Cybersecurity Law of the People’s Republic of China

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 2 — Operation Security of Critical Information Infrastructure 5

Chapter IV — Network Information Security 6

Chapter V — Monitoring, Early Warning, and Emergency Response 8

Chapter VI — Legal Liability 9

Chapter VII — Supplementary Provisions 12

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 protecting social and public interests and the legitimate rights and interests of citizens, legal persons, and other organizations, and promoting the sound 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 attach equal importance to the development of cybersecurity and informatization, follow the principles of active utilization, scientific development, lawful administration, and security

assurance, advance the construction and interconnection of network infrastructure, encourage innovation in network technology and its application, support the cultivation of cybersecurity professionals, establish and improve the cybersecurity assurance system, and enhance cybersecurity protection capabilities.

Article 4. The state shall formulate and continuously improve its cybersecurity strategy, clearly define the basic requirements and main objectives for ensuring cybersecurity, and put forward cybersecurity policies, work tasks, and measures for key sectors.

Article 5. The state shall take measures to monitor, defend against, and address cybersecurity risks and threats originating from within or outside the territory of the People's Republic of China, protect critical information infrastructure from attack, intrusion, interference, and damage, punish unlawful and criminal network activities in accordance with the law, and maintain security and order in cyberspace.

Article 6. The state shall advocate honest, trustworthy, healthy, and civilized network conduct, promote the dissemination of the core socialist values, and take measures to raise the cybersecurity awareness and competence of the whole society, so as to create a favorable environment in which all of society participates jointly in promoting cybersecurity.

Article 7. The state shall actively carry out international exchange and cooperation in the areas of cyberspace governance, network technology research and development, standard-setting, and the combat against cybercrime and other illegal activities, promote the building of a peaceful, secure, open, and cooperative cyberspace, and establish a multilateral, democratic, and transparent network governance system.

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

Article 9. In conducting business and service activities, network operators shall comply with laws and administrative regulations, respect social morality, observe commercial ethics, act in good faith, fulfill their cybersecurity protection obligations, accept supervision by the government and society, and bear social responsibility.

Article 10. Those who construct or operate networks, or provide services through networks, shall, in accordance with the provisions of laws and administrative regulations and the mandatory requirements of national standards, adopt technical measures and other necessary measures to ensure the secure and stable operation of networks, effectively respond to cybersecurity incidents, prevent cybercrime and other illegal activities, and safeguard the integrity, confidentiality, and availability of network data.

Article 11. Network-related industry organizations shall, in accordance with their charters, strengthen industry self-discipline, formulate cybersecurity codes of conduct, 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, promote the popularization of network access, improve the level of network services, provide safe and convenient network services for society, and ensure the orderly and free flow of network information in accordance with the law. Any individual or organization using a network shall comply with the Constitution and laws, observe public order, and respect social morality; shall not endanger

cybersecurity; and shall not use the network to engage in activities that endanger national security, honor, or interests, incite the subversion of state power or the overthrow of the socialist system, incite secession or undermine national unity, advocate terrorism or extremism, incite ethnic hatred or ethnic discrimination, disseminate violent or obscene pornographic information, fabricate or disseminate false information to disrupt economic or social order, or infringe upon the reputation, privacy, intellectual property, or other legitimate rights and interests of others.

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

Article 14. Any individual or organization shall have the right to report conduct that endangers cybersecurity to the cyberspace administration, telecommunications, public security, and other relevant departments. The department receiving such a report shall handle it in a timely manner in accordance with the law; if the matter does not fall within the scope of its duties, it shall promptly refer the report to the department with the authority to handle it. The relevant departments shall keep confidential any relevant information concerning the reporter and protect the legitimate rights and interests of the reporter.

Chapter II — Support and Promotion of Cybersecurity

Article 15. The state shall establish and improve the cybersecurity standards system. The administrative department in charge of standardization 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 national standards and industry standards relating to cybersecurity administration, as well as 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 standards 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 intellectual property rights in network technology, 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 establishment of a socialized cybersecurity service system and encourage relevant enterprises and institutions to carry out security services such as cybersecurity certification, testing, and risk assessment.

Article 18. The state shall encourage the development of technologies for the protection and utilization of network data security, promote the opening of public data resources, and advance technological innovation and economic and social development. The state shall support innovation in cybersecurity management methods and the application 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 entities to conduct cybersecurity publicity and education work effectively. Mass media shall carry out targeted cybersecurity publicity and education for the public.

