PRC Cybersecurity Law

Dan Young Business Consultancy — www.danyoungcpa.com

Unofficial English translation prepared for reference only. The official Chinese text prevails.

Contents

Table of Contents 1

Chapter I — General Provisions 1

Chapter II — Support and Promotion of Cybersecurity 3

Chapter III — Network Operations Security 3

Chapter IV — Network Information Security 6

Chapter V — Monitoring, Early Warning and Emergency Response 8

Chapter VI — Legal Liability 9

Chapter VII — Supplementary Provisions 11

Adopted at the 24th Session of the Standing Committee of the Twelfth National People's Congress on November 7, 2016
Effective: June 1, 2017

Table of Contents

- Chapter I — General Provisions
- Chapter II — Support and Promotion of Cybersecurity
- Chapter III — Network Operations Security
- Chapter IV — Network Information Security
- Chapter V — Monitoring, Early Warning and Emergency Response
- Chapter VI — Legal Liability
- Chapter VII — Supplementary Provisions

Chapter I — General Provisions

Article 1 — This Law is enacted for the purposes of ensuring cybersecurity, safeguarding cyberspace sovereignty and national security, protecting the lawful rights and interests of citizens, legal persons, and other organizations, and promoting the sound development of the informatization of the economy and society.

Article 2 — This Law shall apply to the construction, operation, maintenance, and use of networks within the territory of the People's Republic of China, as well as the supervision and administration of cybersecurity.

Article 3 — The state shall adhere to the principle of attaching equal importance to cybersecurity and informatization development, follow the guidelines of active utilization, scientific development, lawful

Source: https://www.danyoungcpa.com/cybersecurity-law-peoples-republic-of-china-full-text-en/

administration, and ensured security, advance the construction of network infrastructure and interconnectivity, encourage innovation and application of network technologies, establish sound cybersecurity guarantee systems, and enhance cybersecurity protection capabilities.

Article 4 — The state shall formulate and continuously improve cybersecurity strategies, specify the basic requirements and main objectives for ensuring cybersecurity, and put forward cybersecurity policies, work tasks, and measures in key areas.

Article 5 — The state shall adopt measures to monitor, defend against, and handle cybersecurity risks and threats originating from within or outside the territory of the People's Republic of China, protect critical information infrastructure from attacks, intrusions, interference, and destruction, punish illegal and criminal online activities in accordance with the law, and maintain security and order in cyberspace.

Article 6 — The state shall advocate honest, trustworthy, healthy, and civilized online conduct, promote the dissemination of core socialist values, and adopt measures to raise the cybersecurity awareness and protection capability of the whole society, and create a wholesome online environment.

Article 7 — The state shall actively carry out international exchanges and cooperation in cyberspace governance, research and development of network technologies, formulation of technical standards, combating illegal and criminal online activities, and other fields, promote the building of a peaceful, secure, open, and cooperative cyberspace, and establish a multilateral, democratic, and transparent system for internet governance.

Article 8 — The national cyberspace administration authority shall be responsible for the overall planning and coordination of cybersecurity work and the related supervision and administration. The competent telecommunications authority under the State Council, the public security authority, and other relevant authorities shall, in accordance with the provisions of this Law and relevant laws and administrative regulations, be responsible for the protection of cybersecurity, supervision, and administration within the scope of their respective functions and duties. Cybersecurity protection, supervision, and administration functions and duties of the relevant departments of the local people's governments at or above the county level shall be determined in accordance with the relevant provisions of the state.

Article 9 — Network operators shall, when carrying out business and service activities, comply with laws and administrative regulations, respect social morality and business ethics, be honest and trustworthy, fulfill their cybersecurity protection obligations, accept supervision by the government and the public, and assume social responsibility.

Article 10 — When constructing or operating a network or providing services through a network, technical measures and other necessary measures shall be taken in accordance with the provisions of laws and administrative regulations and the mandatory requirements of national standards to ensure the secure and stable operation of the network, effectively respond to cybersecurity incidents, prevent illegal and criminal online activities, and safeguard the integrity, confidentiality, and availability of network data.

Article 11 — Network-related industry organizations shall, in accordance with their articles of association, strengthen industry self-discipline, formulate codes of conduct for cybersecurity, guide their members in strengthening cybersecurity protection, raise the level of cybersecurity protection, and promote the sound development of the industry.

