China Cybersecurity Law

Chapter I: General Provisions

Article 1: This law is formulated so as to ensure network security, to safeguard cyberspace sovereignty, national security and the societal public interest, to protect the lawful rights and interests of citizens, legal persons and other organizations, and to promote the healthy development of economic and social informatization.

Article 2: This law applies with respect to the construction, operation, maintenance and usage of networks, as well as network security supervision and management within the mainland territory of the People's Republic of China.

Article 3: The State persists in equally stressing network security and informatization development, and abides by the directives of active use, scientific development, management in accordance with law, and ensuring security; and advances the construction of network infrastructure and interconnectivity, encouraging innovation and application of network technology, supporting cultivation of network talent, establishing and completing systems to safeguard network security, and raising the capacity to protect network security.

Article 4: The State formulates and continuously improves a network security strategy, clarifies the fundamental requirements and primary goals of network security, and puts forward network security policies, work tasks, and procedures for key fields.

Article 5: The State takes measures for monitoring, preventing, and handling network security risks and threats arising both within and without the mainland territory of the People's Republic of China, protects critical information infrastructure against attacks, intrusions, interference and destruction; and pushes unlawful and criminal network activities in accordance with law, preserving cyberspace security and order.

Article 6: The State advocates sincere, honest, healthy and civilized network conduct; promoting dissemination of the core socialist values, adopting measures to raise the entire society's awareness and level of network security, and forming a good environment for the entire society to jointly participate in advancing network security.

Article 7: The State actively carries out international exchange 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; promoting the construction of a peaceful, secure, open and cooperative cyberspace; and establishing a network governance system that is multilateral, democratic and transparent.

Article 8: The State network information departments are responsible for comprehensively planning and coordinating network security efforts and related supervision and management efforts. The State Council Departments for telecommunications, public security, and other relevant organs, are responsible for network security protection, supervision and management efforts within the scope of their responsibilities, in accordance with the provisions of this Law, relevant laws and administrative regulations.

Network security 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 the laws and administrative regulations, obey social mores and obey commercial ethics, be honest and credible, perform obligations to protect network security, 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 in accordance with the provisions of laws and administrative regulations, and with the mandatory requirements of State standards; adopting technical measures and other necessary measures to safeguard network security and operational stability, effectively responding to network security incidents, preventing cybercrimes, and unlawful activity, and preserving the integrity, secrecy and usability of online data.

Article 11: Relevant network industry organizations are to, according to their Articles of Association, strengthen industry self-discipline, formulate behavioral network security norms, guide their members in strengthening network security protection according to the law, raise the protection levels of network security, 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 law; it promotes widespread network access, raises the level of network

services, it 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 network security, and must not use the network to engage in activities endangering national security, national honor and interests, inciting subversion of national sovereignty, the overturn of the socialist system, inciting separatism, undermining national unity, advocating terrorism or extremism, inciting ethnic hatred and ethnic discrimination, disseminating violent, obscene or sexual information, creating or disseminating false information to disrupt the economic or social order, as well as infringing 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, lawfully punishing the exploitation of the networks to engage in activities that endanger the psychological and physical well-being of minors, and providing a safe and healthy network environment for minors.

Article 14: All individuals and organizations have the right to report conduct endangering network security to the departments for network information, telecommunications, public security and so forth. Departments receiving reports shall promptly process them in accordance with law; where these do not fall within the responsibilities of that department, they shall promptly transfer the matters 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 the informant.

Chapter II: Support and Promotion of Network Security

Article 15: The State establishes and improves a system of network security standards. The State Council administrative department for standardization and other relevant State Council departments, on the basis of their individual responsibilities, organize the formulation and timely revision of relevant national and industry standards for network security 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 network security.

Article 16: The State Council and people's governments of provinces, autonomous regions and directly-governed municipalities shall make comprehensively plans; expand their input; support key network security technology industries and programs; support network security technology research and

development, application and popularization; spread safe and trustworthy network products and services; protect the intellectual property rights for network technologies; and support research and development institutions, schools of higher learning, and so forth to participate in State network security technology innovation programs.

