

CHINA'S
CYBERSECURITY
LAW



Cybersecurity Law of the People's Republic of China

January 2019



ASIA BRIEFING



DEZAN SHIRA & ASSOCIATES

Your Partner for Growth in Asia

This document is for research purposes only; it should not be used as an official document.

Chapter I

General Provisions

Article 1

This Law is formulated in order to ensure cybersecurity; safeguard cyberspace sovereignty and national security, and social and public interests; protect the lawful rights and interests of citizens, legal persons, and other organizations; and promote the healthy development of the informatization of the economy and society.

Article 2

This Law is applicable to the construction, operation, maintenance, and use of networks, as well as to cybersecurity supervision and management within the mainland territory of the People's Republic of China.

Article 3

The State persists in equally stressing cybersecurity and informatization development, and abides by the principles of active use, scientific development, management in accordance with law, and ensuring security. The State advances the construction of network infrastructure and interconnectivity, encourages the innovation and application of network technology, supports the cultivation of qualified cybersecurity personnel, establishes a complete system to safeguard cybersecurity, and raises capacity to protect cybersecurity.

Article 4

The State formulates and continuously improves cybersecurity strategy, clarifies the fundamental requirements and primary goals of ensuring cybersecurity, and puts forward cybersecurity policies, work tasks, and procedures for key sectors.

Article 5

The State takes measures for monitoring, preventing, and handling cybersecurity risks and threats arising both within and without the mainland territory of the People's Republic of

China. The State protects critical information infrastructure against attacks, intrusions, interference, and destruction; the State punishes unlawful and criminal cyber activities in accordance with the law, preserving the security and order of cyberspace.

Article 6

The State advocates sincere, honest, healthy and civilized online conduct; it promotes the dissemination of core socialist values, adopts measures to raise the entire society's awareness and level of cybersecurity, and formulates a good environment for the entire society to jointly participate in advancing cybersecurity.

Article 7

The State actively carries out international exchanges and cooperation in the areas of cyberspace governance, research and development of network technologies, formulation of standards, attacking cybercrime and illegality, and other such areas; it promotes constructing a peaceful, secure, open, and cooperative cyberspace, and establishing a multilateral, democratic, and transparent Internet governance system.

Article 8

State cybersecurity and informatization departments are responsible for comprehensively planning and coordinating cybersecurity efforts and related supervision and management efforts. The State Council departments for telecommunications, public security, and other relevant organs, are responsible for cybersecurity protection, supervision, and management efforts within the scope of their responsibilities, in accordance with the provisions of this Law and relevant laws and administrative regulations.

Cybersecurity protection, supervision, and management duties for relevant departments in people's governments at the county level or above will be determined by relevant national regulations.

Article 9

Network operators carrying out business and service activities must follow laws and administrative regulations, respect social morality, abide by commercial ethics, be honest and credible, perform obligations to protect cybersecurity, accept supervision from the government and public, and bear social responsibility.

Article 10

The construction and operation of networks, or the provision of services through networks, shall be done in accordance with the provisions of laws and administrative regulations, and with the mandatory requirements of national standards; adopting technical measures and other necessary measures to safeguard cybersecurity and operational stability; effectively responding to cybersecurity incidents; preventing cybercrimes and unlawful activity; and preserving the integrity, secrecy, and usability of online data.

Article 11

Relevant Internet industry organizations, according to their Articles of Association, shall strengthen industry self-discipline, formulate cybersecurity norms of behavior, guide their members in strengthening cybersecurity protection according to the law, raise the level of cybersecurity protection, and stimulate the healthy development of the industry.

Article 12

The State protects the rights of citizens, legal persons, and other organizations to use networks in accordance with the law; it promotes widespread network access, raises the level of network services, provides secure and convenient network services to society, and guarantees the lawful, orderly, and free circulation of network information.