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

Chapter III — Network Operation Security

Section 1 — General Provisions

Article 21. The state shall implement a graded cybersecurity protection system. Network operators shall, in accordance with the requirements of the graded cybersecurity protection system, perform the following security protection obligations to ensure that networks are free from interference, damage, or unauthorized access, and to prevent network data from being leaked, stolen, or tampered with:

(1) Formulate internal security management rules and operating procedures, designate persons responsible for cybersecurity, and implement cybersecurity protection responsibilities;

(2) Adopt technical measures to prevent computer viruses, network attacks, network intrusions, and other conduct endangering cybersecurity;

(3) Adopt technical measures for monitoring and recording network operation status and cybersecurity incidents, and retain relevant network logs for no less than six months as required by regulations;

(4) Adopt measures such as data classification, backup of important data, and encryption; and

(5) Perform other obligations prescribed 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 malicious programs; where they discover that their network products or services have security defects, vulnerabilities, or other risks, they shall immediately take remedial measures and promptly inform users and report to the relevant competent authorities in accordance with regulations. Providers of network products and services shall continuously provide security maintenance for their products and services; they shall not cease providing security maintenance within the period prescribed by regulations or agreed upon with the parties concerned. Where network products or services have the function of collecting user information, their providers shall expressly notify users and obtain their consent; where personal information of users is involved, the provisions of this Law and relevant laws and administrative regulations on the protection of personal information shall also be complied with.

Article 23. Critical network equipment and specialized cybersecurity products may be sold or provided only after they have passed security certification by a qualified institution or met the requirements of security testing in accordance with the mandatory requirements of relevant national standards. The national cyberspace administration authority shall, in conjunction with the relevant departments under the State Council, formulate and publish a catalog of critical network equipment and specialized cybersecurity products, and promote the mutual recognition of security certification and security testing results to avoid duplicate certification and testing.

Article 24. When handling network access or domain name registration services for users, handling network access procedures for fixed-line telephones, mobile telephones, or other services, or providing users with information release, instant messaging, or other services, network operators shall, when entering into an agreement with users or confirming the provision of services, require users to provide their true identity information. Where a user does not provide true identity information, the network operator shall not provide the relevant service to that user. The state shall implement a trusted online identity strategy, support the research and development of secure and convenient electronic identity authentication technology, and promote mutual recognition among different electronic identity authentication systems.

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

authorities in accordance with regulations.

Article 26. Activities such as cybersecurity certification, testing, and risk assessment, and the public release of cybersecurity information such as system vulnerabilities, computer viruses, network attacks, and network intrusions, shall comply with the relevant provisions of the state.

Article 27. No individual or organization may engage in activities endangering cybersecurity, such as illegally intruding into others' networks, interfering with the normal functioning of others' networks, or stealing network data; no individual or organization may provide programs or tools specifically designed for activities endangering cybersecurity, such as intruding into networks, interfering with the normal functioning of or protective measures for networks, or stealing network data; and no individual or organization may, knowing that others are engaging in activities endangering cybersecurity, provide them with assistance such as technical support, advertising promotion, or payment and settlement.

Article 28. Network operators shall provide technical support and assistance to public security organs and state security organs for their lawful activities in safeguarding national security and investigating crimes.

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 assurance capabilities of network operators. Relevant industry organizations shall establish and improve cybersecurity protection norms and coordination mechanisms for their respective industries, strengthen the analysis and assessment of cybersecurity risks, periodically issue risk warnings to their members, and support and assist members in responding to cybersecurity risks.

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

Section 2 — Operation Security of Critical Information Infrastructure

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

Article 32. In accordance with the division of duties prescribed by the State Council, the departments responsible for the security protection of critical information infrastructure shall separately formulate and organize the implementation of critical information infrastructure security plans for their respective industries and sectors, and guide and supervise the operation security protection of critical information infrastructure.

Article 33. The construction of critical information infrastructure shall ensure that it has the performance to support the stable and continuous operation of services, and shall ensure that security technical measures are planned, constructed, and applied synchronously.

Article 34. In addition to the obligations set forth in Article 21 of this Law, operators of critical information infrastructure shall also perform the following security protection obligations:

(1) Establish a dedicated security management body and designate persons responsible for security management, and conduct security background checks on such responsible persons and personnel in key positions;

Source: https://www.danyoungcpa.com/cybersecurity-law-prc-2017-english-translation/

(2) Periodically provide cybersecurity education, technical training, and skills assessment for practitioners;

(3) Conduct disaster recovery backup for important systems and databases;

(4) Formulate emergency response plans for cybersecurity incidents and conduct periodic drills; and

(5) Perform other obligations prescribed by laws and administrative regulations.

