribution of cybersecurity information.

The analysis and reporting work shall be carried out in accordance with regulations to uniformly release network security monitoring and early warning information.

Article 54 The department responsible for the security protection of critical information infrastructure,

A sound network security monitoring, early warning, and information reporting system should be established for this industry and field.

They shall, in accordance with regulations, report network security monitoring and early warning information.

Article 55 The State Internet Information Office shall coordinate with relevant departments to establish and improve network security

Establish a comprehensive risk assessment and emergency response mechanism, formulate emergency response plans for cybersecurity incidents, and...

Organize drills regularly.

The department responsible for the security protection of critical information infrastructure shall formulate its own regulations.

Develop emergency response plans for cybersecurity incidents in the industry and field, and organize drills regularly.

Cybersecurity incident emergency response plans should be tailored to the severity and impact of the incident.

Cybersecurity incidents are classified according to factors such as the scope of impact, and corresponding emergency response measures are stipulated.

measure.

Article 56 When the risk of a cybersecurity incident increases, the provincial-level or higher people's government shall take appropriate action.

Relevant departments of the people's government shall, in accordance with the prescribed authority and procedures, and based on cybersecurity risks, [take appropriate action].

Given the characteristics of the risk and the potential harm it may cause, the following measures should be taken:

(i) Relevant departments, institutions, and personnel are required to collect and report relevant information in a timely manner.

Strengthen the monitoring of cybersecurity risks;

(ii) Organize relevant departments, institutions, and professionals to assess cybersecurity risks.

The information is analyzed and assessed to predict the likelihood of the event occurring, the scope of its impact, and the degree of harm.

(iii) Issue cybersecurity risk warnings to the public and release guidelines on avoiding and mitigating harm.

Measures.

Article 57 In the event of a cybersecurity incident, a cybersecurity response mechanism shall be immediately initiated.

An emergency response plan is in place to investigate and assess cybersecurity incidents, requiring network operators to...

Take technical and other necessary measures to eliminate safety hazards and prevent the spread of harm.

And promptly release warning information to the public.

Article 58. Relevant departments of the people's governments at or above the provincial level shall, in fulfilling their duties related to cybersecurity...

In the course of supervisory and management responsibilities, if significant security risks are discovered on the network or a security incident occurs...

Yes, the legal representative of the network operator can be subject to the prescribed authority and procedures.

Or, the main person in charge may be summoned for a meeting. Network operators should take measures as required.

Rectification should be carried out to eliminate potential hazards.

Article 59. In the event of a cybersecurity incident, a sudden incident, or a production safety incident,

In the event of an accident, it shall be handled in accordance with the "Emergency Response Law of the People's Republic of China" and the "Law of the People's Republic of China on Responding to Public Health Emergencies".

In accordance with the provisions of the "Work Safety Law of the People's Republic of China" and other relevant laws and administrative regulations, this matter shall be handled accordingly.

Article 60. In order to safeguard national security and public order, and to handle major emergencies

In cases of public security incidents, with the decision or approval of the State Council, [action may be taken] in specific areas.

Temporary measures such as restrictions on network communications were implemented.

Chapter Six Legal Liability

Article 61 If a network operator fails to comply with Articles 23 and 27 of this Law...

Those who fail to fulfill their cybersecurity protection obligations as stipulated in the regulations shall be ordered to rectify the situation by the relevant competent authorities and shall be given [punishment/punishment].

A warning may be issued, and a fine of between 10,000 and 50,000 yuan may be imposed; failure to rectify the situation or causing danger may result in further consequences.

Those who cause harm to network security or other consequences shall be fined between 50,000 and 500,000 yuan.

The responsible supervisors and other directly responsible personnel shall be fined between 10,000 and 100,000 yuan.

payment.

Operators of critical information infrastructure who fail to comply with Articles 35 and 30 of this Law

Those who have the network security protection obligations stipulated in Articles 6, 38, and 40 shall be subject to the provisions of Article 6, 38, and 40.

The relevant authorities may order rectification, issue a warning, and impose a fine of between 50,000 and 100,000 yuan.

A fine; if the violation is not rectified or results in consequences such as endangering cybersecurity, a fine of 100,000 yuan or more will be imposed.

Fines of up to one million yuan will be imposed on the directly responsible supervisors and other directly responsible personnel.

A fine of between 10,000 and 100,000 yuan shall be imposed.

The first two types of behavior resulted in massive data breaches and the loss of critical information infrastructure.

