

Cybersecurity Law of the PRC

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 Operation Security	4
Section 1 — General Provisions	4
Section 2 — Critical Information Infrastructure Operation Security	5
Chapter IV — Network Information Security	6
Chapter V — Monitoring, Early Warning, and Emergency Response	7
Chapter VI — Legal Liability	8
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 Operation 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, and public interests, protecting the lawful rights and interests of citizens, legal persons, and other organizations, and promoting the healthy development of economic and social informatization.

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

Article 3 — The state shall adhere to the principles of equally emphasizing cybersecurity and informatization development, comply with the guidelines of active use, scientific development, lawful management, and ensuring security, promote the construction of network infrastructure and interconnection, encourage innovation and application of network technology, establish and improve 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, tasks, and measures for key areas.

Article 5 — The state shall adopt measures to monitor, defend against, and deal with cybersecurity risks and threats originating from within and outside the territory of the PRC, protect critical information infrastructure from attacks, intrusions, interference, and damage, punish illegal and criminal cyber activities in accordance with the law, and maintain security and order in cyberspace.

Article 6 — The state shall advocate honest, trustworthy, wholesome, and civilized cyber conduct, promote the dissemination of the core values of socialism, and adopt measures to improve the cybersecurity awareness and competence of the whole society, so as to form a favorable environment in which the whole society jointly participates in promoting cybersecurity.

Article 7 — The state shall actively carry out international exchanges and cooperation in cyberspace governance, research and development of cybersecurity technologies, formulation of cybersecurity standards, combating cyber crimes and other areas, promote the building of a peaceful, secure, open, and cooperative cyberspace, and establish a multilateral, democratic, and transparent system of cyberspace governance.

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

Article 9 — When conducting business and service activities, network operators shall abide by laws and administrative regulations, respect social morals, abide by business ethics, be honest and trustworthy, perform cybersecurity protection obligations, accept supervision by the government and the public, and assume social responsibilities.

Article 10 — Where the construction or operation of a network or the provision of services through a network shall obtain administrative licensing in accordance with the provisions of laws and administrative regulations, such obligations shall be complied with. Network operators providing services shall provide services in accordance with the provisions of laws and administrative regulations and the mandatory requirements of national standards.

Article 11 — Network-related industry organizations shall, in accordance with their articles of association and in compliance with industry norms, strengthen industry self-discipline, guide their members in strengthening cybersecurity protection, and improve the level of cybersecurity protection.

Article 12 — The state shall protect the rights of citizens, legal persons, and other organizations to use networks in accordance with the law, promote the widespread availability of network access, improve the level of network services, make secure and convenient network services available, and ensure the lawful, orderly, and free flow of network information. No individual or organization shall use the network to endanger

national security, national honor, or national interests, to incite subversion of state power or overthrow of the socialist system, to incite secession of the country or undermine national unity, to promote terrorism or extremism, to promote ethnic hatred or ethnic discrimination, to disseminate violence, obscenity, or sexual information, to fabricate and disseminate false information to disrupt economic and social order, or to infringe upon the reputation, privacy, intellectual property, or other lawful rights and interests of others.

Article 13 — The state shall support the research and development of network products and services conducive to the healthy growth of minors, and shall punish the acts of endangering the physical and mental health of minors by using networks in accordance with the law, so as to provide a safe and healthy network environment for minors.

Article 14 — Any individual or organization shall have the right to report to the cyberspace administration authority, the telecommunications authority, the public security authority, or other relevant authorities about acts endangering cybersecurity. The authorities receiving such reports shall handle them in a timely manner in accordance with the law; where the reports do not fall within the scope of their duties, they shall promptly transfer them to the authority with jurisdiction over such matters. The relevant authorities shall keep confidential the information on the reporters and protect their lawful rights and interests.

Chapter II — Support and Promotion of Cybersecurity

Article 15 — The state shall establish and improve a system of cybersecurity standards. The competent standardization administrative department under the State Council and other relevant departments under the State Council shall, in accordance with their respective duties, organize the formulation and timely revision of relevant national standards and industry standards for cybersecurity management and the security of network products, services, and operations. The state shall support enterprises, research institutions, higher education institutions, network-related industry organizations, and other relevant entities 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 cybersecurity technologies, promote secure and trustworthy network products and services, protect the intellectual property of network technologies, and support enterprises, research institutions, higher education institutions, and other relevant entities in participating in national cybersecurity technology innovation projects.