Article 12 — The state shall protect the rights of citizens, legal persons, and other organizations to use networks in accordance with the law, and promote the widespread use of network technologies and the improvement of the level of network services, so as to enable the public to share the fruits of the development of cybersecurity. The state shall ensure the lawful and orderly free flow of network information in accordance with the law. No individual or organization may use a network to engage in activities that endanger national security, national honor, or national interests; incite subversion of state power or the

overthrow of the socialist system; incite secession or undermine national unity; advocate terrorism or extremism; advocate ethnic hatred or ethnic discrimination; disseminate violent or obscene information; fabricate or disseminate false information to disrupt economic and social order; or infringe upon the reputation, privacy, intellectual property rights, or other lawful rights and interests of others.

Article 13 — The state shall support research and development of network products and services that are conducive to the healthy growth of minors, punish online activities that harm the physical and mental health of minors in accordance with the law, and provide a safe and healthy online environment for minors.

Article 14 — Every individual and organization shall have the right to report to the cyberspace administration authority, the telecommunications authority, the public security authority, and other relevant authorities any acts that endanger cybersecurity. The authorities receiving the reports shall handle the reports in a timely manner in accordance with the law; where the matter does not fall within the scope of their functions and duties, the authority shall promptly transfer it to the authority with jurisdiction. The relevant authorities shall keep confidential the information on the reporters and protect the lawful rights and interests of the reporters.

Chapter II — Support and Promotion of Cybersecurity

Article 15 — The state shall establish and improve a system of cybersecurity standards. The standardization administrative authority under the State Council and other relevant authorities under the State Council shall, in accordance with their respective functions and duties, organize the formulation and timely revision of relevant national and industry standards for cybersecurity administration and the security of network products, services, and operations. The state shall support enterprises, research institutions, institutions of higher learning, and network-related industry organizations in participating in the formulation of national and industry standards for cybersecurity.

Article 16 — The State Council and the people's governments of provinces, autonomous regions, and municipalities directly under the Central Government shall make overall plans, increase investment, support key cybersecurity technology industries and projects, support the research, development, and application of secure and reliable network products and services, protect the intellectual property rights of network technologies, and support enterprises, research institutions and institutions of higher learning in participating in national cybersecurity technology innovation projects.

Article 17 — The state shall promote the development of a cybersecurity social service system and encourage relevant enterprises and institutions to provide security services such as cybersecurity certification, testing, and risk assessment.

Article 18 — The state shall encourage the development of network data security protection and utilization technologies, promote the opening of public data resources, and promote technological innovation and economic and social development. The state shall support innovative cybersecurity management methods and the use of new network technologies to enhance the level of cybersecurity protection.

Article 19 — People's governments at all levels and their relevant departments shall organize and carry out regular cybersecurity publicity and education, and guide and urge relevant units to do a good job in cybersecurity publicity and education. The mass media shall conduct targeted cybersecurity publicity and education for the general public.

Article 20 — The state shall support enterprises and institutions of higher learning, vocational schools, and other education and training institutions in carrying out cybersecurity-related education and training, adopt multiple methods to cultivate cybersecurity talents, and promote the exchange of cybersecurity talents.

Chapter III — Network Operations Security

Section 1 — General Provisions

Article 21 — The state shall implement a tiered cybersecurity protection system. Network operators shall, in accordance with the requirements of the tiered cybersecurity protection system, fulfill the following security protection obligations to ensure that the network is free from interference, disruption, or unauthorized access, and to prevent network data from being leaked, stolen, or tampered with: (1) formulate internal security management systems and operating procedures, determine persons responsible for cybersecurity, and implement cybersecurity protection responsibilities; (2) adopt technical measures to prevent computer viruses, network attacks, network intrusions, and other acts endangering cybersecurity; (3) adopt technical measures to monitor and record network operation status and cybersecurity incidents, and retain relevant network logs for not less than six months in accordance with the provisions; (4) adopt measures such as data classification, backup of important data, and encryption; and (5) perform other obligations provided for by laws and administrative regulations.

