Cybersecurity Law of the People's Republic of China (Draft) (Second Draft)

Table of Contents

Chapter I. General Provisions

Article 1 This Law is enacted for the purpose of maintaining network security, safeguarding the cyber space sovereignty, national security and public interests, protecting the legal rights and interests of citizens, corporations and other organizations, and promoting the healthy development of information technology in the economic and social sectors.

Article 2 This Law shall apply to networks established, operated, maintained and used within the territory of the People's Republic of China as well as to the supervision and management practices concerning network security.

Article 3 The State attaches equal importance to network security and the development of information technology (IT). Pursuant to the principle of "active utilization, scientific development, lawful administration and guaranteed security", the State pushes forward the development of network infrastructures, encourages network technical innovations and application, and creates and optimizes network security system to improve the protection of network security.

Article 4 The State formulates and from time to time revises the network security strategy, in order to clarify primary requirements and objectives of ensuring network security and set forth network security policies, tasks and measures for key areas.

Article 5 The State takes necessary measures to oversee, prevent and deal with network security risks originated from both inside and outside of the territory of the People's Republic of China, protects essential information infrastructures from attacks, intrusions, interferences and vandalism, imposes punishments on network crimes according to law, and safeguards the security and maintain the good order of cyber space.

Article 6 The State encourages honest, trustworthy and lawful network practices to disseminate the core values of socialism, and adopts measures to raise social awareness of network security and create a sound environment for the protection of network security through public involvement.

Article 7 The State actively makes international exchanges and cooperation in respect of cyber space governance, network technology R&D and formulation of standards, and campaign against network crimes, in order to shape a peaceful, safe, open and cooperative cyber space and establish a multilateral, democratic and transparent network governance system.

Article 8 The state network and IT authorities take charge of making overall plans for and coordination of network security-related works and regulatory practices. The telecommunications authority of the State Council, the public security authorities and other competent authorities shall assume network security and regulation responsibilities within their respective jurisdictions pursuant to the Law and applicable laws and administrative regulations.

Competent authorities of local governments at county level and above shall take the responsibilities for network security and regulation as stipulated in state regulations.

Article 9 When undertaking operation and/or service activities, network operators shall abide by the laws and administrative regulations, social and business ethics, honesty and trustworthiness. They shall also be obligated to protect network security, be subject government and public supervision and assume social responsibilities.

Article 10 Network operation and provision of services via network shall be made in the light of the compulsory rules set forth in laws, administrative regulations and national standards. Technical and other necessary measures shall be taken to ensure the safe and steady network operation, effectively cope with network security events, prevent network criminal offenses, and protect the integrity, confidentiality and usability of network data.

Article 11 Organizations of network-related industries shall intensify self-discipline pursuant to their Articles of Association/constitution. They shall stipulate codes of conducts to guide their members to enhance network security and boost the healthy development of industries.

Article 12 The State safeguards the rights of citizens, corporations and organizations to lawful access to network, promotes network accessibility, improves network services, provides the society with safe and convenient network services, and ensures free dissemination of network information in a lawful and orderly fashion.

Individuals and organizations shall abide by the Constitution and laws, observe public order, and respect social ethics. They shall not impair network security, and are prohibited to engage in activities that threaten national security, incite subversion of the state power or overthrow of the socialist system, propagate terrorism and/or extremism, ethnic hatred and/or discrimination, violent and/or obscene/erotic information, disrupt economic and social orders with fabricating and disseminating false information, or infringe the reputation, privacy, intellectual property and other legal rights and interests of another.

Article 13 Individuals and organizations shall be entitled to report to the network and IT, telecommunications and public security authorities on any activities that impair network security. The authority that receives such report shall respond in a timely manner to or, if it is beyond its jurisdiction, swiftly transfer the report to a competent authority.

Chapter II. Support for and Promotion of Network Security

Article 14 The State establishes and perfects the standard system for network security. The standardization administration and competent departments of the State Council shall, within their respective functions, organize formulation and appropriate revision of national and industrial standards regarding network security management and network products, services and operation security.

The State supports businesses, network-related industries, among others, to involve in formulation of national and industrial standards for network security, and encourage businesses to design their own standards that are more rigorous than the national and industrial standards.

Article 15 The State Council and the governments of provinces, autonomous regions and municipalities directly under the central government shall make overall plans and intensify inputs to support key industries and projects of network security technologies, support R&D and application of network security technologies, disseminate safe and reliable network products and services, protect the intellectual property of network technologies, and encourage businesses, research institutions and colleges to engage in national projects of innovation in network security technologies.