Article 17 — The state shall promote the building of a socialized service system for cybersecurity, and encourage relevant enterprises and institutions to carry out certifications, testing, risk assessment, and other security services for cybersecurity.

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 the innovation of cybersecurity management methods and the application of new technologies.

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

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

Chapter III — Network Operation Security

Section 1 — General Provisions

Article 21 — The state shall implement a system of graded cybersecurity protection. Network operators shall, in accordance with the requirements of the graded cybersecurity protection system, perform the following security protection obligations to ensure that the network is protected against interference, damage, or unauthorized access, and to prevent network data leakage, theft, or tampering: (1) formulating internal security management systems and operating procedures, determining the persons responsible for cybersecurity, and implementing cybersecurity protection responsibilities; (2) adopting technical measures to prevent computer viruses, network attacks, network intrusions, and other acts endangering cybersecurity; (3) adopting technical measures to monitor and record network operation status and cybersecurity incidents, and retaining network logs for not less than six months in accordance with the provisions; (4) adopting measures such as data classification, backup of important data, and encryption; (5) performing other obligations provided for by laws and administrative regulations.

Article 22 — Network products and services shall comply with the mandatory requirements of the relevant national standards. Providers of network products and services shall not install malware. Where a provider discovers any risk such as a security defect or vulnerability in its network products or services, it shall immediately adopt remedial measures, promptly notify users in accordance with the provisions, and report to the relevant competent departments. 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 time limit specified in the provisions or as agreed upon by the parties. Where network products or services have the function of collecting user information, their providers shall expressly indicate the same to users and obtain their consent; and shall comply with the provisions of this Law and relevant laws and administrative regulations on the protection of citizens' personal information where the collection of such personal information is involved.

Article 23 — Critical network equipment and specialized cybersecurity products shall, in accordance with the mandatory requirements of the relevant national standards, pass security certification by qualified institutions or pass a security test before they are sold or provided. The national cyberspace administration authority shall, in conjunction with the relevant departments under the State Council, formulate and publish catalogues of critical network equipment and specialized cybersecurity products, and promote the mutual recognition of security certification and security test results, so as to avoid repeated certification and testing.

Article 24 — Network operators providing network access and domain name registration services for users, handling network access formalities such as fixed-line telephone or mobile phone, or providing information publication and instant messaging services for users shall, when signing agreements with users or confirming the provision of services, require users to provide truthful identity information. Where users do not provide truthful identity information, network operators shall not provide them with the relevant services. The state shall implement a credible identity strategy for cyberspace, and support research and development of secure and convenient electronic identity authentication technologies and promote the mutual recognition between different electronic identity authentication technologies.

Article 25 — Network operators shall formulate emergency response plans for cybersecurity incidents to promptly deal with security risks such as system vulnerabilities, computer viruses, network attacks, and network intrusions; and when an incident endangering cybersecurity occurs, they shall immediately activate the emergency response plan, adopt corresponding remedial measures, and report to the relevant competent departments in accordance with the provisions.

Article 26 — When carrying out activities such as cybersecurity certification, security testing, and security risk assessment, or publishing cybersecurity information such as system vulnerabilities, computer viruses, network attacks, and network intrusions to the public, enterprises and institutions shall comply with the

relevant state provisions.

Article 27 — No individual or organization shall engage in activities endangering 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 shall they provide programs or tools specifically used for engaging in activities endangering cybersecurity, such as network intrusion, interfering with the normal functions and protective measures of networks, or stealing network data; where they clearly know that another person engages in activities endangering cybersecurity, they shall not provide technical support, advertising promotion, payment and settlement services, or any other assistance to such person.

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

Article 29 — The state supports cooperation among network operators in areas such as the collection, analysis, reporting, and emergency handling of cybersecurity information, so as to improve the cybersecurity protection capabilities of network operators. Relevant industry organizations shall establish and improve cybersecurity protection norms and cooperation mechanisms for their respective industries, strengthen the analysis and assessment of cybersecurity risks, regularly provide risk warnings to members, and support and assist members in dealing with cybersecurity risks.

Article 30 — Information obtained by the cyberspace administration authority and relevant departments in the course of performing their cybersecurity protection duties may only be used for the need of safeguarding cybersecurity, and shall not be used for other purposes.

Section 2 — Critical Information Infrastructure Operation Security

Article 31 — The state shall, on the basis of the graded cybersecurity protection system, provide special protection for critical information infrastructure in important industries and fields such as public communications and information services, energy, transport, water conservancy, finance, public services, e-government affairs, and national defense science, technology, and industry, as well as other critical information infrastructure that, once damaged, loss of function, or data leakage occurs, may seriously endanger national security, the national economy, people's livelihood, or public interests. The specific scope of critical information infrastructure and security protection measures shall be formulated by the State Council. The state shall encourage network operators outside the scope of critical information infrastructure to voluntarily participate in the critical information infrastructure protection system.