Article 22 — Network products and services shall comply with the mandatory requirements of relevant national standards. Providers of network products and services shall not install malware; where they discover that there are security defects, vulnerabilities, or other risks in their network products or services, they shall immediately adopt remedial measures, promptly inform users of the situation in accordance with the provisions, and report the same to the relevant competent authority. Providers of network products and services shall provide continuous security maintenance for their products and services; they shall not terminate the provision of security maintenance within the prescribed time limit or the time limit agreed upon with the user. Where network products or services have the function of collecting user information, the providers shall expressly indicate the same to the users and obtain their consent; where personal information of users is involved, the providers 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, in accordance with the mandatory requirements of relevant national standards, pass security certification by a qualified institution or meet the requirements of a security inspection before being sold or provided. The national cyberspace administration authority shall, in conjunction with the relevant authorities under the State Council, formulate and publish a catalogue of critical network equipment and specialized cybersecurity products and promote reciprocal recognition of security certification and security inspection results to avoid duplicate certification and inspection.

Article 24 — When network operators handle network access and domain name registration services for users, handle fixed-line telephone and mobile phone network access procedures, or provide information release, instant messaging, and other services to users, they shall require users to provide their real identity information when signing agreements with users or confirming the provision of services. Where users do not provide their real identity information, network operators shall not provide them with the relevant services. The state shall implement a strategy for trusted identities in cyberspace, support research and development of secure and convenient electronic identity authentication technologies, and promote mutual recognition among different electronic identity authentication technologies.

Article 25 — Network operators shall formulate emergency response plans for cybersecurity incidents to promptly handle system vulnerabilities, computer viruses, network attacks, network intrusions, and other security risks; where any incident endangering cybersecurity occurs, the network operator shall immediately initiate the emergency response plan, take corresponding remedial measures, and report the same to the relevant competent authority in accordance with the provisions.

Article 26 — Where relevant information on the commission of crimes is disseminated through a network, or activities endangering cybersecurity such as computer viruses, network attacks, or network intrusions are carried out, network operators shall, upon discovery, take technical measures such as stopping the transmission and eliminating the relevant information to prevent the spread of the information, keep relevant records, and report the same to the relevant competent authority. Where network operators, in the

performance of their cybersecurity protection obligations, discover illegal or criminal information, they shall report the same to the relevant competent authority in accordance with the law and shall not delete or modify the relevant information without authorization.

Article 27 — No individual or organization may engage in any activity that endangers cybersecurity, such as illegally intruding into another person's network, interfering with the normal functions of another person's network, or stealing network data; nor may they provide programs or tools specifically used for activities endangering cybersecurity, such as network intrusion, interference with normal network functions and protective measures, or stealing network data; where they know that another person is engaged in activities endangering cybersecurity, they shall not provide the person with technical support, advertising promotion, payment and settlement services, or any other assistance.

Article 28 — Network operators shall provide technical support and assistance to the public security authorities and national security authorities in safeguarding national security and investigating crimes in accordance with the law.

Article 29 — The state shall support cooperation among network operators in the collection, analysis, notification, and emergency response of cybersecurity information, so as to enhance the security protection capabilities of network operators. Relevant industry organizations shall establish and improve mechanisms and rules for cybersecurity protection norms and coordination within their industries, strengthen the analysis and assessment of cybersecurity risks, periodically carry out risk warnings to their members, and support and assist their members in responding to cybersecurity risks.

Article 30 — Information obtained by the cyberspace administration authority and relevant authorities in the performance of their cybersecurity protection functions and duties shall only be used for the needs of cybersecurity protection and shall not be used for other purposes.

Section 2 — Critical Information Infrastructure Operations Security

Article 31 — The state shall, on the basis of the tiered cybersecurity protection system, provide key protection for critical information infrastructure in important industries and fields such as public communications and information services, energy, transportation, water conservancy, finance, public services, and e-government, as well as other critical information infrastructure that, if damaged, disabled, or subject to data leakage, may seriously endanger national security, the national economy and people's livelihood, or the public interest. The specific scope of and security protection measures for critical information infrastructure shall be formulated by the State Council. The state shall encourage network operators other than those operating critical information infrastructure to voluntarily participate in the critical information infrastructure protection system.