Article 35. Where the procurement of network products or services by an operator of critical information infrastructure may affect national security, such procurement shall be subject to a national security review organized by the national cyberspace administration authority in conjunction with the relevant departments under the State Council.

Article 36. When procuring network products and services, operators of critical information infrastructure shall, in accordance with regulations, enter into security and confidentiality agreements with the providers, clearly defining the security and confidentiality obligations and responsibilities.

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. Where such information or data must be provided 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 prevail.

Article 38. Operators of critical information infrastructure shall, either by themselves or by commissioning cybersecurity service institutions, conduct at least one annual inspection and assessment of the security and potential risks of their networks, and submit the inspection and assessment results and improvement measures to the department responsible for the security protection of critical information infrastructure.

Article 39. The national cyberspace administration authority shall make overall plans and coordinate with the relevant departments to adopt the following measures for the security protection of critical information infrastructure:

(1) Conduct random inspection and testing of the security risks of critical information infrastructure, propose improvement measures, and, where necessary, commission cybersecurity service institutions to inspect and assess the security risks existing in the networks;

(2) Periodically organize cybersecurity emergency response drills for operators of critical information infrastructure to improve their capability to respond to cybersecurity incidents and their coordination and cooperation capabilities;

(3) Promote the sharing of cybersecurity information among relevant departments, operators of critical information infrastructure, relevant research institutions, and cybersecurity service institutions; and

(4) Provide technical support and assistance for the emergency response to cybersecurity incidents and the recovery of network functions.

Chapter IV — Network Information Security

Article 40. Network operators shall strictly maintain the confidentiality of user information they collect and shall establish and improve user information protection systems.

Article 41. When collecting and using personal information, network operators shall adhere to the principles of lawfulness, propriety, and necessity, publicly disclose the rules for collection and use, expressly state the purpose, method, and scope of collection and use of information, and obtain the consent of the person from whom the information is collected. Network operators shall not collect personal information unrelated to the services they provide, shall not collect or use personal information in violation of the provisions of laws and

administrative regulations or their agreements with users, and shall, in accordance with the provisions of laws and administrative regulations and their agreements with users, process the personal information they store.

Article 42. Network operators shall not disclose, tamper with, or destroy the personal information they collect, and shall not provide personal information to others without the consent of the person from whom the information is collected, unless the information has been processed such that specific individuals cannot be identified 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 leakage, destruction, or loss of such information. Where an incident involving the leakage, destruction, or loss of personal information occurs or may occur, they shall immediately adopt remedial measures, promptly inform users, and report to the relevant competent authorities in accordance with regulations.

Article 43. Where an individual discovers that a network operator has collected or used his or her personal information in violation of the provisions of laws and administrative regulations or the agreement between the parties, he or she 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 about him or her contains errors, he or she shall have the right to request the network operator to make corrections. The network operator shall adopt measures to effect such deletion or correction.

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

Article 45. Departments legally charged with cybersecurity supervision and administration duties and their staff must strictly maintain the confidentiality of personal information, privacy, and commercial secrets that come to their knowledge in the performance of their duties, and shall not disclose, sell, or illegally provide such information to others.

Article 46. Any individual or organization shall be responsible for their conduct in using networks, and shall not establish websites or communication groups for the purpose of committing fraud, teaching criminal methods, producing or selling prohibited or controlled goods, or other illegal or criminal activities, nor shall they use networks to release information related to committing fraud, producing or selling prohibited or controlled goods, or other illegal or criminal activities.

Article 47. Network operators shall strengthen the management of information released by their users; where they discover information the release or transmission of which is prohibited by laws or administrative regulations, they shall immediately cease the transmission of such information, adopt measures such as deletion to prevent the information from spreading, preserve relevant records, and report to the relevant competent authorities.

Article 48. Electronic information sent or application software provided by any individual or organization shall not contain malicious programs, nor shall they contain information the release or transmission of which is prohibited by laws or administrative regulations. Providers of electronic information sending services and providers of application software download services shall perform their security management obligations and, where they become aware that their users have committed the acts specified in the preceding paragraph, shall cease providing services, adopt measures such as deletion, preserve relevant records, and report to the relevant competent authorities.