Article 16 The State pushes forward the development of network security social service system, and encourages related businesses and institutions to provide such services as network security certification, examination and risk assessment.

Article 17 The State encourages the development of network data protection and utilization technologies to allow access to public data resources and boost technology innovations and economic and social development.

The State encourages innovative network security management and new network technologies to elevate the level of network security.

Article 18 Governments and competent authorities at all levels shall organize regularly educational campaigns on network security, and guide and urge organizations concerned to do so.

The public media shall carry out targeted educational campaigns for the public.

Article 19 The State encourages businesses, colleges, occupational schools and related education and training institutions to carry out educational and training activities regarding network security, foster in diverse means and facilitate exchanges of network security professionals.

Chapter III. Network Operations Security

Section 1 General

Article 20 The State adopts network security classification system which requires network operators to perform the following obligations to protect networks from interference, disruption or unauthorized access and protect network data from disclosure or theft or alteration:

1. Formulating internal security management policies and operating rules to identify responsible personnel and define network security accountabilities;

1. Taking technical measures to prevent computer virus, network attacks, network intrusions and other risks;

3. Taking technical measures to monitor and record network operation and network security events, and maintaining the logs for no less than six months;

4. Taking such measures as data classification, backup and encryption of important data, etc.; and

5. Other obligations specified by laws and administrative regulations.

Article 21 Network products and services shall satisfy the mandatory requirements set forth in applicable national standards. Providers of network products and services shall not set malicious programs and, in case of safety risks such as defects or vulnerabilities, timely notify the users and make remedies, and report to competent authorities in accordance with rules and regulations.

Providers of network products and services shall also provide consistent security maintenance for their products and services. Such maintenance shall not be discontinued within the set term or the term agreed among relevant parties.

Providers of network products and services shall expressly notify and obtain consent of the user if the products and/or services collect user information; in this case, the collection shall be made in the light of the clauses on the confidentiality of citizens' personal information specified in this Law and applicable laws and administrative regulations.

Article 22 Critical network equipment and network security products shall, in the light of the compulsory rules set forth in national standards, be subject to security certificate or security tests by certified organs before marketing. State network and IT authorities shall work with competent departments of the State Council to formulate and publish catalogues of critical network equipment and network security products, and cause mutual recognition between security certificate and security test results for the avoidance of overlaps.

Article 23 Network operators shall require the users to provide their true identity when signing agreements or confirmations on the provision of such services as network access, domain

name registration, fixed phone and mobile phone network access, or information distribution and instant communication. In case a user refuses or fails to provide his/her true identity, the network operation shall not provide such services for him or her.

The State implements trusted network ID strategy, supports R&D of safe, convenient E-identity authentication technology and cause mutual recognition between various E-authentications.

Article 24 Network operators shall have in-place emergency plans for network security events to timely respond to such risks as system vulnerabilities, computer virus, network attack and intrusion. In case of events that threaten network security, the emergency plan shall be promptly activated, appropriate remedies shall be made and reports shall be submitted to competent authorities.

Article 25 Network security authentication, test, risk assessment, and publication of network security information such as system vulnerabilities, computer virus, network attack and intrusion shall be made in the light of applicable state regulations.

Article 26 Individuals and/or organizations shall not engage in any activities that threaten network security, including but not limited to unauthorized intrusion into networks, interfering normal network functions or stealing network data, or provide programs or implements for such intrusion, interference or stealing, or, if they are aware of such threatening activities, provide any help including but not limited to technical support, advertisement, payment or settlement.

Article 27 Network operators shall provide technical support and assistance for the public security and national security authorities in their attempts to safeguarding national security and investigation into criminal offenses.

Article 28 The State supports the cooperation between network operators on the collection, analysis and notification of network security information and emergency response, in order to build up their capability for safeguarding network security.

Industrial organizations shall establish and perfect their respective network security rules and coordination mechanisms, in order to intensify the analysis and assessment on network security risks, regularly issue risk warnings to their members and support and assist their members to cope with network security risks.

Section 2 Operations Security of Key Information Infrastructures

Article 29 Key information infrastructures that, once vandalized, disabled or data disclosed, may severely threaten national security, national economy, people's livelihood and public interests shall, in addition to the network security classification system, be subject to priority protection. Specific scope of and security measures for key information infrastructures shall be developed by the State Council.