Those who seriously endanger network security due to partial functionalities or other reasons shall be fined 500,000 yuan by the relevant competent authorities.

A fine of between RMB 100,000 and RMB 2 million shall be imposed on the directly responsible supervisors and other directly responsible persons.

Personnel responsible will be fined between 50,000 and 200,000 yuan; damage to critical information infrastructure

Those who cause particularly serious harm to cybersecurity, such as loss of primary functions, shall be subject to a fine of two million yuan or more.

Fines of up to ten million yuan will be imposed on the directly responsible supervisors and other directly responsible personnel.

A fine of between 200,000 and 1 million yuan shall be imposed.

Article 62 Violations of Article 24, Paragraphs 1 and 2, and Article 50 of this Law

Article 1 stipulates that if any of the following acts are committed, the relevant competent authority shall order rectification.

ÿ16ÿ

A warning will be given; if the violation is not rectified or results in consequences such as endangering cybersecurity, a fine of 50,000 yuan will be imposed.

Fines ranging from 500,000 to 100,000 yuan shall be imposed on the directly responsible supervisors.

Fines under 10,000 yuan:

(i) Setting up malicious programs; (ii) Failing to take

immediate remedial measures for security defects, vulnerabilities, or other risks in its products or services, or failing to promptly inform users

and relevant authorities as required.

Reported;

(iii) Terminating the provision of security maintenance for its products and services without authorization.

If the conduct described in items (1) or (2) of the preceding paragraph causes harm as stipulated in Article 61, Paragraph 3 of this Law,

Those who cause certain consequences shall be punished in accordance with the provisions of this clause.

Article 63. Violating Article 25 of this Law by selling or providing goods that have not been properly certified...

Safety certification, safety testing, or failure to pass safety certification or safety testing requirements.

For critical network equipment and dedicated network security products, the relevant competent authorities shall order a halt to their use.

Stop selling or providing it, issue a warning, and confiscate illegal gains; if there are no illegal gains or

If the illegal gains are less than 100,000 yuan, a fine of between 20,000 and 100,000 yuan shall be imposed;

For those whose illegal gains exceed 100,000 yuan, a fine of one to five times the illegal gains shall be imposed; if the circumstances are serious...

In serious cases, the relevant business may be suspended, the business may be ordered to cease operations for rectification, or the relevant business license may be revoked.

The business license may be revoked or its issuance may be suspended. If otherwise stipulated by laws or administrative regulations, those provisions shall prevail.

Certainly.

Article 64. If a network operator violates the provisions of Article 26, Paragraph 1 of this Law,

The system failed to require users to provide their real identity information, or did not provide users with their real identity information.

If a customer provides related services, the relevant competent authority shall order them to rectify the situation; if they refuse to rectify the situation or...

For serious offenses, a fine of between 50,000 and 500,000 yuan may be imposed, and the offender may be ordered to suspend related activities.

Closing down operations, suspending business for rectification, shutting down websites or applications, and revoking relevant business licenses.

The license or business license may be revoked, and the directly responsible supervisors and other directly responsible persons shall be dealt with accordingly.

The employee will be fined between 10,000 and 100,000 yuan.

Article 65. Violating Article 28 of this Law by conducting network security certification,

Activities such as detection and risk assessment, or releasing information about system vulnerabilities and computer viruses to the public.

For cybersecurity information such as cyberattacks and cyber intrusions, the relevant competent authorities shall order rectification.

For violations, a warning may be issued, and a fine of between 10,000 and 100,000 yuan may be imposed; if the violation is not corrected, or

Those whose circumstances are serious shall be fined between 100,000 and 1 million yuan, and may be ordered to temporarily suspend their duties.

Suspend related business operations, suspend operations for rectification, shut down websites or applications, or revoke related business licenses.

The license or business license will be revoked, and the directly responsible supervisors and other directly responsible persons will be punished.

Those who violate this rule will be fined between 10,000 and 100,000 yuan.

If the conduct described in the preceding paragraph causes the consequences specified in Article 61, Paragraph 3 of this Law, the offender shall be punished in accordance with the law.

Punishment shall be imposed in accordance with the provisions of this clause.

Article 66. Violating Article 29 of this Law by engaging in activities that endanger cybersecurity.

Activities that endanger cybersecurity, or provide programs or tools specifically designed for such activities.

Or providing technical support or advertising to others for activities that endanger cybersecurity.