Any person and organization using networks shall abide by the Constitution and laws, observe public order, and respect social morality; they must not endanger cybersecurity, and must not use the Internet to engage in activities endangering national

security, national honor, and national interests; they must not incite subversion of national sovereignty, overturn the socialist system, incite separatism, break national unity, advocate terrorism or extremism, advocate ethnic hatred and ethnic discrimination, disseminate violent, obscene, or sexual information, create or disseminate false information to disrupt the economic or social order, or information that infringes on the reputation, privacy, intellectual property or other lawful rights and interests of others, and other such acts.

Article 13

The State encourages research and development of network products and services conducive to the healthy upbringing of minors; the State will lawfully punish the use of networks to engage in activities that endanger the psychological and physical well-being of minors; and the State will provide a safe and healthy network environment for minors.

Article 14

All individuals and organizations have the right to report conduct endangering cybersecurity to cybersecurity and informatization, telecommunications, public security, and other departments. Departments receiving reports shall promptly process them in accordance with law; where matters do not fall within the responsibilities of that department, they shall promptly transfer them to the department empowered to handle them.

Relevant departments shall preserve the confidentiality of the informants' information and protect the lawful rights and interests of informants.

Chapter II The Support and Promotion of Cybersecurity

Article 15

The State establishes and improves a system of cybersecurity standards. State Council standardization administrative departments

and other relevant State Council departments, on the basis of their individual responsibilities, shall organize the formulation and timely revision of relevant national and industry standards for cybersecurity management, as well as for the security of network products, services, and operations.

The State supports enterprises, research institutions, schools of higher learning, and network-related industry organizations to participate in the formulation of national and industry standards for cybersecurity.

Article 16

The State Council and people's governments of provinces, autonomous regions, and directly-governed municipalities shall do comprehensive planning; expand investment; support key cybersecurity technology industries and programs; support cybersecurity technology research and development, application, and popularization; promote secure and trustworthy network products and services; protect intellectual property rights for network technologies; and support research and development institutions, schools of higher learning, etc., to participate in State cybersecurity technology innovation programs.

Article 17

The State advances the establishment of socialized service systems for cybersecurity, encouraging relevant enterprises and institutions to carry out cybersecurity certifications, testing, risk assessment, and other such security services.

Article 18

The State encourages the development of network data security protection and utilization technologies, advancing the opening of public data resources, and promoting technical innovation and economic and social development.

The State supports innovative methods of cybersecurity management, utilizing new network technologies to enhance the level of cybersecurity protection.

Article 19

All levels of people's governments and their relevant departments shall organize and carry out regular cybersecurity publicity and education, and guide and stimulate relevant units in properly carrying out cybersecurity publicity and education work.

The mass media shall conduct targeted cybersecurity publicity and education aimed at the public.

Article 20

The State supports enterprises and education or training institutions, such as schools of higher learning and vocational schools, in carrying out cybersecurity-related education and training, and it employs multiple methods to cultivate qualified personnel in cybersecurity and promote the interaction of cybersecurity professionals.

Chapter III Network Operations Security

Section 1

Ordinary Provisions

Article 21

The State implements a cybersecurity multi-level protection system [MLPS]. Network operators shall perform the following security protection duties according to the requirements of the cybersecurity multi-level protection system to ensure the network is free from interference, damage, or unauthorized access, and to prevent network data leaks, theft, or falsification

- (1) Formulate internal security management systems and operating rules, determine persons who are responsible for cybersecurity, and implement cybersecurity protection responsibility;
- (2) Adopt technical measures to prevent computer viruses, cyber-attacks, network intrusions, and other actions endangering cybersecurity;

- (3) Adopt technical measures for monitoring and recording network operational statuses and cybersecurity incidents, and follow provisions to store network logs for at least six months;
- (4) Adopt measures such as data classification, backup of important data, and encryption;
- (5) Other obligations provided by law or administrative regulations.

Article 22

Network products and services shall comply with the relevant national and mandatory requirements. Providers of network products and services must not install malicious programs; when discovering that their products and services have security flaws or vulnerabilities, they shall immediately adopt remedial measures, and follow provisions to promptly inform users and report to the competent departments.