Article 32 — The authorities responsible for the security protection of critical information infrastructure shall, in accordance with the functions and duties prescribed by the State Council, organize and carry out, on their own or by entrusting a specialized institution, security inspections and assessments of the critical information infrastructure under their respective charge, identify the hidden security risks, and urge the operators of the critical information infrastructure to make rectification within a prescribed time limit, at least once a year.

Article 33 — When constructing critical information infrastructure, the operators shall ensure that it has the performance to support the business stability and continuous operation, and guarantee the simultaneous design, simultaneous construction, and simultaneous operation of security technical measures. The operators shall establish and improve the relevant internal management system for cybersecurity, specify the persons responsible for cybersecurity, and implement cybersecurity protection responsibilities.

Article 34 — In addition to fulfilling the obligations provided for in Article 21 of this Law, operators of critical information infrastructure shall also fulfill the following security protection obligations: (1) set up specialized security management institutions and persons responsible for security management, and conduct security

background checks on the responsible persons and personnel in key positions; (2) periodically conduct cybersecurity education, technical training, and skill assessments for employees; (3) conduct disaster recovery backups of important systems and databases; (4) formulate emergency response plans for cybersecurity incidents and conduct regular drills; and (5) perform other obligations provided for by laws and administrative regulations.

Article 35 — When operators of critical information infrastructure procure network products and services that may affect national security, they shall pass a national security review organized by the national cyberspace administration authority in conjunction with the relevant authorities under the State Council.

Article 36 — When operators of critical information infrastructure procure network products and services, they shall enter into a security confidentiality agreement with the provider in accordance with the provisions, specifying the security and confidentiality obligations and responsibilities of the provider, and supervise the provider's performance of the obligations.

Article 37 — Personal information and important data collected and generated by operators of critical information infrastructure during their operations within the territory of the People's Republic of China shall be stored within the territory of the People's Republic of China. Where such information or data needs to be provided overseas due to business needs, a security assessment shall be conducted in accordance with the measures formulated by the national cyberspace administration authority in conjunction with the relevant authorities under the State Council, unless otherwise provided for by laws or administrative regulations.

Article 38 — Operators of critical information infrastructure shall conduct, on their own or by entrusting a specialized cybersecurity service institution, at least once a year, inspections and assessments of the security of their networks and the possible risks that may exist, and shall submit the inspection and assessment results and the corresponding improvement measures to the authorities responsible for the security protection of critical information infrastructure.

Article 39 — The national cyberspace administration authority shall coordinate with the relevant authorities in taking the following measures for the security protection of critical information infrastructure: (1) conducting spot checks and testing of the security risks of critical information infrastructure, proposing improvement measures, and when necessary, entrusting a specialized cybersecurity service institution to conduct inspections and assessments of the security risks existing in the network; (2) periodically organizing operators of critical information infrastructure to conduct emergency cybersecurity drills to enhance the level of response to cybersecurity incidents and coordination and cooperation capabilities; (3) promoting cybersecurity information sharing among the relevant authorities, operators of critical information infrastructure, relevant research institutions, and specialized cybersecurity service institutions; and (4) providing technical support and assistance for emergency response to cybersecurity incidents and recovery of network functions.

Chapter IV — Network Information Security

Article 40 — Network operators shall strictly keep confidential the user information they collect, and shall establish and improve the user information protection system.

Article 41 — When network operators collect and use personal information, they shall abide by the principles of lawfulness, legitimacy, and necessity, disclose the rules for collection and use, expressly indicate the purpose, method, and scope of collection and use of information, and obtain the consent of the persons whose information is collected. Network operators shall not collect personal information irrelevant to the services they provide, and shall not collect or use personal information in violation of laws, administrative regulations, or the agreement between the parties; they shall process and keep personal information in accordance with the provisions of laws, administrative regulations, and the agreement with the users.

Article 42 — Network operators shall not disclose, tamper with, or destroy the personal information they collect; they shall not provide personal information to others without the consent of the persons whose information is collected. However, this shall not apply where the information has been processed and cannot be used to identify a specific person and cannot be restored. Network operators shall adopt technical measures and other necessary measures to ensure the security of the personal information they collect, and to prevent the information from being leaked, destroyed, or lost. Where a leak, destruction, or loss of personal information occurs or may occur, remedial measures shall be taken immediately, and the users shall be notified in a timely manner in accordance with the provisions, and the matter shall be reported to the relevant competent authority.