Article 49. Network operators shall establish a complaint and reporting system for network information security, publicly disclose information such as the means for making complaints and reports, and promptly accept and handle complaints and reports concerning network information security. Network operators shall cooperate with the lawful supervision and inspection conducted by the cyberspace administration authority and the relevant departments.

Article 50. Where the national cyberspace administration authority and the relevant departments, in the lawful performance of their network information security supervision and administration duties, discover information the release or transmission of which is prohibited by laws or administrative regulations, they shall require the network operator to cease transmission and adopt measures such as deletion, and to preserve relevant records; where such information originates from outside the territory of the People's Republic of China, they shall notify the relevant institutions to adopt technical measures and other necessary measures to block its dissemination.

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 make overall plans and coordinate with the relevant departments to strengthen the collection, analysis, and notification of cybersecurity information, and shall uniformly release cybersecurity monitoring and early warning information in accordance with regulations.

Article 52. The departments responsible for the security protection of critical information infrastructure shall establish and improve cybersecurity monitoring, early warning, and information notification systems for their respective industries and sectors, and shall submit cybersecurity monitoring and early warning information in accordance with regulations.

Article 53. The national cyberspace administration authority shall coordinate with the relevant departments to establish and improve cybersecurity risk assessment and emergency response mechanisms, formulate emergency response plans for cybersecurity incidents, and organize periodic drills. The departments responsible for the security protection of critical information infrastructure shall formulate emergency response plans for cybersecurity incidents in their respective industries and sectors, and organize periodic drills. Emergency response plans for cybersecurity incidents shall classify cybersecurity incidents according to factors such as the degree of harm and scope of impact after an incident occurs, and shall prescribe corresponding emergency response measures.

Article 54. Where the risk of a cybersecurity incident occurring increases, the relevant departments of people's governments at or above the provincial level shall, in accordance with the prescribed authority and procedures and based on the characteristics of the cybersecurity risk and the potential harm it may cause, take the following measures:

(1) Require the relevant departments, institutions, and personnel to promptly collect and report relevant information, and strengthen the monitoring of cybersecurity risks;

(2) Organize the relevant departments, institutions, and professionals to analyze and assess cybersecurity risk information, and predict the likelihood of an incident occurring, the scope of its impact, and the degree of harm; and

(3) Issue cybersecurity risk warnings to the public, and publish measures to avoid or mitigate harm.

Article 55. Where a cybersecurity incident occurs, the emergency response plan for cybersecurity incidents shall be activated immediately, an investigation and assessment of the cybersecurity incident shall be conducted, and network operators shall be required to adopt technical measures and other necessary measures to eliminate security hazards, prevent the harm from spreading, and promptly release public warning information to the public.

Article 56. Where the relevant departments of people's governments at or above the provincial level, in the course of performing their cybersecurity supervision and administration duties, discover that a network has a relatively significant security risk or that a security incident has occurred, 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 take measures, carry out rectification, and eliminate hazards as required.

Article 57. Where a cybersecurity incident gives rise to an emergency or a production safety incident, it shall be handled in accordance with the provisions of the Emergency Response Law of the People's Republic of China, the Production Safety Law of the People's Republic of China, and other relevant laws and administrative regulations.

Article 58. Where it is necessary to take temporary measures such as restricting network communications in specific areas for the purpose of safeguarding national security and public order in response to a major public security incident, such measures may be taken 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 set forth in Articles 21 and 25 of this Law, the relevant competent authority shall order it to make corrections and issue a warning; where it refuses to make corrections or causes harm to cybersecurity or other consequences, it shall be fined not less than RMB 10,000 but not more than RMB 100,000, and the directly responsible person in charge shall be fined not less than RMB 5,000 but not more than RMB 50,000. Where an operator of critical information infrastructure fails to perform the cybersecurity protection obligations set forth in Articles 33, 34, 36, and 38 of this Law, the relevant competent authority shall order it to make corrections and issue a warning; where it refuses to make corrections or causes harm to cybersecurity or other consequences, it shall be fined not less than RMB 100,000 but not more than RMB 1,000,000, and the directly responsible person in charge shall be fined not less than RMB 10,000 but not more than RMB 100,000.