The State encourages network operators, who are not engaged in key information infrastructures, to voluntarily involve in the protection system of key information infrastructures.

Article 30 In conformity with their respective responsibility assigned to them by the State Council, the authorities in charge of the security of key information infrastructures shall formulate and implement the plans for the key information infrastructures of specific industries/disciplines within their respective jurisdiction, and guide and oversee the operation security of such key information infrastructures.

Article 31 The key information infrastructures shall be developed with the capacity to support the steady and continuous business operation, and security technologies shall be planned, applied and put into use in a simultaneous manner.

Article 32 In addition to Article 20 of this Law, the operators of key information infrastructures shall be also obligated to:

1. Define dedicated security management bodies and personnel, and check the security backgrounds of such personnel and those in key posts;

2. Provide practitioners with regular network security education, technical training and assessment;

3. Make disaster recovery backup of important systems and database;

4. Establish emergency plans for network security events and organize regular drills; and

5. Other obligations specified by laws and administrative regulations.

Article 33 Purchase of network products and services by the operators of key information infrastructures that may threaten national security shall be subject to the national security review conducted by the state network and IT authorities together with competent departments of the State Council.

Article 34 The operators of key information infrastructures shall, in the purchase of network products and services, sign agreements with the product/service providers in which obligations for security and confidentiality shall be specified.

Article 35 The operators of key information infrastructures shall store within the territory of the People's Republic of China citizens' personal information and critical business data collected and generated during their operations within the territory of the People's Republic of China. Where such information and data shall be exported for business purpose, security assessment shall be gone through pursuant to the measures formulated by the state network and IT authorities together with competent departments of the State Council, unless otherwise provided in laws and administrative regulations.

Article 36 The operators of key information infrastructures shall conduct, at least once a year, examination and assessment on their network security status and potential risks, or authorize network security service providers to do so, and submit the results and rectification plans to competent authorities in charge of the security of key information infrastructures.

Article 37 The state network and IT authorities shall make overall plan for and coordinate competent authorities to take the following measures for the security of key information infrastructures:

1. Making random risk examination on key information infrastructures followed by rectification measures and, in necessary cases, examination and assessment on network security risks conducted by authorized network security service providers;

2. Regularly organizing network security emergency response drills for operators to improve their ability to cope with network security events and coordinate;

3. Causing network security information sharing between competent authorities, operators of key information infrastructures, relevant research institutions and network security service providers; and

4. Providing technical support and assistance regarding emergency response to network security events and recovery.

Article 38 The information obtained by the state network and IT authorities and competent authorities from the protection practices of key information infrastructures shall be exclusively used for the purpose of safeguarding network security.

Chapter IV. Network Information Security

Article 39 Network operators shall establish and optimize user information protection policies to carefully protect the confidentially of such information.

Article 40 Network operators shall, in collecting and using citizens' personal information, abide by the "lawful, justifiable and necessary" principle, expressly notify the purpose, manner and scope of such collection and use, and acquire consent of the citizen whose personal information are to be collected and used.

Network operators shall not collect such personal information of citizens that are not necessarily related to the services they provide. They shall collect and use and process and store citizens' personal information in the light of laws and administrative regulations and agreements reached with the users.

Network operators shall make public their policies on the collection and use of citizens' personal information.

Article 41 Network operators shall not disclose, alter or destroy citizen's personal information collected by them, or disclose such information to others without prior consent of the citizen whose personal information have been collected, unless such information have been processed to prevent specific person from being identified and such information from being restored.

Network operators shall take technical and necessary measures to ensure the security of citizens' personal information, and protect such information from disclosure, damage or loss. In case of disclosure, damage or loss, or possible disclosure, damage or loss of such information, they shall take immediate remedies, notify the users who may be subject to the consequences, and report to competent authorities according to regulations.

Article 42 Citizens are entitled to require network operators to delete their personal information if they find the collection and use of such information violate the provisions of laws, administrative regulations or the agreement reached there between, or require the network operators to make corrections if they find errors in such information so collected and stored.

Article 43 Individuals and organizations shall not steal or obtain in illegal manners citizens' personal information, or sell or unlawfully provide such information to others.

Article 44 Authorities legitimately bearing regulatory responsibilities for network security and their staff members must carefully maintain the confidentiality of citizens' personal information, privacy and business secrets obtained during their performance of duties. They shall not disclose, sell or unlawfully provide such information to others.