Article 17: The State advances the establishment of socialized service systems for network security, encouraging relevant enterprises and institutions to carry out network security certifications, testing, risk assessment and other such security services.

Article 18: The State encourages the development of network data security protections and utilization technologies, advancing the opening of public data resources, and promoting technological innovation, and economic and social development.

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

Article 19: All levels' of people's governments and their relevant departments shall organize and carry out regular network security publicity and education, and guide and stimulate relevant units in doing network security publicity and education work well.

The mass media shall conduct targeted network security 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 network security-related education and training, and employs multiple methods to cultivate talent in network security, and promote interaction of network security professionals.

Chapter III: Network Operations Security

Section 1: Ordinary Provisions

Article 21: The State implements a tiered system of network security protections. Network operators shall perform the following security protection duties according to the requirements of the tiered network security protection system to ensure the network avoids interference, damage or unauthorized visits, and to prevent network data leaks, theft or falsification:

(1) Formulate internal security management systems and operating rules, determine persons responsible for network security, and implement network security protection responsibility;

(2) Adopt technological measures to prevent computer viruses, network attacks, network intrusions and other actions endangering network security;

(3) Adopt technological measures for monitoring and recording network operational statuses and network security incidents, and follow relevant provisions to store network logs for at least six months;

(4) Adopt measures such as data classification, back-up 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 must not terminate providing security maintenance during the time limits or period agreed on with clients.

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

Article 23: Critical network equipment and specialized network security products shall follow the national standards and mandatory requirements, and be safety certified by a qualified establishment or meet the requirements of a safety inspection, before being sold or provided. The state network information departments, together with the relevant departments of the State Council, formulate and release a catalog of critical network equipment and specialized network security products, and promote reciprocal recognition of safety certifications and security inspection results to avoid duplicative certifications and inspections.

Article 24: Network operators handling network access and domain 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 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 confirmation technologies, promoting reciprocal acceptance among different electronic identity confirmations.

Article 25: Network operators shall formulate emergency response plans for network security incidents, promptly addressing system vulnerabilities, computer viruses,network attacks, network incursions, and other such network security risks; and when network security incidents occur, immediately initiate the emergency response plan, adopt corresponding remedial measures, and report to the relevant competent departments in accordance with relevant provisions.

Article 26: Those carrying out network security certification, testing, risk assessment or other such activities, and publicly publishing network security 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 entry of others' networks, disruption of the normal function of others' networks, theft of network data or other activities endangering network security; must not provide programs, or tools specially used in network incursions, disrupting normal network functions and protection measures, stealing network data or other acts endangering network security; and where clearly knowing that others will engage in actions endangering network security, must not provide them with help such as technological support, advertisements and promotion, or paying expenses.

Article 28: Network operators shall provide technical support and assistance to public security organs' and state security organs; lawful activities preserving national security and investigating crimes.

Article 29: The State supports cooperation between network operators in areas such as gathering, analyzing, reporting and responding to network security information, increasing the security safeguard capacity of network operators.

Relevant industry organizations are to establish and complete mechanisms for regulation and coordination of network security for their industry, strengthen their analysis and assessment of network security, and periodically conduct risk warnings for members, and shall support and coordinate members' responses to network security risks.

Article 30: Information obtained by network information departments and relevant departments performing network security protection duties can only be used as necessary for the protection of network security, and must not be used in other ways.

Section 2: Operations Security for Critical Information Infrastructure

Article 31: The State implements key protection of public communication and information services, power, traffic, water, finance, public service, electronic governance and other critical information infrastructure that if destroyed, losing function or leaking data might seriously endanger national security, national welfare and the people's livelihood, or the public interest, on the basis of their tiered protection system. The State Council will formulate the specific scope and security protection measures for critical information infrastructure.