Providers of network products and services shall provide security maintenance for their products and services, and they must not terminate the provision of security maintenance during the time limits or period agreed on with clients.

If a network product or service has the function of collecting user information, its provider shall clearly indicate this and obtain consent from the user; and if this involves a user's personal information, the provider shall also comply with the provisions of this law and relevant laws and administrative regulations on the protection of personal information.

Article 23

Critical network equipment and specialized cybersecurity products shall follow national standards and mandatory requirements and be security certified by a qualified establishment or meet the requirements of a security inspection, before being sold or provided. The state cybersecurity and informatization departments, together with the relevant departments of the State Council, will formulate and release a catalog of critical network equipment and specialized cybersecurity products, and promote reciprocal recognition of security

certifications and security inspection results to avoid duplicative certifications and inspections.

Article 24

Network operators handling network access and domain name registration services for users, handling stationary or mobile phone network access, or providing users with information publication or instant messaging services, shall require users to provide real identity information when signing agreements with users or confirming the provision of services. Where users do not provide real identity information, network operators must not provide them with relevant services.

The State implements a network identity credibility strategy and supports research and development of secure and convenient electronic identity authentication technologies, promoting reciprocal acceptance among different electronic identity authentication methods.

Article 25

Network operators shall formulate emergency response plans for cybersecurity incidents and promptly address system vulnerabilities, computer viruses, cyber-attacks, network intrusions, and other such cybersecurity risks. When cybersecurity incidents occur, network operators should immediately initiate an emergency response plan, adopt corresponding remedial measures, and report to the relevant competent departments in accordance with relevant provisions.

Article 26

Those carrying out cybersecurity certification, testing, risk assessment, or other such activities—or publicly publishing cybersecurity information such as system vulnerabilities, computer viruses, network attacks, or network incursions—shall comply with relevant national provisions.

Article 27

Individuals and organizations must not engage in illegal intrusion into the networks of other parties, disrupt the normal functioning of the

networks of other parties, or steal network data or engage in other activities endangering cybersecurity; they must not provide programs, or tools specially used in network intrusions, that disrupt normal network functions and protection measures, steal network data, or engage in other acts endangering cybersecurity; and where they clearly are aware that others will engage in actions that endanger cybersecurity, they must not provide help such as technical support, advertisement and promotion, or payment of expenses.

Article 28

Network operators shall provide technical support and assistance to public security organs and national security organs that are safeguarding national security and investigating criminal activities in accordance with the law.

Article 29

The State supports cooperation between network operators in areas such as the gathering, analysis, reporting, and emergency handling of cybersecurity information, increasing the security safeguarding capacity of network operators.

Relevant industrial organizations are to establish and complete mechanisms for standardization and coordination of cybersecurity for their industry, strengthen their analysis and assessment of cybersecurity, and periodically conduct risk warnings, support, and coordination for members in responding to cybersecurity risks.

Article 30

Information obtained by cybersecurity and informatization departments and relevant departments performing cybersecurity protection duties can only be used as necessary for the protection of cybersecurity and must not be used in other ways.

Section 2

Operations Security for Critical Information Infrastructure

Article 31

The State implements key protection on the basis of the cybersecurity multi-level protection system for public communication and information services, power, traffic, water resources, finance, public service, e-government, and other critical information infrastructure which—if destroyed, suffering a loss of function, or experiencing leakage of data—might seriously endanger national security, national welfare, the people's livelihood, or the public interest. The State Council will formulate the specific scope and security protection measures for critical information infrastructure.

The State encourages operators of networks outside the [designated] critical information infrastructure systems to voluntarily participate in the critical information infrastructure protection system.

Article 32

In accordance with the duties and division of labor provided by the State Council, departments responsible for security protection work for critical information infrastructure are to separately compile and organize security implementation plans for their industry's or sector's critical information infrastructure, and to guide and supervise security protection efforts for critical information infrastructure operations.

Article 33

Those constructing critical information infrastructure shall ensure that it has the capability to support business stability and sustained operations, and ensure the synchronous planning, synchronous establishment, and synchronous application of security technical measures.