Article 43 — Where an individual discovers that a network operator has collected or used his or her personal information in violation of laws, administrative regulations, or the agreement between the parties, the individual shall have the right to request the network operator to delete his or her personal information; where an individual discovers that the personal information collected or stored by a network operator contains errors, the individual shall have the right to request the network operator to make corrections. Network operators shall adopt measures to delete or correct the information.

Article 44 — No individual or organization may steal or obtain personal information by other illegal means, nor shall they sell or illegally provide personal information to others.

Article 45 — Authorities and their staff members that have lawfully obtained personal information in the performance of their cybersecurity supervision and administration functions and duties shall keep such personal information strictly confidential, and shall not disclose, sell, or illegally provide the same to others.

Article 46 — No individual or organization shall be responsible for sending commercial electronic information to the fixed-line telephones, mobile phones, or personal e-mail addresses of others without their consent or request, or where the recipients have expressly refused to receive such information.

Article 47 — Network operators shall strengthen the administration of information published by their users. Where they discover any information that is prohibited from being published or transmitted by laws or administrative regulations, they shall immediately stop the transmission of such information, take measures such as elimination to prevent the spread of the information, keep relevant records, and report the same to the relevant competent authority.

Article 48 — Electronic information sent by any individual or organization, or application software provided by them, shall not be set up with malware, and shall not contain information that is prohibited from being published or transmitted by laws or administrative regulations. Where an electronic information distribution service provider or an application software download service provider discovers that any of the circumstances as set out in the preceding paragraph exist, it shall immediately stop providing services, take measures such as elimination, keep relevant records, and report the same to the relevant competent authority.

Article 49 — Network operators shall establish systems for accepting and handling complaints and reports regarding network information security, and shall publish the methods for making complaints and reports, and shall promptly accept and handle complaints and reports. The competent cyberspace administration authority and relevant authorities shall supervise network operators' acceptance and handling of complaints and reports in accordance with the law.

Article 50 — The national cyberspace administration authority and relevant authorities shall, in accordance with the law, perform their functions and duties of supervision and administration of network information security. Where they discover any information that is prohibited from being published or transmitted by laws or administrative regulations, they shall require the network operator to stop the transmission of the information, adopt measures such as elimination to prevent the spread of the information, and keep relevant records; where the above information originates from outside the territory of the People's Republic of China,

they shall notify the relevant institution to adopt technical measures and other necessary measures to block the dissemination of the information.

Chapter V — Monitoring, Early Warning and Emergency Response

Article 51 — The state shall establish a cybersecurity monitoring, early warning, and information notification system. The national cyberspace administration authority shall coordinate with the relevant authorities in strengthening the collection, analysis, and notification of cybersecurity information, and shall, in accordance with the provisions, uniformly release cybersecurity monitoring and early warning information.

Article 52 — The authorities responsible for the security protection of critical information infrastructure shall establish and improve the cybersecurity monitoring, early warning, and information notification systems within their respective industries and fields, and shall report cybersecurity monitoring and early warning information in accordance with the provisions.

Article 53 — The national cyberspace administration authority shall coordinate with the relevant authorities in establishing and improving mechanisms for cybersecurity risk assessment and emergency response, formulating emergency response plans for cybersecurity incidents, and organizing regular drills. The authorities responsible for the security protection of critical information infrastructure shall formulate emergency response plans for cybersecurity incidents within their respective industries and fields, and shall organize regular drills. Emergency response plans for cybersecurity incidents shall classify cybersecurity incidents on the basis of factors such as the degree of harm caused and the scope of impact after the occurrence of the incidents, and shall provide for corresponding emergency response measures.

Article 54 — Where the likelihood of a cybersecurity incident increases, the relevant authorities of the people's governments at or above the provincial level shall, in accordance with the prescribed authority and procedures and based on the characteristics and possible harm of the cybersecurity risk, take the following measures: (1) requiring the relevant authorities, institutions, and personnel to collect and report relevant information in a timely manner and strengthen monitoring of the occurrence of cybersecurity risks; (2) organizing the relevant authorities, institutions, and professionals to analyze and assess the information on cybersecurity risks and predict the likelihood of the occurrence of the incident, the scope of impact, and the degree of harm; and (3) releasing early warning information on cybersecurity risks to the public, and issuing measures for avoidance or reduction of harm.