If assistance in payment settlement or other matters does not constitute a crime, the public security authorities shall confiscate the illegal gains.

Detention for up to five days may be imposed, and a fine of between 50,000 and 500,000 yuan may also be imposed; [The sentence is incomplete and requires further context.]

For more serious offenses, the offender shall be detained for not less than five days but not more than fifteen days, and may also be fined not less than 100,000 yuan.

Fines of less than 10,000 yuan.

If an entity engages in the conduct described in the preceding paragraph, the public security authorities shall confiscate its illegal gains and impose a fine of up to 100,000 yuan.

A fine of up to one million yuan will be imposed, and the directly responsible supervisors and other directly liable personnel will also be punished.

Personnel shall be punished in accordance with the provisions of the preceding paragraph.

Anyone who violates Article 29 of this law and is subject to administrative penalties for public security violations shall be subject to a five-year ban.

Those who are criminally detained are prohibited from working in key positions related to network security management and network operations;

Those who are punished will be permanently barred from holding key positions in network security management and network operations.

Work.

Article 67 Operators of critical information infrastructure who violate Article 30 of this Law

The seven provisions stipulate that using network products that have not undergone security review or have failed security review is prohibited.

Those providing services shall be ordered by the relevant competent authorities to rectify within a specified period, cease use, and eliminate the harm to the country.

For violations affecting home security, a fine of one to ten times the purchase amount will be imposed, and those directly responsible will be held accountable.

Supervisors and other directly responsible personnel shall be fined between 10,000 and 100,000 yuan.

Article 68. Violating Article 48 of this Law by establishing an institution for the purpose of committing illegal acts.

Websites and communication groups used for criminal activities, or the use of the internet to publish information related to illegal activities.

Information regarding criminal activities that do not yet constitute a crime shall be subject to detention of up to five days by the public security authorities.

A fine of between 10,000 and 100,000 yuan may be imposed; in serious cases, a sentence of five days or more may be imposed.

Detention for up to 15 days may be accompanied by a fine of between 50,000 and 500,000 yuan.

Websites and communication groups used to carry out illegal and criminal activities.

If an entity commits any of the acts mentioned in the preceding paragraph, the public security organ shall impose a fine of not less than 100,000 yuan but not more than 500,000 yuan.

A fine shall be imposed, and the directly responsible supervisors and other directly responsible personnel shall be punished in accordance with the provisions of the preceding paragraph.

A penalty will be imposed.

Article 69 If a network operator violates Article 49 of this Law, causing damage to the law,

Information that is prohibited from being published or transmitted by administrative regulations has not been stopped from being transmitted or has not been removed.

Measures, preservation of relevant records, reporting to the relevant competent authorities, or violation of Article 5 of this Law

Article 12 stipulates that failure to comply with the requirements of relevant departments regarding the publication of information prohibited by laws and administrative regulations is prohibited.

Alternatively, the transmitted information may be stopped, deletion measures may be taken, or relevant records may be preserved.

If so, the relevant competent authorities shall order rectification, issue a warning, and issue a public notice, and may impose a fine of five...

A fine of between 10,000 and 500,000 yuan; if the violation is refused or the circumstances are serious, a fine of 50,000 yuan will be imposed.

A fine of between 10,000 and 2 million yuan may be imposed, and the business may be ordered to suspend related operations or cease operations for rectification.

Shutting down the website or application, revoking the relevant business license, or suspending the business license.

The license will be revoked, and the directly responsible supervisors and other directly responsible personnel will be fined more than 50,000 yuan.

A fine of less than 200,000 yuan.

If the conduct described in the preceding paragraph causes particularly serious impact or consequences, the relevant authorities shall...

The relevant authorities shall impose a fine of between two million and ten million yuan and order the suspension of related business operations.

Suspension of business for rectification, closure of website or application, revocation of relevant business license or suspension of business operations.

The business license will be revoked, and the directly responsible supervisor and other directly responsible personnel will be fined twenty...

Fines ranging from 10,000 to 1 million yuan.

Electronic information transmission service providers and application software download service providers fail to fulfill their obligations.

Those who fail to fulfill the safety management obligations stipulated in Article 50, Paragraph 2 of this Law shall be subject to the provisions of the preceding two paragraphs.

Punishment.

Article 70. If a network operator violates the provisions of this Law by engaging in any of the following acts,

The relevant authorities shall order rectification; if rectification is refused or the circumstances are serious, a fine of 50,000 yuan shall be imposed.