Article 34

In addition to the provisions of Article 21 of this Law, critical information infrastructure operators shall also perform the following security protection duties

- (1) Set up specialized security management bodies and persons responsible for security management, and conduct security background checks on those responsible persons and personnel in critical positions;
- (2) Periodically conduct cybersecurity education, technical training, and skills evaluations for employees;
- (3) Conduct disaster recovery backups of important systems and databases;
- (4) Formulate emergency response plans for cybersecurity incidents, and periodically organize drills;
- (5) Other duties provided by law or administrative regulations.

Article 35

Critical information infrastructure operators purchasing network products and services that might impact national security shall undergo a national security review organized by the State cybersecurity and informatization departments and relevant departments of the State Council.

Article 36

Critical information infrastructure operators purchasing network products and services shall follow relevant provisions and sign a security and confidentiality agreement with the provider, clarifying duties and responsibilities for security and confidentiality.

Article 37

Critical information infrastructure operators that gather or produce personal information or important data during operations within the mainland territory of the People's Republic of China, shall store it within mainland China. Where due to business requirements it is truly necessary to provide it outside the mainland, they shall follow the measures jointly formulated by the State cybersecurity and informatization departments and the relevant

departments of the State Council to conduct a security assessment; where laws and administrative regulations provide otherwise, follow those provisions.

Article 38

At least once a year, critical information infrastructure operators shall conduct an inspection and assessment of their networks' security and risks that might exist, either on their own or through retaining a cybersecurity services organization; CII operators should submit a cybersecurity report on the circumstances of the inspection and assessment as well as improvement measures, to be sent to the relevant department responsible for critical information infrastructure security protection efforts.

Article 39

State cybersecurity and informatization departments shall coordinate relevant departments in employing the following measures for critical information infrastructure security protection

- (1) Conduct spot testing of critical information infrastructure security risks, put forward improvement measures, and when necessary they can retain a cybersecurity services organization to conduct testing and assessment of cybersecurity risks;
- (2) Periodically organize critical information infrastructure operators to conduct emergency cybersecurity response drills, increasing the level, coordination, and capacity of responses to cybersecurity incidents.
- (3) Promote cybersecurity information sharing among relevant departments, critical information infrastructure operators, and also relevant research institutions and cybersecurity services organizations.
- (4) Provide technical support and assistance for cybersecurity emergency management and recovery, etc.

Chapter IV

Network Information Security

Article 40

Network operators shall strictly maintain the confidentiality of user information they collect and establish and complete user information protection systems.

Article 41

Network operators collecting and using personal information shall abide by the principles of legality, propriety, and necessity; they shall publish rules for collection and use, explicitly stating the purposes, means, and scope for collecting or using information, and obtain the consent of the persons whose data is gathered.

Network operators must not gather personal information unrelated to the services they provide; must not violate the provisions of laws, administrative regulations or agreements between the parties to gather or use personal information; and shall follow the provisions of laws, administrative regulations, and agreements with users to process personal information they have stored.

Article 42

Network operators must not disclose, tamper with, or destroy personal information they gather; and, absent the consent of the person whose information was collected, must not provide personal information to others. However, this is the case with the exception that information can be provided if after processing there is no way to identify a specific individual, and the identity cannot be recovered.

Network operators shall adopt technical measures and other necessary measures to ensure the security of personal information they gather and to prevent personal information from leaking, being destroyed, or lost. When the leak, destruction, or loss of personal information occurs, or might have occurred, remedial measures shall be immediately taken, and provisions followed to promptly inform

users and to make a report to the competent departments in accordance with regulations.

Article 43

Where individuals discover that network operators have violated the provisions of laws, administrative regulations, or agreements between the parties to gather or use their personal information, they have the right to demand the network operators delete their personal information; where discovering that personal information gathered or stored by network operators has errors, they have the right to demand the network operators make corrections. Network operators shall employ measures for deletions and corrections.

Article 44

Individuals or organizations must not steal or use other illegal methods to acquire personal information and must not unlawfully sell or unlawfully provide others with personal information.