Article 32 — The departments responsible for the security protection of critical information infrastructure shall, in accordance with the provisions of the State Council, formulate and organize the implementation of security plans for the critical information infrastructure of their respective industries and fields, and guide and supervise the security protection of the operation of critical information infrastructure.

Article 33 — Those constructing critical information infrastructure shall ensure that the critical information infrastructure has the performance of supporting the stability and continuous operation of the business and shall ensure that security technical measures are planned, constructed, and used concurrently.

Article 34 — In addition to the obligations provided for in Article 21 of this Law, critical information infrastructure operators shall also perform the following security protection obligations: (1) setting up special security management bodies and persons in charge of security management, and conducting security background checks on such persons in charge and personnel in key positions; (2) periodically conducting education on cybersecurity, technical training, and skill assessments for practitioners; (3) conducting disaster recovery backup of important systems and databases; (4) formulating emergency response plans for cybersecurity incidents and conducting drills periodically; (5) other obligations provided for by laws and administrative regulations.

Article 35 — Where critical information infrastructure operators purchase network products and services that may affect national security, they shall undergo a national security review organized by the national cyberspace administration authority in conjunction with the relevant departments under the State Council.

Article 36 — When critical information infrastructure operators purchase network products and services, they shall, in accordance with the provisions, conclude security and confidentiality agreements with the providers, specifying the security and confidentiality obligations and responsibilities of the providers and supervising the same.

Article 37 — Critical information infrastructure operators shall store within the territory of the PRC the personal information and important data collected and generated during their operations within the territory of the PRC. Where it is truly necessary to provide such information and data abroad 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 departments under the State Council; where laws or administrative regulations provide otherwise, such provisions shall apply.

Article 38 — Critical information infrastructure operators shall, on their own or by entrusting a cybersecurity service institution, conduct at least one annual inspection and assessment of the security of their networks and the risks that may exist, and submit the inspection and assessment results and the improvement measures taken to the relevant departments responsible for the security protection of critical information infrastructure.

Article 39 — The national cyberspace administration authority shall coordinate the relevant departments to adopt the following measures for the security protection of critical information infrastructure: (1) conducting spot checks and tests of the security risks of critical information infrastructure, putting forward improvement measures, and entrusting cybersecurity service institutions to conduct security risk assessment of the networks when necessary; (2) regularly organizing critical information infrastructure operators to conduct emergency response drills for cybersecurity incidents to improve the level of response to cybersecurity incidents and the capability of collaborative coordination; (3) promoting cybersecurity information sharing among relevant departments, critical information infrastructure operators, relevant research institutions, and cybersecurity service institutions; (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 user information protection systems.

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

Article 42 — Network operators shall not disclose, tamper with, or destroy the personal information they have collected; they shall not provide personal information to others without the consent of the person whose information is collected. However, this shall not apply where the specific individual cannot be identified after processing and the information cannot be restored. Network operators shall adopt technical measures and other necessary measures to ensure the security of the personal information they have collected and prevent information leakage, damage, or loss. Where personal information is or may be leaked, damaged, or lost,

remedial measures shall be immediately taken, users shall be promptly notified in accordance with the provisions, and a report shall be made to the relevant competent departments.

Article 43 — Where an individual discovers that a network operator has collected or used his personal information in violation of the provisions of laws or administrative regulations or the agreement between the parties, he shall have the right to request the network operator to delete his personal information; where he discovers that the personal information of his that has been collected or stored by a network operator is erroneous, he shall have the right to request the network operator to make corrections. The network operator shall adopt measures to delete the information or make corrections.

Article 44 — No individual or organization shall steal or otherwise illegally obtain personal information, nor shall they illegally sell or provide personal information to others.

Article 45 — Departments legally vested with cybersecurity supervision and administration duties and their staff shall keep strictly confidential the personal information, privacy, and trade secrets they come to know in the course of performing their duties, and shall not disclose, sell, or illegally provide the same to others.

Article 46 — Any individual or organization shall be responsible for their behavior when using a network, and shall not set up websites or communication groups for the purpose of committing fraud, teaching criminal methods, producing or selling prohibited or controlled goods, or engaging in other illegal or criminal activities, nor shall they use a network to publish information involving the commission of fraud, the production or sale of prohibited or controlled goods, or other illegal or criminal activities.