Article 55 — Where a cybersecurity incident occurs, the emergency response plan for cybersecurity incidents shall be immediately initiated, investigation and assessment of the cybersecurity incident shall be conducted, the network operator shall be required to adopt technical measures and other necessary measures to eliminate potential security hazards, prevent the expansion of the harm, and promptly release warning information related to the public.

Article 56 — Where the relevant authorities of the people's governments at or above the provincial level, in the performance of their cybersecurity supervision and administration functions and duties, discover that there are major security risks or security incidents in the network, they may, in accordance with the prescribed authority and procedures, conduct interviews with the legal representative or principal responsible person of the network operator. The network operator shall, in accordance with the requirements of the interview, adopt measures to make rectification and eliminate the hidden dangers.

Article 57 — Where any emergency incident or production safety accident occurs due to cybersecurity reasons, it shall be handled in accordance with the provisions of the Law of the People's Republic of China on Emergency Response, the Law of the People's Republic of China on Production Safety, and other relevant laws and administrative regulations.

Article 58 — Where it is necessary to take temporary measures such as restricting network communications in specific areas in order to protect national security and public order and deal with major social security

emergencies, such measures shall be taken upon a decision made or an approval obtained by the State Council in accordance with the law.

Chapter VI — Legal Liability

Article 59 — Where a network operator fails to fulfill the cybersecurity protection obligations provided for in Articles 21 and 25 of this Law, the relevant competent authority shall order it to make corrections and give it a warning. Where it refuses to make corrections or the circumstances are serious, a fine of not less than RMB 10,000 but not more than RMB 100,000 shall be imposed, and a fine of not less than RMB 5,000 but not more than RMB 50,000 shall be imposed on the directly responsible person in charge. Where the operator of critical information infrastructure fails to fulfill the cybersecurity protection obligations provided for in Articles 33, 34, 36, and 38 of this Law, the relevant competent authority shall order it to make corrections and give it a warning. Where it refuses to make corrections or the circumstances are serious, a fine of not less than RMB 100,000 but not more than RMB 1,000,000 shall be imposed, and a fine of not less than RMB 10,000 but not more than RMB 100,000 shall be imposed on the directly responsible person in charge.

Article 60 — Where a network operator violates the provisions of the first paragraph of Article 22 or Article 48 of this Law by committing any of the following acts, the relevant competent authority shall order it to make corrections and give it a warning; where it refuses to make corrections or the circumstances are serious, a fine of not less than RMB 50,000 but not more than RMB 500,000 shall be imposed, and a fine of not less than RMB 10,000 but not more than RMB 100,000 shall be imposed on the directly responsible person in charge: (1) installing malware; (2) failing to immediately adopt remedial measures for security defects, vulnerabilities, or other risks in its products or services, or failing to promptly inform users and report to the relevant competent authority in accordance with the provisions; or (3) terminating the provision of security maintenance for its products or services without authorization.

Article 61 — Where a network operator violates the provisions of the first paragraph of Article 24 of this Law by failing to require users to provide real identity information, or provides the relevant services to users who do not provide real identity information, the relevant competent authority shall order it to make corrections; where it refuses to make corrections or the circumstances are serious, a fine of not less than RMB 50,000 but not more than RMB 500,000 shall be imposed, and a fine of not less than RMB 10,000 but not more than RMB 100,000 shall be imposed on the directly responsible person in charge, and the relevant competent authority may order it to suspend the relevant business, suspend business for rectification, close down the website, or revoke the relevant business permit or business license.

Article 62 — Where a network operator violates the provisions of Article 26 of this Law by failing to handle illegal or criminal information as required, the relevant competent authority shall order it to make corrections and give it a warning; where it refuses to make corrections or the circumstances are serious, a fine of not less than RMB 50,000 but not more than RMB 500,000 shall be imposed, and a fine of not less than RMB 10,000 but not more than RMB 100,000 shall be imposed on the directly responsible person in charge.