Article 45

Departments lawfully having cybersecurity supervision and management duties, and their staffs, must keep strictly confidential personal information, private information, and commercial secrets that they learn of in performing their duties, and they must not leak, sell, or unlawfully provide it to others.

Article 46

All individuals and organizations shall be responsible for their use of websites and must not establish websites or communications groups for use in perpetrating fraud, imparting criminal methods, the creation or sale of prohibited or controlled items, or other unlawful activities, and websites must not be exploited to publish information related to perpetrating fraud, the creation or sale of prohibited or controlled items, or other unlawful activities.

Article 47

Network operators shall strengthen management of information published by users and, upon discovering information that the law

or administrative regulations prohibits the publication or transmission of, they shall immediately stop transmission of that information, employ handling measures such as deleting the information, prevent the information from spreading, save relevant records, and report to the relevant competent departments.

Article 48

Electronic information sent, or application software provided by any individual or organization, must not install malicious programs, and must not contain information that laws, and administrative regulations prohibit the publication or transmission of.

Electronic information distribution service providers, and application software download service providers, shall perform security management duties; where they know that their users have engaged in conduct provided for in the preceding paragraph, they shall employ measures such as stopping provision of services and removal of information or malicious programs; store relevant records; and report to the relevant competent departments.

Article 49

Network operators shall establish network information security complaint and reporting systems, publicly disclose information such as the methods for making complaints or reports, and promptly accept and handle complaints and reports relevant to network information security.

Network operators shall cooperate with cybersecurity and informatization departments and relevant departments in conducting implementation of supervision and inspections in accordance with the law.

Article 50

State cybersecurity and informatization departments and relevant departments will perform network information security supervision and management responsibilities in accordance with law; and where they discover the publication or transmission of

information which is prohibited by laws or administrative regulations, shall request that network operators stop transmission, employ disposition measures such as deletion, and store relevant records; for information described above that comes from outside the mainland People's Republic of China, they shall notify the relevant organization to adopt technical measures and other necessary measures to block transmission.

Chapter V Monitoring, Early Warning, and Emergency Response

Article 51

The State will establish a cybersecurity monitoring, early warning, and information communication system. The State cybersecurity and informatization departments shall do overall coordination of relevant departments to strengthen collection, analysis, and reporting efforts for cybersecurity information, and follow regulations for the unified release of cybersecurity monitoring and early warning information.

Article 52

Departments responsible for critical information infrastructure security protection efforts shall establish and complete cybersecurity monitoring, early warning, and information reporting systems for their respective industry or sector, and report cybersecurity monitoring and early warning information in accordance with regulations.

Article 53

State cybersecurity and informatization departments will coordinate with relevant departments to establish and complete mechanisms for cybersecurity risk assessment and emergency response efforts, formulate cybersecurity incident emergency response plans, and periodically organize drills.

Departments responsible for critical information infrastructure security protection efforts shall formulate cybersecurity incident emergency

response plans for their respective industry or sector, and periodically organize drills.

Cybersecurity incident emergency response plans shall rank cybersecurity incidents on the basis of factors such as the degree of damage after the incident occurs and the scope of impact and provide corresponding emergency response handling measures.

Article 54

When the risk of cybersecurity incidents increases, the relevant departments of people's governments at the provincial level and above shall follow the scope of authority and procedures provided, and employ the following measures on the basis of the characteristics of the cybersecurity risk and the damage it might cause

- (1) Require that relevant departments, institutions, and personnel promptly gather and report relevant information, and strengthen monitoring of the occurrence of cybersecurity risks;
- (2) Organize relevant departments, institutions, and specialist personnel to conduct analysis and assessment of information on the cybersecurity risk, and predict the likelihood of incident occurrence, the scope of impact, and the level of damage;
- (3) Issue cybersecurity risk warnings to the public and publish measures for avoiding or reducing damage.