Article 47 — Network operators shall strengthen the management of information published by their users; where they discover information that is prohibited by laws or administrative regulations from being published or transmitted, they shall immediately cease the transmission of such information, adopt measures such as deletion, prevent its dissemination, retain relevant records, and report the same to the relevant competent departments.

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 by laws or administrative regulations from being published or transmitted. Where an electronic information transmission service provider or application software download service provider discovers any act specified in the preceding paragraph, it shall cease the provision of services, adopt measures such as deletion, prevent the dissemination of the information, retain relevant records, and report the same to the relevant competent departments.

Article 49 — Network operators shall establish network information security complaint and reporting systems, publish information such as the methods for making complaints and reports, and promptly accept and handle complaints and reports about network information security.

Article 50 — The national cyberspace administration authority and relevant departments shall lawfully perform their duties of supervision and administration of network information security, and where they discover information that is prohibited by laws or administrative regulations from being published or transmitted, shall require network operators to cease the transmission, adopt measures such as deletion, and retain relevant records; and where the above-mentioned information originates from outside the territory of the PRC, they shall notify the relevant institutions to adopt technical measures and other necessary measures to block the transmission of such information.

Chapter V — Monitoring, Early Warning, and Emergency Response

Article 51 — The state shall establish a cybersecurity monitoring, early warning, and information reporting system. The national cyberspace administration authority shall coordinate the relevant departments in strengthening the collection, analysis, and reporting of cybersecurity information, and shall, in accordance

with the provisions, uniformly publish cybersecurity monitoring and early warning information.

Article 52 — The departments responsible for the security protection of critical information infrastructure shall establish and improve cybersecurity monitoring and early warning and information reporting systems for 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 the relevant departments in establishing and improving cybersecurity risk assessment and emergency response work mechanisms, formulating emergency response plans for cybersecurity incidents, and organizing drills periodically. The departments responsible for the security protection of critical information infrastructure shall formulate emergency response plans for cybersecurity incidents for their respective industries and fields, and organize drills periodically. Emergency response plans for cybersecurity incidents shall grade cybersecurity incidents on the basis of factors such as the degree of harm caused by the incident after it occurs and the scope of impact.

Article 54 — When a cybersecurity incident is likely to occur or the probability of occurrence of a cybersecurity risk increases, the people's governments at the provincial level and above and their relevant departments shall, in accordance with the prescribed authority and procedures and based on the characteristics of the cybersecurity risk and the possible harm, adopt the following measures: (1) requiring the relevant departments, institutions, and personnel to promptly collect and report relevant information, and strengthen the monitoring of the occurrence and development of the cybersecurity risk; (2) organizing the relevant departments, institutions, and professionals to analyze and assess the cybersecurity risk information and predict the probability of the incident, the scope of impact, and the intensity of the harm; (3) issuing a public early warning to the public and issuing measures for avoiding and mitigating the harm.

Article 55 — When a cybersecurity incident occurs, the emergency response plan for cybersecurity incidents shall be immediately activated, the cybersecurity incident shall be investigated and an assessment made, and the network operators shall be required to adopt technical measures and other necessary measures to eliminate potential security risks, prevent the expansion of harm, and promptly release to the public early warning information relevant to the public.

Article 56 — When performing cybersecurity supervision and administration duties, the relevant departments of the people's governments at the provincial level and above may interview the legal representative or principal responsible person of a network operator where it is discovered that there are relatively large security risks in the network. The network operator shall adopt measures to rectify and eliminate the risks as required.

Article 57 — Where a cybersecurity incident occurs as a result of a sudden event or production safety accident, the relevant provisions of the Emergency Response Law of the PRC, the Work Safety Law of the PRC, and other relevant laws and administrative regulations shall apply.

Article 58 — Where it is necessary to take temporary measures such as restricting network communications in order to safeguard national security and public order and deal with major sudden social security incidents, such measures may be adopted in accordance with the relevant provisions of the State Council and upon the decision or approval of the State Council.

Chapter VI — Legal Liability

Article 59 — Where a network operator fails to perform the cybersecurity protection obligations provided for in Articles 21 and 25 of this Law, the relevant competent department shall order correction and issue a warning; where correction is refused or the consequences of endangering cybersecurity or other circumstances arise, a fine of not less than RMB 10,000 but not more than RMB 100,000 shall be imposed; the directly responsible person in charge shall be fined not less than RMB 5,000 but not more than RMB

50,000.