Fines of up to 500,000 yuan will be imposed on the directly responsible supervisors and other directly responsible personnel.

Personnel involved will be fined between 10,000 and 100,000 yuan.

(i) Refusing or obstructing the lawful supervision and inspection carried out by relevant departments;

(ii) Refusing to provide technical support and assistance to public security organs and national security organs.

of.

Article 71 Any of the following acts shall be punished in accordance with relevant laws and administrative regulations.

Regulations for handling and punishment:

(i) Publishing or transmitting Article 13, Paragraph 2 of this Law and other laws and administrative regulations.

Information that is prohibited from being published or transmitted by laws and regulations;

(ii) Violation of Article 24, Paragraph 3, and Articles 43 to 45 of this Law

This provision stipulates that infringement of personal information rights;

(iii) Violating Article 39 of this Law by storing personal information and important data overseas, or providing personal information

and data to overseas entities.

Important data.

Violating Article 46 of this Law by stealing or otherwise illegally obtaining

The illegal sale or provision of personal information to others, without constituting a crime, shall be handled by the public security authorities.

The public security authorities shall impose penalties in accordance with the provisions of relevant laws and administrative regulations.

Article 72. Anyone who commits an illegal act as stipulated in this Law shall be punished in accordance with relevant laws and regulations.

The provisions of laws and regulations shall be recorded in the credit file and made public.

Article 73. Violations of this Law, but which fall under the category of violations of the Administrative Litigation Law of the People's Republic of China, shall be subject to the following penalties:

If the circumstances for mitigation, reduction, or exemption from punishment are stipulated in the Penalty Law, they shall be handled in accordance with those provisions.

The punishment may be mitigated, reduced, or waived.

Article 74. Operators of government networks of state organs who fail to perform the provisions of this Law shall be subject to penalties.

If a party fails to fulfill its network security protection obligations, its superior authority or relevant authority shall order it to rectify the situation.

The directly responsible supervisors and other directly responsible personnel shall be punished in accordance with the law.

Article 75. If the Cyberspace Administration and relevant departments violate Article 32 of this Law...

It is determined that information obtained in the course of fulfilling cybersecurity protection responsibilities will not be used for other purposes.

The directly responsible supervisors and other directly responsible personnel shall be punished in accordance with the law.

Staff members of the Cyberspace Administration and relevant departments neglected their duties, abused their power, and acted out of favoritism.

Those who engage in cheating but whose actions do not constitute a crime shall be punished in accordance with the law.

Article 76 Anyone who violates the provisions of this Law and causes damage to others shall bear legal responsibility.

civil liability.

Anyone who violates the provisions of this law and whose conduct constitutes a violation of public security administration shall be punished in accordance with the law.

Those who violate the law will be punished; if their actions constitute a crime, they will be prosecuted according to law.

Article 77. Foreign institutions, organizations, and individuals engaging in activities that endanger the People's Republic of China

Those who engage in activities that endanger national cybersecurity will be held legally responsible; those causing serious consequences will be punished.

The State Council's public security department and relevant departments may decide to take action against this institution, organization, or individual.

Take measures such as freezing assets or other necessary sanctions.

Chapter Seven Supplementary Provisions

Article 78 The following terms in this Law shall have the following meanings:

(a) A network refers to a system consisting of computers or other information terminals and related equipment.

The process of collecting, storing, transmitting, and exchanging information according to certain rules and procedures.

The system being processed.

(ii) Network security refers to taking necessary measures to prevent attacks on networks.

Attacks, intrusions, interference, damage, unauthorized use, and accidents can disrupt network stability.

To ensure reliable operation and guarantee the integrity, confidentiality, and availability of network data.

Sexual capacity.

(iii) Network operators refer to the owners, managers, and service providers of the network.

Provider.

(iv) Network data refers to data collected, stored, transmitted, processed, and transmitted through a network.

Various types of electronic data generated.

(v) Personal information refers to various information recorded electronically or otherwise that can identify a natural

person, either alone or in combination with other information, including but not limited to...

Limited to the name, date of birth, ID number, and personal biometric information of natural persons.

Information, address, telephone number, etc.

Article 79 Security of the operation of networks storing and processing information involving state secrets

In addition to complying with this law, full protection must also comply with confidentiality laws and administrative regulations.

Regulation.

Article 80 The security protection of military networks shall be separately stipulated by the Central Military Commission.

Certainly.

Article 81 This Law shall come into force on June 1, 2017.