Article 55

When a cybersecurity incident occurs, the cybersecurity incident emergency response plan shall be immediately initiated, an evaluation and assessment of the cybersecurity incident shall be conducted, network operators shall be requested to adopt technical and other necessary measures, potential security risks shall be removed, the threat shall be prevented from expanding, and warnings relevant to the public shall be promptly published.

Article 56

Where, while performing cybersecurity supervision and management duties, relevant departments of people's governments at the provincial level or above discover that networks have a relatively large security risk or the occurrence of a security incident, they may call in the legal representative or responsible party for the operator of that network to conduct interviews in accordance with the scope of authority and procedures provided. Network operators shall follow requirements to employ procedures, make corrections, and eliminate hidden dangers.

Article 57

Where sudden emergencies or production security accidents occur as a result of cybersecurity incidents, they shall be handled in accordance with the provisions the "Emergency Response Law of the People's Republic of China," the "Production Safety Law of the People's Republic of China," and other relevant laws and administrative regulations.

Article 58

To fulfil the need to protect national security and the social public order, and to respond to the requirements of major security incidents within the society, it is possible, as stipulated or approved by the State Council, to take temporary measures regarding network communications in a specially designated region, such as limiting such communications.

Chapter VI Legal Responsibility

Article 59

Where network operators do not perform cybersecurity protection duties provided for in Articles 21 and 25 of this Law, the competent departments will order corrections and give warnings; where corrections are refused, or it leads to harm to cybersecurity or other such consequences, a fine of between RMB 10,000 and 100,000 shall be levied; and the directly

responsible management personnel shall be fined between RMB 5,000 and 50,000.

Where critical information infrastructure operators do not perform cybersecurity protection duties as provided for in Articles 33, 34, 36, and 38 of this Law, the competent departments will order corrections and give warnings; where corrections are refused or it leads to harm to cybersecurity or other such consequences, a fine of between RMB 100,000 and 1,000,000 shall be levied; and the directly responsible management personnel shall be fined between RMB 10,000 and 100,000.

Article 60

Where Article 22 Paragraphs 1 or 2 or Article 48 Paragraph 1 of this Law are violated by any of the following conduct, the relevant competent departments shall order corrections and give warnings; where corrections are refused or it causes harm to cybersecurity or other consequences, a fine of between RMB 50,000 and 500,000 shall be levied; and the persons who are directly in charge shall be fined between RMB 10,000 and 100,000

- (1) Installing malicious programs;
- (2) Failure to immediately take remedial measures for security flaws or vulnerabilities that exist in products or services, or not informing users and reporting to the competent departments in accordance with regulations;
- (3) Unauthorized ending of the provision of security maintenance for their products or services.

Article 61

Network operators violating Article 24 Paragraph 1 of this Law in failing to require users to provide real identity information or providing relevant services to users who do not provide real identity information, are ordered to make corrections by the relevant competent department; where corrections are refused or the circumstances are serious, a fine of between RMB 50,000 and 500,000 shall be levied, and the relevant competent department may order a temporary suspension of operations, a suspension of business for

corrections, closing down of websites, cancellation of relevant operations permits, or cancellation of business licenses; persons who are directly in charge and other directly responsible personnel shall be fined between RMB 10,000 and 100,000.

Article 62

Where Article 26 of this Law is violated in carrying out cybersecurity certifications, testing, or risk assessments, or publishing cybersecurity information such as system vulnerabilities, computer viruses, cyber-attacks, or network incursions, corrections are to be ordered and a warning given; where corrections are refused or the circumstances are serious, a fine of between RMB 10,000 and 100,000 shall be imposed, and the relevant competent department may order a temporary suspension of operations, a suspension of business for corrections, closing down of websites, cancellation of relevant operations permits, or cancellation of business licenses; persons who are directly in charge and other directly responsible personnel shall be fined between RMB 5,000 and 50,000.