The State encourages operators of networks outside the critical information infrastructure 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 of critical information infrastructure, are to separately compile and organize implementation of security plans for that industry or field's critical information infrastructure, and guide and supervise security protection efforts for the critical information infrastructure operations.

Article 33: Construction of critical information infrastructure shall ensure that it has properties for supporting business stability and sustaining operations, and ensures that technical security measures are planned, established and used concurrently.

Article 34: In addition to the provisions of article 21 of this Law, critical information infrastructure operators shall also perform the following security protection obligations:

(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 network security education, technical training and skills evaluations for employees;

(3) Conduct disaster recovery backups of important systems and databases;

(4) Formulate emergency response plans for network security incidents, and periodically organize drills;

(5) Other obligations provided by law or administrative regulations.

Article 35: Critical information infrastructure information infrastructure operators purchasing network products and services that might impact national security shall go through a national security review

organized by the State network information 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: Personal information and other important data gathered or produced by critical information infrastructure operators 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 network information departments and the relevant departments of the State Council to conduct a security assessment; but 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 exists either personally, or through retaining a network security services establishment; and submit a network security 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 network information 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 may retain a network security service establishment to conduct testing and assessment of network security risks;

(2) Periodically organize critical information infrastructure operators to conduct emergency network security response drills, increasing the level, coordination, and capacity of responses to network security incidents.

(3) Promote network security information sharing among relevant departments, critical information infrastructure operators, and also relevant research institutions, network security services establishments.

(4) Provide technical support and assistance for network security emergency management and recovery and so forth.

Chapter IV: Network Information Security

Article 40: Network operators shall strictly maintain the confidentiality of user information they collect, 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; make public rules for collection and use, explicitly stating the purposes, means, and scope for collecting or using information, and obtaining the consent of the person 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. Except, however, where it has been processed so that the specific individual is unidentifiable and cannot be recovered.

Network operators shall adopt technological measures and other necessary measures to ensure the security of personal information they gather, and prevent personal information from leaking, being destroyed or lost. When the leak, destruction or loss of personal information occur, or might occur, remedial measures shall be immediately taken, and provisions followed to promptly inform users and to make 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 request 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 request 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 network security supervision and management duties, and their staffs, must keep personal information, private information and commercial secrets, which they learn of in performing their duties, strictly confidential, and 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 it, to prevent the information from spreading, save relevant records, and report it 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; and where they know that their users have conduct provided for in the preceding paragraph, shall stop providing services and employ measures such as removal, 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 network information departments and relevant departments lawful implementation of supervision and inspections.

Article 50: The State network information departments and relevant departments perform network information security supervision and management responsibilities in accordance with law; and where discovering information the release or transmission of which is prohibited by laws or administrative regulations, shall request the network operators stop transmission, employ disposition measures such as deletion, and store relevant records; for information described above that comes from outside mainland People's Republic of China, they shall notify the relevant organization to adopt technological measures and other necessary measures to block transmission.

Chapter V: Monitoring, Early Warnings, and Emergency Responses

Article 51: The state establishes systems for network security monitoring, early warnings, information communication. The State network information departments shall do overall coordination of relevant departments to strengthen collection, analysis and reporting efforts for network security information,

and follow regulations for the unified release of network security monitoring and early warning information.

Article 52: Departments responsible for critical information infrastructure security protection efforts shall establish and complete that industry or that field's network security monitoring, early warning and information reporting systems, and report network security monitoring and early warning information in accordance with regulations.

Article 53: The State network information departments coordinates relevant departments' establishment and completion of mechanisms for network security risk assessment and emergency response efforts, formulates network security incident emergency response plans, and periodically organizes drills.

Departments responsible for critical information infrastructure security protection efforts shall formulate that industry or that field's network security incident emergency response plans, and periodically organize drills.

Network security incident emergency response plans shall rank network security incidents on the basis of factors such as the degree of threat after the incident occurs and the scope of impact, and provide corresponding emergency response handling measures.