Article 45 Network operators shall enhance the management of the information released to the users. In case of information prohibited by laws and administrative regulations from publication or transmission, transmission of such information shall be immediately halted and deleted to prevent dissemination, and records shall be kept and reports be made to competent authorities.

Article 46 Electronic information sent and applications provided by individuals and organizations shall be free of malicious programs and/or information prohibited by laws and administrative regulations from publication or transmission.

Providers of electronic information transmission and application download services shall assume the obligations for security management. In case the user is found of the abovementioned offenses, such services shall be immediately halted and deleted, and records shall be kept and reports be made to competent authorities.

Article 47 Network operators shall establish network information security complaint and reporting mechanisms to publish the complaint and reporting channels and timely accept and settle complaints and reports concerning network information security.

Network operators shall assist the network and IT authorities and competent authorities in lawfully conducted inspections.

Article 48 The state network and IT authorities and competent authorities shall perform regulatory responsibilities for network information security. In case of information prohibited by laws and administrative regulations from publication or transmission, they shall require the network operators to halt the transmission of, delete such information and keep the records. In case of such information from outside of the territory of the People's Republic of China, they shall notify competent organs to take technical and/or other necessary measures to block such transmission.

Chapter V. Monitoring & Warning and Emergency Response

Article 49 The State establishes network security monitoring & warning mechanism and information reporting mechanism. The state network and IT authorities shall make overall plan for and coordinate competent authorities to strengthen the collection, analysis and reporting of network security information, and release network security monitoring & warning information as specified in applicable regulations.

Article 50 Authorities in charge of the protection of key information infrastructures shall establish and perfect the network security monitoring & warning mechanism and information reporting mechanism for specific industries/disciplines within their respective jurisdiction, and report network security monitoring & warning information according to applicable regulations.

Article 51 The state network and IT authorities coordinate competent authorities to establish and perfect the network security risk assessment and emergency response mechanisms, develop emergency plans for network security events and organize drills in a regular manner.

The authorities in charge of the security of key information infrastructures shall develop emergency plans for network security events for specific industries/disciplines within their respective jurisdiction, and organize drills in a regular manner.

Such plans shall classify network security events based on their possible severity and impact, and prescribe corresponding emergency response measures.

Article 52 In case of increasing risk of network security events, governments at provincial level and above shall take the following measures according to their jurisdictions and prescribed procedures, and based on the characteristics and possible damages of such risks:

1. Requiring competent authorities, organs and personnel to promptly collect and report necessary information and intensify monitoring over network security risks;

2. Organizing competent authorities, organs and professionals to analyze and evaluate network security risks, and estimate the possibility, impact and severity of such risks; and

3. Warning the public of network security risks and release prevention and mitigation measures.

Article 53 In case of network security events, the emergency plans for network security events shall be immediately activated, investigation and assessment of such events shall be made, network operators shall take technical and necessary measures to eliminate security risks and prevent the damages from amplification, and warnings shall be made to the public.

Article 54 In the performance of their regulatory responsibilities for network security, competent authorities of the governments at provincial level and above may, pursuant to prescribed jurisdictions and procedures, arrange interview with the legal representatives or principals of the network operator concerning detected significant security risks or security events. The network operator shall take necessary measures for rectification and elimination of potential risks as required.

Article 55 In case of emergency events or production safety accidents resulted from network security events, the *Emergency Response Law of the People's Republic of China*, the *Production Safety Law of the People's Republic of China* and other competent laws and administrative regulations shall apply.

Article 56 Such interim measures as network communication restriction in specific areas may be taken following the decision of or approval by the State Council, for the purpose of safeguarding national security, maintaining public order, and dealing with significant social security emergencies.

Chapter VI. Legal Liability

Article 57 Network operators violating Articles 20 and 24 shall be warned and ordered by competent authorities to make rectifications. A fine of RMB10,000-RMB100,000 shall be imposed in case of refusal to make rectifications or severe damage to the network, and a fine of RMB5,000-RMB50,000 shall be imposed on the immediate responsible management.

Operators of key information infrastructures violating Articles 31, 32, 34 and 36 shall be warned and ordered by competent authorities to make rectifications. A fine of RMB100,000-RMB1,000,000 shall be imposed in case of refusal to make rectifications or severe damage to the network, and a fine of RMB10,000-RMB100,000 shall be imposed on the immediate responsible management.