Article 63

Where Article 27 of this Law is violated in engaging in activities harming cybersecurity, or by providing specialized software or tools used in engaging in activities harming cybersecurity, or by providing others engaging in activities harming cybersecurity with assistance such as technical support, advertising and promotions, or payment of expenses, and where this does not constitute a crime, public security organizations shall confiscate unlawful gains and impose up to 5 days detention, and may levy a fine of between RMB 50,000 and 500,000; and where circumstances are serious, shall impose between 5 and 15 days detention, and may levy a fine of between 100,000 and 1,000,000 RMB.

Where units have engaged in the conduct of the preceding paragraph, public security organizations shall confiscate unlawful gains and levy a fine of between RMB 100,000 and 1,000,000, and the directly responsible persons in charge and other directly

responsible personnel shall be fined in accordance with the preceding paragraph.

Where Article 27 of this Law is violated, persons who receive public security administrative sanctions must not engage in cybersecurity management or key network operations positions for 5 years; those receiving criminal punishments will be subject to a lifetime ban on engaging in work in cybersecurity management and key network operations positions.

Article 64

Network operators, and network product or service providers violating Article 22 Paragraph 3 or Articles 41-43 of this Law by infringing on personal information that is protected in accordance with law, shall be ordered to make corrections by the relevant competent department and may, either independently or concurrently, be given warnings, be subject to confiscation of unlawful gains, and/or be fined between 1 to 10 times the amount of unlawful gains; where there are no unlawful gains, the fine shall be up to RMB 1,000,000, and a fine of between RMB 10,000 and 100,000 shall be given to persons who are directly in charge and other directly responsible personnel; where the circumstances are serious, the relevant competent department may order a temporary suspension of operations, a suspension of business for corrections, closing down of websites, cancellation of relevant operations permits, or cancellation of business licenses.

Where Article 44 of this Law is violated in stealing or using other illegal means to obtain, illegally sell, or illegally provide others with personal information, and this does not constitute a crime, public security organizations shall confiscate unlawful gains and levy a fine of between 1 and 10 times the amount of unlawful gains, and where there are no unlawful gains, levy a fine of up to RMB 1,000,000.

Article 65

Where critical information infrastructure operators violate Article 35 of this Law by using network products or services that have not had security inspections or did not pass security

inspections, the relevant competent department shall order the usage to stop and levy a fine in the amount of 1 to 10 times the purchase price; the persons who are directly in charge and other directly responsible personnel shall be fined between RMB 10,000 and 100,000.

Article 66

Where critical information infrastructure operators violate Article 37 of this Law by storing network data outside the mainland territory, or provide network data to those outside of the mainland territory, the relevant competent department shall order corrective measures, provide warning, confiscate unlawful gains, and levy fines between RMB 50,000 and 500,000; and may order a temporary suspension of operations, a suspension of business for corrective measures, closing down of websites, revocation of relevant operations permits, or cancellation of business licenses. Persons who are directly in charge and other directly responsible personnel shall be fined between RMB 10,000 and 100,000.

Article 67

Where Article 46 of this Law is violated by establishing a website or communications group used for the commission of illegal or criminal activities, or the network is used to publish information related to the commission of illegal or criminal activities, but a crime has not been committed, public security organizations shall impose up to 5 days detention and may levy a fine of between RMB 10,000 and 15,000; and where circumstances are serious, they may impose between 5 and 15 days detention, and may give a fine of between 50,000 and 500,000 RMB. They may also close websites and communications groups used for illegal or criminal activities.

Where units have engaged in conduct covered by the preceding paragraph, a fine of between RMB 100,000 and 500,000 shall be levied by public security organizations, and the principal responsible managers and other directly responsible personnel shall be fined in accordance with the preceding paragraph.

Article 68

Where network operators violate Article 47 of this Law by failing to stop the transmission of information for which transmission and publication are prohibited by laws or administrative regulations, failing to employ disposition measures such as deletion or failing to preserve relevant records, the relevant competent department shall order correction, provide warning, and confiscate unlawful gains; where correction is refused or circumstances are serious, fines between RMB 100,000 and 500,000 shall be imposed, and a temporary suspension of operations, a suspension of business to conduct correction, closing down of websites, cancellation of relevant operations permits, or cancellation of business licenses may be ordered; and persons who are directly in charge and other directly responsible personnel are fined between RMB 10,000 and 100,000.