Article 54: When the risk of network security 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 network security risk's characteristics and the harms it might cause:

(1) Require that relevant departments, institutions and personnel promptly gather and report relevant information, and strengthen monitoring of the occurrence of network security risks;

(2) Organize relevant departments, institutions and specialist personnel to conduct analysis and assessment of information on the network security risk, and predict the likelihood of an incident's occurrence, the scope of its impact and its level of harm;

(3) Publish network security risk warnings to the public, and publish measures for avoiding or reducing harms.

Article 55: On occurrence of a network security incident, the network security incident emergency response plan shall be immediately initiated, an evaluation and assessment of the network security incident shall be conducted, network operators shall be requested to adopt technological and other

necessary measures, potential security risks shall be removed, the threat shall be prevented from growing, and warnings relevant to the public shall be promptly published.

Article 56: Where, while performing network security 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 legally-designated representative or responsible party for the operator of that network for a talking to, 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 safety accidents occur as a result of network security 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 fulfill the need to protect national security and social public order, and respond to major social security incidents, the State Council, or the governments of provinces, autonomous regions and municipalities with approval by the State Council, may take temporary measures regarding network communications in certain regions, such as restricting it.

Chapter VI: Legal Responsibility

Article 59: Where network operators do not perform network security 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 endangerment of network security or other such consequences, a fine of between RMB 10,000 and 100,000 is given; and the directly responsible management personnel are fined between RMB 5,000 and 50,000.

Where critical information infrastructure operators do not perform network security protection duties 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 endangerment of network security or other such consequences, a fine of between RMB 100,000 and 1,000,000 is give; and the directly responsible management personnel is fined between RMB 10,000 and 100,000.

Article 60: Where paragraphs 1 or 2 of article 22, or paragraph 1 of article 48 of this law are violated by any of the following conduct, the relevant competent departments order corrections and give warnings; where corrections are refused or it causes endangerment of network security or other consequences, a fine of between RMB 50,000 and 500,000 is given; and the persons who are directly in charge are 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 this to the competent departments in accordance with provisions;

(3) Unauthorized ending of the provision of security maintenance for their products or services.

Article 61: Network operators violating paragraph 1 of articles 24 of this law in failing to require users to provide truthful identity information or providing relevant services to users who do not provide truthful 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 is given, 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 are fined between RMB 10,000 and 100,000.

Article 62: Where Article 26 of this law is violated in carrying out network security certifications, testing or risk assessments, or publishing network security information such as system vulnerabilities, computer viruses, network 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 is given, 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 are fined between RMB 5,000 and 50,000.

Article 63: Where Article 27 of this law is violated in engaging in activities endangering national security, or by providing specialized software or tools used in engaging in activities endangering national security, or by providing others engaging in activities endangering network security with assistance such as technical support, advertising and promotions or payment of expenses; and a crime is no constituted, the public security organs are to confiscate unlawful gains and impose up to 5 days detention, and may give a fine of between 50,000 and 50,000 RMB; and where circumstances are serious, impose between 5 and 15 days detention, and may give a fine of between 100,000 and 1,00,000 RMB.

Where units have the conduct of the preceding paragraph, the public security organs are to confiscate unlawful gains and give a fine of up to RMB 100,000, and the directly responsible persons in charge and other directly responsible personnel are 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 key network security management or network operations positions for 5 years; those receiving criminal punishments must not take on work in key network security management and network operations positions for their lifetimes.

Article 64: Network operators, and network product or service providers, violating paragraph 3 of article 22 and Articles 41-43 of this Law by infringing on personal information that is protected in accordance with law, are ordered to make corrections by the relevant competent department and may, either independently or concurrently, be given warnings, confiscation of unlawful gains, and/or fined between 1 to 10 times the amount of unlawful gains; where there are no unlawful gains the fine is up to RMB 1,000,000 and a fine of between RMB 10,000 and 100,000 is given to persons who are directly in charge and other directly responsible personnel; where the circumstances are serious, a fine of between RMB 50,000 and 500,000 is given, 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.