Article 60. Where a party violates the provisions of the first and second paragraphs of Article 22 and the first paragraph of Article 48 of this Law by committing any of the following acts, the relevant competent authority shall order it to make corrections and issue a warning; where it refuses to make corrections or causes harm to cybersecurity or other consequences, it shall be fined not less than RMB 50,000 but not more than RMB 500,000, and the directly responsible person in charge shall be fined not less than RMB 10,000 but not more than RMB 100,000:

(1) Installing malicious programs;

(2) Failing to immediately take remedial measures for security defects, vulnerabilities, or other risks existing in its products or services, or failing to promptly inform users and report to the relevant competent authorities in accordance with regulations; or

(3) Unilaterally ceasing to provide security maintenance for its products or services.

Article 61. Where a network operator, in violation of the first paragraph of Article 24 of this Law, fails to require users to provide true identity information, or provides relevant services to users who do not provide true identity information, the relevant competent authority shall order it to make corrections; where it refuses to make corrections or the circumstances are serious, it shall be fined not less than RMB 50,000 but not more than RMB 500,000, and the relevant competent authority may also order the suspension of the relevant business, suspension of business for rectification, closure of the website, revocation of the relevant business license, or revocation of the 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 62. Where a party, in violation of Article 26 of this Law, engages in activities such as cybersecurity certification, testing, or risk assessment, or publicly releases cybersecurity information such as system vulnerabilities, computer viruses, network attacks, or network intrusions, the relevant competent authority shall order it to make corrections and issue a warning; where it refuses to make corrections or the

circumstances are serious, it shall be fined not less than RMB 10,000 but not more than RMB 100,000, and the relevant competent authority may also order the suspension of the relevant business, suspension of business for rectification, closure of the website, revocation of the relevant business license, or revocation of the business license; 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 party, in violation of Article 27 of this Law, engages in activities endangering cybersecurity, or provides programs or tools specifically designed for activities endangering cybersecurity, or provides others with assistance such as technical support, advertising promotion, or payment and settlement for engaging in activities endangering cybersecurity, and such conduct does not yet constitute a crime, the public security organ shall confiscate the illegal gains and impose detention of not more than five days, and may concurrently 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 be concurrently imposed. Where an entity commits the act referred to in the preceding paragraph, the public security organ shall confiscate the 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. A person who has been subjected to public security administrative penalties for violating Article 27 of this Law shall not hold a position critical to cybersecurity management and network operations within five years; a person who has been subjected to criminal penalties shall be prohibited for life from holding a position critical to cybersecurity management and network operations.

Article 64. Where a network operator or a provider of network products or services, in violation of the third paragraph of Article 22 and Articles 41 through 43 of this Law, infringes upon the right of personal information to be protected in accordance with the law, the relevant competent authority shall order it to make corrections, and may, in light of the circumstances, impose a warning and confiscate illegal gains individually or concurrently, 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, 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 authority may also order the suspension of the relevant business, suspension of business for rectification, closure of the website, revocation of the relevant business license, or revocation of the business license. Where a party, in violation of Article 44 of this Law, steals or obtains personal information by other illegal means, or illegally sells or illegally provides personal information to others, and such conduct does not yet constitute a crime, the public security organ 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, a fine of not more than RMB 1,000,000.

Article 65. Where an operator of critical information infrastructure, in violation of Article 35 of this Law, uses network products or services that have not undergone a security review or have failed a security review, the relevant competent authority shall order it to cease using such products or services and impose a fine of not less than one time but not more than ten times the procurement 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 an operator of critical information infrastructure, in violation of Article 37 of this Law, stores network data overseas or provides network data overseas, the relevant competent authority shall order it to make corrections, issue 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 also order the suspension of the relevant business, suspension of business for rectification, closure of the website, revocation of the relevant business license, or revocation of the 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 party, in violation of Article 46 of this Law, establishes websites or communication groups for the purpose of committing illegal or criminal activities, or uses networks to release information related to committing illegal or criminal activities, and such conduct does not yet constitute a crime, the public security organ shall impose detention of not more than five days, and may concurrently impose a fine of not less than RMB 10,000 but not more than RMB 100,000; 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 50,000 but not more than RMB 500,000 may be concurrently imposed. The websites and communication groups established for the purpose of committing illegal or criminal activities shall be closed. Where an entity commits the act referred to in the preceding paragraph, the public security organ shall impose a fine of not less than RMB 100,000 but not more than RMB 500,000, and the directly responsible person in charge and other directly responsible persons shall be punished in accordance with the provisions of the preceding paragraph.