Where electronic information service providers and application software download service providers do not perform their security management duties provided for in Paragraph 2 of Article 48 of this Law, punishment shall be in accordance with the provisions of the preceding paragraph.

Article 69

Network operators violating the provisions of this Law, who exhibit any of the following conduct, will be ordered to make corrections by the relevant competent departments; where corrections are refused, or the circumstances are serious, a fine of between RMB 50,000 and 500,000 shall be imposed, and directly responsible management personnel and other directly responsible personnel are to be fined between RMB 10,000 and 100,000

- (1) Not following the requirements of relevant departments to adopt disposition measures such as stopping dissemination or deleting information for which laws or administrative regulations prohibit publication or dissemination;
- (2) Refusal or obstruction of the competent departments in their lawful supervision and inspection;

- (3) Refusing to provide technical support and assistance to public security organs and state security organs.

Article 70

Publication or transmission of information prohibited by Article 12 Paragraph 2 of this Law or other laws or administrative regulations shall be punished in accordance with the provisions of the relevant laws and administrative regulations.

Article 71

When there is conduct violating the provisions of this Law, it shall be recorded in credit files and made public in accordance with relevant laws and administrative regulations.

Article 72

Where state organization government affairs network operators do not perform cybersecurity protection duties as provided by this Law, the organization at the level above or relevant organizations will order corrections; sanctions will be levied on the directly responsible managers and other directly responsible personnel.

Article 73

Where cybersecurity and informatization and other relevant departments violate the provisions of Article 30 of this Law by using personal information acquired while performing cybersecurity protection duties for other purposes, the directly responsible persons in charge and other directly responsible personnel shall be given sanctions.

Where cybersecurity and informatization departments and other relevant departments' personnel neglect their duties, abuse their authority, show favoritism, and it does not constitute a crime, sanctions will be imposed in accordance with law.

Article 74

Where violations of the provisions of this Law cause harm to others, civil liability is borne in accordance with law.

Where provisions of this Law are violated, constituting a violation of public order management, public order administrative sanctions will be imposed in accordance with law; where a crime is constituted, criminal responsibility will be pursued in accordance with law.

Article 75

Where foreign institutions, organizations, or individuals engage in attacks, intrusions, interference, damage, or other activities the endanger the critical information infrastructure of the People's Republic of China, and cause serious consequences, legal responsibility is to be pursued in accordance with the law; public security departments under the State Council and relevant departments may also decide to freeze institutional, organization, or individual assets or take other necessary punitive measures.

Chapter VII Supplementary Provisions

Article 76

The language below has the following meanings in this law

- (1) "Network" [网络, also "cyber"] refers to a system comprised of computers or other information terminals and related equipment that follows certain rules and procedures for information gathering, storage, transmission, exchange, and processing.
- (2) "Cybersecurity" [网络安全, also "network security"] refers to taking the necessary measures to prevent cyber-attacks, intrusions, interference, destruction, and unlawful use, as well as unexpected accidents, to place networks in a state of stable and reliable operation, as well as

ensuring the capacity for network data to be complete, confidential, and usable.

- (3) "Network operators" [网络运营者] refers to network owners, managers, and network service providers.
- (4) "Network data" [网络数据] refers to all kinds of electronic data collected, stored, transmitted, processed, and produced through networks.
- (5) "Personal information" [个人信息] refers to all kinds of information, recorded electronically or through other means, that taken alone or together with other information, is sufficient to identify a natural person's identity, including but not limited to natural persons' full names, birth dates, national identification numbers, personal biometric information, addresses, telephone numbers, and so forth.

Article 77

Protection of the operational security of networks that store or process information touching on national secrets shall follow this Law and shall also uphold the provisions of laws and administrative regulations pertaining to secrecy protection.

Article 78

The security protection rules for military networks are formulated by the Central Military Commission.

Article 79

This Law shall enter into effect June 1, 2017.