Article 63 — Where a network operator violates the provisions of Article 27 of this Law by engaging in activities endangering cybersecurity or providing programs or tools for such activities, or provides technical support, advertising promotion, payment and settlement services, or other assistance to activities endangering cybersecurity, if the violation does not constitute a crime, the public security authority shall confiscate the illegal gains and impose detention of not more than five days, and may impose a fine of not less than RMB 50,000 but not more than RMB 500,000; where the circumstances are relatively serious, detention of not less than five days but not more than 15 days shall be imposed, and a fine of not less than RMB 100,000 but not more than RMB 1,000,000 may also be imposed. Where an entity commits the acts provided for in the preceding paragraph, the public security authority shall confiscate the illegal gains and impose a fine of not less than RMB 100,000 but not more than RMB 1,000,000 on the entity, and shall impose punishment on the directly responsible person in charge and other directly responsible persons in

Source: https://www.danyoungcpa.com/cybersecurity-law-peoples-republic-of-china-full-text-en/

accordance with the provisions of the preceding paragraph. Where a network operator violates the provisions of Article 27 of this Law by obtaining information such as electronic data illegally obtained by others, the relevant competent authority shall, in accordance with the provisions, impose punishment.

Article 64 — Where a network operator or a provider of network products or services violates the provisions of the third paragraph of Article 22 or Articles 41 through 43 of this Law by infringing upon the lawful rights and interests of personal information, the relevant competent authority shall order it to make corrections and may, in accordance with the circumstances, additionally give a warning, confiscate illegal gains, impose a fine of not less than one time but not more than ten times the illegal gains, or, where there are no illegal gains, impose a fine of not more than RMB 1,000,000, and impose a fine of not less than RMB 10,000 but not more than RMB 100,000 on the directly responsible person in charge and other directly responsible persons; where the circumstances are serious, the relevant competent authority may order it to suspend the relevant business, suspend business for rectification, close down the website, or revoke the relevant business permit or business license. Where a network operator violates the provisions of Article 44 of this Law by stealing or obtaining personal information by other illegal means, or selling or illegally providing personal information to others, if the violation does not constitute a crime, the public security authority shall confiscate the illegal gains and impose a fine of not less than one time but not more than ten times the illegal gains, or, where there are no illegal gains, impose a fine of not more than RMB 1,000,000.

Article 65 — Where an operator of critical information infrastructure violates the provisions of Article 35 of this Law by using network products or services that have not passed a security review or have failed the security review, the relevant competent authority shall order it to stop using the products or services and impose a fine of not less than one time but not more than ten times the purchase amount; and a fine of not less than RMB 10,000 but not more than RMB 100,000 shall be imposed on the directly responsible person in charge and other directly responsible persons.

Article 66 — Where an operator of critical information infrastructure violates the provisions of Article 37 of this Law by storing network data overseas or providing network data overseas, the relevant competent authority shall order it to make corrections, give it a warning, confiscate its illegal gains, and impose a fine of not less than RMB 50,000 but not more than RMB 500,000, and may order it to suspend the relevant business, suspend business for rectification, close down the website, or revoke the relevant business permit or business license; and a fine of not less than RMB 10,000 but not more than RMB 100,000 shall be imposed on the directly responsible person in charge.

Article 67 — Where a network operator violates the provisions of Article 47 of this Law by failing to stop the transmission of information prohibited from being published or transmitted by laws or administrative regulations, failing to adopt measures such as elimination, or failing to keep relevant records, the relevant competent authority shall order it to make corrections and give it a warning, confiscate its illegal gains; where it refuses to make corrections or the circumstances are serious, a fine of not less than RMB 100,000 but not more than RMB 500,000 shall be imposed, and a fine of not less than RMB 10,000 but not more than RMB 100,000 shall be imposed on the directly responsible person in charge and other directly responsible persons; where the circumstances are serious, the relevant competent authority may order it to suspend the relevant business, suspend business for rectification, close down the website, or revoke the relevant business permit or business license.

Article 68 — Where a network operator violates the provisions of Article 47 of this Law by failing to properly keep or providing to others information that may be suspected of being illegal or criminal as released, transmitted, or disseminated by users, the relevant competent authority shall order it to make corrections and give it a warning; where it refuses to make corrections or the circumstances are serious, a fine of not less than RMB 50,000 but not more than RMB 500,000 shall be imposed, and a fine of not less than RMB 10,000 but not more than RMB 100,000 shall be imposed on the directly responsible person in charge and other directly responsible persons.