Article 68. Where a network operator, in violation of Article 47 of this Law, fails to cease transmission of, adopt measures such as deletion with respect to, or preserve relevant records of information the release or transmission of which is prohibited by laws or administrative regulations, the relevant competent authority shall order it to make corrections, issue a warning, and confiscate its illegal gains; where it refuses to make corrections or the circumstances are serious, it shall be fined not less than RMB 100,000 but not more than RMB 500,000, and the authority may also order the suspension of the relevant business, suspension of business for rectification, closure of the website, revocation of the relevant business license, or revocation of the 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. Where a provider of electronic information sending services or a provider of application software download services fails to perform the security management obligations set forth in the second paragraph of Article 48 of this Law, it shall be punished in accordance with the provisions of the preceding paragraph.

Article 69. Where a network operator, in violation of the provisions of this Law, commits 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, it shall be fined not less than RMB 50,000 but not more than RMB 500,000, and 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 adopt measures such as ceasing transmission or deletion with respect to information the release or transmission of which is prohibited by laws or administrative regulations as required by the relevant departments;

(2) Refusing or obstructing the lawful supervision and inspection conducted by the relevant departments; or

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

Article 70. Where a party releases or transmits information the release or transmission of which is prohibited by the second paragraph of Article 12 of this Law or other laws and administrative regulations, it shall be punished in accordance with the provisions of the relevant laws and administrative regulations.

Article 71. Where a party engages in illegal conduct under this Law, such conduct shall be recorded in its credit files and publicly disclosed in accordance with the provisions of the relevant laws and administrative regulations.

Article 72. Where an operator of a government network of a state organ fails to perform the cybersecurity protection obligations prescribed by this Law, its superior organ or the relevant organ shall order it to make corrections; the directly responsible person in charge and other directly responsible persons shall be subject to sanctions in accordance with the law.

Article 73. Where the cyberspace administration authority and the relevant departments, in violation of Article 30 of this Law, use the information obtained in the course of performing their cybersecurity protection duties for other purposes, the directly responsible person in charge and other directly responsible persons shall be subject to sanctions in accordance with the law. Where staff members of the cyberspace administration authority and the relevant departments neglect their duties, abuse their powers, or engage in malpractices for personal gain, and such conduct does not yet constitute a crime, they shall be subject to sanctions in accordance with the law.

Article 74. Where a party, in violation of the provisions of this Law, causes damage to others, it shall bear civil liability in accordance with the law. Where a violation of the provisions of this Law constitutes a violation of public security administration, public security administrative 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 overseas institutions, organizations, or individuals engage in activities such as attacking, intruding into, interfering with, or damaging critical information infrastructure of the People's Republic of China, causing serious consequences, legal liability shall be pursued in accordance with the law; the public security department under the State Council and the relevant departments may also decide to freeze assets or impose other necessary sanctions against such institutions, organizations, or individuals.

Chapter VII — Supplementary Provisions

Article 76. For the purposes of this Law, the following terms shall have the meanings set forth below:

(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) "Cybersecurity" means the ability, through the adoption of necessary measures, to prevent attacks on, intrusion into, interference with, and damage and illegal use of networks, as well as unexpected accidents, so as to maintain networks in a state of stable and reliable operation, and to ensure the integrity, confidentiality, and availability of network data.

(3) "Network operator" means the owner and manager of a network, and a network service provider.

(4) "Network data" means all kinds of electronic data collected, stored, transmitted, processed, and generated through networks.

(5) "Personal information" means all kinds of information recorded in electronic or other forms that can, independently or in combination with other information, identify the personal identity of a natural person, including but not limited to the name, date of birth, identity document number, personal biometric information, address, and telephone number of a natural person.

Article 77. The operation security protection of networks that store or process information involving state secrets shall, in addition to complying with this Law, also comply with the provisions of 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 take effect as of June 1, 2017.

Source: https://www.danyoungcpa.com/cybersecurity-law-prc-2017-english-translation/

Disclaimer: This is an unofficial English translation prepared by Dan&Young Business Consultancy for informational purposes only. The original Chinese text (adopted November 7, 2016, effective June 1, 2017) remains the sole authoritative version. While every effort has been made to ensure accuracy, this translation does not constitute legal advice. For matters involving the Cybersecurity Law of the People's Republic of China, readers should consult qualified legal counsel. Dan&Young Business Consultancy assumes no liability for any reliance placed on this translation. For professional legal and compliance services related to China's cybersecurity regulations, please contact us.