Article 60 — Where a network operator commits any of the following acts in violation of the provisions of Article 24, paragraph 1 of this Law, the relevant competent department shall order correction; where correction is refused or the circumstances are serious, a fine of not less than RMB 50,000 but not more than RMB 500,000 shall be imposed; the directly responsible person in charge and other directly responsible persons shall be fined not less than RMB 10,000 but not more than RMB 100,000: (1) failing to require users to provide truthful identity information when providing services such as network access and domain name registration, or when handling network access formalities for users, or when providing services such as information publication and instant messaging to users; (2) providing relevant services to users who fail to provide truthful identity information.

Article 61 — Where a network operator violates the provisions of Article 24, paragraph 1 of this Law and fails to require users to provide truthful identity information, it shall be punished in accordance with the provisions of the preceding Article. Where a network operator provides network access or domain name registration services for users who do not provide truthful identity information, it shall be ordered to make correction by the relevant competent department and a fine of not less than RMB 50,000 but not more than RMB 500,000 may be imposed.

Article 62 — Where a network operator violates the provisions of Article 26 of this Law by carrying out activities such as cybersecurity certification, security testing, and security risk assessment, or publishing cybersecurity information such as system vulnerabilities, computer viruses, network attacks, and network intrusions, the relevant competent department shall order correction and issue a warning; where correction is refused or the circumstances are serious, a fine of not less than RMB 10,000 but not more than RMB 100,000 shall be imposed; the directly responsible person in charge and other directly responsible persons shall be fined not less than RMB 5,000 but not more than RMB 50,000.

Article 63 — Where a person violates the provisions of Article 27 of this Law, engages in activities endangering cybersecurity, or provides programs or tools specifically used for engaging in activities endangering cybersecurity, or provides technical support, advertising promotion, payment and settlement services, or other assistance to another person engaging in activities endangering cybersecurity where he clearly knows of the same, if no crime is constituted, the public security organ shall confiscate his illegal gains and place him in detention for 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, he shall be placed in detention for not less than five days but not more than 15 days, and may be fined not less than RMB 100,000 but not more than RMB 1,000,000. Where an entity commits any of the acts specified in the preceding paragraph, the public security organ shall confiscate its illegal gains and impose a fine of not less than RMB 100,000 but not more than RMB 1,000,000, and the directly responsible person in charge and other directly responsible persons shall be punished in accordance with the provisions of the preceding paragraph. Where a person violates the provisions of Article 27 of this Law and receives administrative penalties, he shall not hold key positions in cybersecurity management or network operations for five years; where a person receives criminal penalties, he shall be prohibited for life from holding key positions in cybersecurity management or network operations.

Article 64 — Where a network operator or provider of network products or services violates the provisions of Article 22, paragraphs 2 and 3, or Articles 41 through 43 of this Law by infringing upon the personal information that is protected in accordance with the law, the relevant competent department shall order correction and may, on the basis of the circumstances, unilaterally or concurrently issue a warning, confiscate the illegal gains, impose a fine of not less than one time but not more than 10 times the illegal gains, and where there are no illegal gains, impose a fine of not more than RMB 1,000,000; the directly responsible person in charge and other directly responsible persons shall be fined not less than RMB 10,000 but not more than RMB 100,000; where the circumstances are serious, the relevant competent department

may order the suspension of the relevant business, suspension of business for rectification, close the website, revoke the relevant business permit, or revoke the business license. Where any violation of the provisions of Article 44 of this Law occurs, the public security organ shall confiscate the illegal gains and impose a fine of not less than one time but not more than 10 times the illegal gains; where there are no illegal gains, a fine of not more than RMB 1,000,000 shall be imposed.

Article 65 — Where a critical information infrastructure operator violates the provisions of Articles 35, 36, 37, and 38 of this Law by using network products or services that have not undergone a security review or failing to undergo a security assessment, the relevant competent department shall order the operator to cease using them and impose a fine of not less than one time but not more than 10 times the purchase amount; the directly responsible person in charge and other directly responsible persons shall be fined not less than RMB 10,000 but not more than RMB 100,000.

Article 66 — Where a critical information infrastructure operator violates the provisions of Article 37 of this Law by storing network data outside the territory or providing network data abroad, the relevant competent department shall order correction, issue a warning, confiscate the illegal gains, and impose a fine of not less than RMB 50,000 but not more than RMB 500,000, and may order the suspension of the relevant business, suspension of business for rectification, close the website, or revoke the relevant business permit or business license; the directly responsible person in charge and other directly responsible persons shall be fined not less than RMB 10,000 but not more than RMB 100,000.