Article 69 — Where a network operator violates the provisions of this Law by committing any of the following acts, the relevant competent authority shall order it to make corrections; where it refuses to make corrections or the circumstances are serious, a fine of not less than RMB 50,000 but not more than RMB 500,000 shall be imposed, and a fine of not less than RMB 10,000 but not more than RMB 100,000 shall be imposed on the directly responsible person in charge: (1) failing to submit information such as real identity information as required; (2) failing to fulfill the obligation of network operation security protection; or (3) failing to publish the methods for accepting and handling complaints and reports or failing to timely accept and handle complaints and reports.

Article 70 — Where information prohibited from being published or transmitted by laws or administrative regulations is published or transmitted, the relevant competent authority shall, in accordance with the provisions of relevant laws and administrative regulations, impose punishment.

Article 71 — Where a network operator violates the provisions of this Law and the violation constitutes a crime, criminal liability shall be pursued in accordance with the law.

Article 72 — Where a network operator that is a state organ fails to fulfill its cybersecurity protection obligations as provided for in this Law, the authority at a higher level or the relevant authority shall order it to make corrections; and sanctions shall be imposed on the directly responsible person in charge and other directly responsible persons in accordance with the law.

Article 73 — Where the cyberspace administration authority or any relevant authority fails to perform its cybersecurity protection functions and duties as provided for in this Law, abuses its power, or neglects its duties, sanctions shall be imposed on the directly responsible person in charge and other directly responsible persons in accordance with the law. Where any staff member of the cyberspace administration authority or any relevant authority neglects his or her duties, engages in malpractice for personal gain, or abuses his or her power, if the violation does not constitute a crime, sanctions shall be imposed in accordance with the law.

Article 74 — Where any act violates the provisions of this Law and causes damage to others, civil liability shall be borne in accordance with the law. Where any act violates the provisions of this Law and constitutes a violation of public security administration, public security administration penalties shall be imposed in accordance with the law; where a crime is constituted, criminal liability shall be pursued in accordance with the law.

Article 75 — Where an overseas institution, organization, or individual engages in activities endangering the cybersecurity of critical information infrastructure within the territory of the People's Republic of China, such as attacking, intruding into, interfering with, or destroying critical information infrastructure, and causes serious consequences, legal liability shall be pursued in accordance with the law; the public security authority under the State Council and the relevant authorities may decide to freeze the property of such institution, organization, or individual or take other necessary sanctions.

Chapter VII — Supplementary Provisions

Article 76 — For the purposes of this Law, the following terms shall have the following meanings: (1) "network" means a system composed of computers or other information terminals and related equipment for collecting, storing, transmitting, exchanging, and processing information in accordance with certain rules and procedures; (2) "cybersecurity" means taking necessary measures to prevent attacks, intrusions, interference, destruction, and illegal use of networks, as well as accidents occurring in networks, so as to keep networks in a state of stable and reliable operation, and ensure the integrity, confidentiality, and usability of network data; (3) "network operator" means the owner or administrator of a network or the network service provider; (4) "network data" means all kinds of electronic data collected, stored, transmitted, processed, and generated through a network; and (5) "personal information" means all kinds of information

recorded electronically or by other means that can identify the identity of a natural person individually or in combination with other information, including but not limited to the natural person's name, date of birth, identification certificate number, biometric information, address, telephone number, e-mail address, health information, and whereabouts information.

Article 77 — The security protection of the operation and storage of information involving state secrets on networks shall be governed by the provisions of the Law of the People's Republic of China on Guarding State Secrets and other relevant laws and administrative regulations.

Article 78 — The security protection of military networks shall be separately provided for by the Central Military Commission.

Article 79 — This Law shall come into force as of June 1, 2017.

Disclaimer: This English translation is provided for reference purposes only. While every effort has been made to ensure accuracy, the official Chinese text shall prevail in all legal matters. Dan Young Business Consultancy makes no warranty, express or implied, as to the accuracy, completeness, or fitness for any particular purpose of this translation. Users should consult qualified legal professionals for advice on specific cybersecurity compliance matters. The translation reflects the law as adopted on November 7, 2016, and may not incorporate subsequent amendments or interpretations.