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 it does not constitute a crime, the public security organs confiscate unlawful gains and give a fine of between 1 and 10 times the amount of unlawful gains, and where there are no unlawful gains, give 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 safety inspections or did not pass safety inspections, the relevant competent departments order the usage to stop, and give 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 are 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 individuals or organizations outside of the mainland territory without going through a security assessment, the relevant competent department orders corrections, gives warnings, confiscates unlawful gains, gives fines between RMB 50,000 and 500,000, and may order a temporary suspension of operations, a suspension of business for corrections, 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 are 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 networks are used to publish information related to the commission of illegal or criminal activities; and a crime is not constituted, the public security organs are to impose up to 5 days detention, and may give a fine of between 10,000 and 15,000 RMB; and where circumstances are serious, impose between 5 and 15 days detention, and may give a fine of between 50,000 and 500,000 RMB. Close websites and social groups used for illegal or criminal activities.

Where units have the conduct of the preceding paragraph, a fine of up to 100,000 yuan is given by the public security organs, and the principle responsible managers and other directly responsible personnel are 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 that laws of administrative regulations prohibit the publication or transmission of, failing to employ disposition measures such as deletion or failure to preserve relevant records, the relevant competent department orders corrections, gives warnings, and confiscates unlawful gains; where corrections are refused or circumstances are serious, fines between RMB 50,000 and 500,000 are given, and 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 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 is 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 50,000 and RMB 500,000 is given and directly responsible management personnel and other directly responsible personnel are to be fined between RMB 10,000 and RMB 100,000:

(1) Not following the requirements of relevant departments to adopt disposition measures such as stopping dissemination or deleting information that laws or administrative regulations prohibit the public or dissemination of;

(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 that paragraph 2 of Article 12 of this Law or other laws or administrative regulations prohibit the publication or transmission of, is punished in accordance with the provisions of the relevant laws and administrative regulations.

Article 71: Where there is conduct violating the provisions of this law, record it in the credit archives and make it public in accordance with relevant laws and administrative regulations.

Article 72: Where state organ government affairs network operators do not perform network security protection duties as provided by this law, the organ at the level above or relevant department will order corrections; sanctions are given to the directly responsible managers and other directly responsible personnel.

Article 73: Where network and other relevant departments violate the provisions of article 30 of this law by using personal information acquired while performing network security protection duties for other purposes, the directly responsible persons in charge and other directly responsible personnel are given sanctions.

Where network information departments and other relevant departments personnel neglect their duties, abuse their authority, or distort the law for personal gain, and it does not constitute a crime, sanctions are given 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 security management, public security administrative sanctions are given in accordance with law; where a crime is constituted, criminal responsibility is pursued in accordance with law.

Article 75: Where foreign institutions, organizations, or individuals engage in attacks, intrusions, interference, damage or other activities endangering the critical information infrastructure of the People's Republic of China, and cause serious consequences, legal responsibility is to be pursued in accordance with law; the Ministry of Public Security under the State Council and relevant departments may also decide to freeze assets or take other necessary punitive measures.

Chapter VII: Supplementary Provisions

Article 76: The language below has the following meanings in this law:

(1) "Networks" refers to systems comprised of computers or other information terminals and related equipment that follow certain rules and procedures for information gathering, storage, transmission, exchange and processing.

(2) "Network security" refers to taking necessary measures to prevent network attacks, incursions, interference, destruction and their unlawful use, as well as unexpected accidents; to put the 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" refers to network owners, managersm and network service providers.

(4) "Network data" refers to all kinds of electronic data collected, stored, transmitted, processed, and produced through networks.

(5) "personal information" 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, identification numbers, personal biometric information, addresses, telephone numbers, and so forth.

Article 77: Operations security protections for storing and processing networks involving state secret information, shall follow this Law and shall also uphold laws and administrative regulations on secrecy.

Article 78: Security protections for military network are formulated by the Central Military Commission.

Article 79: This Law shall go into effect June 1, 2017.

Перевод: chinalawtranslate.com