Article 67 — Where a network operator violates the provisions of Articles 46 and 47 of this Law, the relevant competent department shall order correction and issue a warning, and confiscate the illegal gains; where correction is refused 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 the relevant competent department may order the suspension of the relevant business, suspension of business for rectification, close the website, or revoke the relevant business permit or business license; the directly responsible person in charge and other directly responsible persons shall be fined not less than RMB 20,000 but not more than RMB 200,000.

Article 68 — Where any network operator violates the provisions of Article 47 of this Law and fails to take measures such as ceasing transmission or deletion for information prohibited by laws or administrative regulations from being published or transmitted, the relevant competent department shall order correction and issue a warning, and confiscate the illegal gains; where correction is refused or the circumstances are serious, a fine of not less than RMB 100,000 but not more than RMB 500,000 shall be imposed; the directly responsible person in charge and other directly responsible persons shall be fined not less than RMB 10,000 but not more than RMB 100,000. Where electronic information transmission service providers or application software download service providers violate the provisions of Article 48, paragraph 2 of this Law, they shall be punished in accordance with the provisions of the preceding paragraph.

Article 69 — Where a network operator violates the provisions of this Law and commits any of the following acts, the relevant competent department shall order correction; where correction is refused or the circumstances are serious, a fine of not less than RMB 50,000 but not more than RMB 500,000 shall be imposed; the directly responsible person in charge and other directly responsible persons shall be fined not less than RMB 10,000 but not more than RMB 100,000: (1) failing to incorporate security measures into the network in accordance with the requirements of the relevant departments; (2) failing to perform the obligations provided for in Article 25 of this Law; (3) failing to provide technical support and assistance in accordance with the provisions of Article 28 of this Law.

Article 70 — For any act of publishing or transmitting information prohibited by Article 12, paragraph 2 of this Law or other laws or administrative regulations, the relevant laws and administrative regulations shall apply for punishment.

Article 71 — Where any illegal act provided for by this Law is committed, the illegal gains shall be confiscated and fines imposed in accordance with the provisions of relevant laws and administrative regulations; where the relevant laws and administrative regulations do not provide for punishment, the relevant competent department shall impose punishment. Where the illegal gains confiscated and fines imposed in accordance with the provisions of this Law are to be turned over to the state treasury, they shall be turned over in accordance with the law.

Article 72 — Where a state organ's government affairs network fails to perform its cybersecurity protection obligations provided for in this Law, the organ at the next higher level or the relevant organ shall order correction; the directly responsible person in charge and other directly responsible persons shall be subject to sanctions in accordance with the law.

Article 73 — Where any staff member of a cyberspace administration authority or relevant department neglects his duties, abuses his power, or engages in fraudulent practices for personal gain, and no crime is constituted, the relevant organ shall impose a sanction on him in accordance with the law.

Article 74 — Where any violation of the provisions of this Law causes damage to others, civil liability shall be borne in accordance with the law. Where any violation of the provisions of this Law 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 such as attacking, intruding into, interfering with, destroying, or otherwise endangering the critical information infrastructure of the PRC, causing serious consequences, legal liability shall be pursued in accordance with the law; the public security authority under the State Council and the relevant departments may also decide to freeze the property or take other necessary sanctions against such institution, organization, or individual.

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 consisting of computers or other information terminals and related equipment that collects, stores, transmits, exchanges, and processes information in accordance with certain rules and procedures. (2) "Network security" means adopting necessary measures to prevent attacks, intrusions, interference, destruction, and illegal use of, as well as accidents to, the network, so as to keep the network in a state of stable and reliable operation, and ensuring the integrity, confidentiality, and availability 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 the network. (5) "Personal information" means all kinds of information recorded by electronic or other means, which can identify the personal identity of a natural person independently or in combination with other information, including but not limited to the name, date of birth, identity document number, personal biometric information, address, and telephone number of the natural person.

Article 77 — The security protection of the networks storing and processing information involving state secrets shall also abide by the provisions of the confidentiality 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 on June 1, 2017.

Disclaimer: This English translation is provided for informational and reference purposes only. While every effort has been made to ensure accuracy, this translation is not an official version and may not reflect the most current amendments or authoritative interpretations of the original Chinese text. For legal purposes, the official Chinese version as published by the National People's Congress of the People's Republic of China shall prevail. Readers should consult qualified legal professionals for advice on specific legal matters. This translation does not constitute legal advice.