Article 58 Violations of Articles 21.1, 21.2 and 46.1 by any of the following shall be warned and ordered by competent authorities to make rectifications. A fine of RMB50,000-RMB500,000 shall be imposed in case of refusal to make rectifications or severe damage to the network, and a fine of RMB RMB10,000-RMB100,000 shall be imposed on the immediate responsible management:

1. Setting malicious programs;

2. Failure to timely notify the user of risks such as defects or vulnerabilities of its products and/or services and to make remedies, or to report to competent authorities pursuant to regulations; and

3. Ceasing providing security maintenance for its products and/or services.

Article 59 Network operators violating Articles 23.1 by failing to obtain true identities of users or providing services to users without obtaining their true identities shall be ordered by competent authorities to make rectifications. A fine of RMB50,000-RMB500,000 shall be imposed in case of refusal to make rectifications or severe violations, and further penalties such as suspension of related business, winding up for rectification, close of website, and revocation of business license may be imposed by competent authorities. A fine of RMB10,000-RMB100,000 shall be imposed on the immediate responsible management and other immediate responsible persons.

Article 60 Network security authentication, test, risk assessment, and publication of network security information such as system vulnerabilities, computer virus, network attack and intrusion made in violation of Articles 25 shall be warned and ordered to make rectifications. A fine of RMB10,000-RMB100,000 shall be imposed in case of refusal to make rectifications or severe violations, and further penalties such as suspension of related business, winding up for rectification, close of website, and revocation of business license may be imposed by competent authorities. A fine of RMB RMB5,000-RMB50,000 shall be imposed on the immediate responsible management and other immediate responsible persons.

Article 61 Violation of Article 26 by engaging in any activities that threaten network security, or providing programs or implements for such activities or providing any help including but not limited to technical support, advertisement, payment or settlement but not constituting a crime shall be subject to confiscation of illegal earnings and detention of 5 days by the public security authority and a fine of RMB10,000-RMB100,000. Severe violation in this regard shall be subject to a detention of 5-15 days and a fine of RMB50,000-RMB500,000.

Any organization with the above violation shall be subject to confiscation of illegal earnings by the public security authority and a fine of RMB100,000-RMB500,000. The immediate responsible management and other immediate responsible persons shall be subject to penalty prescribed in Article 61.1.

Any person who has violated Article 26 and received public security administrative punishment and/or criminal penalties shall not be allowed to engage in key posts of network security and network operation for his/her lifetime.

Article 62 Network operators and providers of network products or services violating Article 21.3 and Articles 40-42 by infringing citizens' legally protected personal information shall be ordered by competent authorities to make rectification and may be subject to warning and/or, depending on the severity, confiscation of illegal earnings, a fine equivalent to one-ten times of the illegal earnings, or a fine less than RMB500,000 if there is no illegal earnings. Severe violation shall be subject to suspension of related business, winding up for rectification, close of website, and revocation of business license may be imposed by competent authorities, and the immediate responsible management and other immediate responsible persons shall be subject to a fine of RMB10,000-RMB100,000.

Violation of Article 43 by stealing or obtaining in illegal manners citizens' personal information, or sell or unlawfully provide such information to others but not constituting a crime shall be subject to confiscation of illegal earnings by the public security authority and a fine equivalent to one-ten times of the illegal earnings or a fine less than RMB500,000 if there is no illegal earnings.

Article 63 Operators of key information infrastructures violating Article 33 by using products and/or services which have not or have failed to go through the security review shall be ordered by competent authorities to halt such use and shall be subject to a fine equivalent to one-ten times of the purchase price, and the immediate responsible management and other immediate responsible persons shall be subject to a fine of RMB10,000-RMB100,000.

Article 64 Operators of key information infrastructures violating Article 35 by storing or exporting network data out of the territory of the People's Republic of China shall be warned and ordered by competent authorities to make rectifications, and shall be subject to confiscation of illegal earnings and a fine of RMB50,000-RMB500,000, and may be subject to suspension of related business, winding up for rectification, close of website, and revocation of business license, and the immediate responsible management and other immediate responsible persons shall be subject to a fine of RMB RMB10,000-RMB100,000.

Article 65 Network operators violating Article 45 by failing to halt the transmission of and delete the information prohibited by laws and administrative regulations from publication or transmission and keep the records shall be warned and ordered by competent authorities to make rectifications, and shall be subject to confiscation of illegal earnings. A fine of RMB100,000-RMB500,000 shall be imposed in case of refusal to make rectifications or severe violations, and further penalties such as suspension of related business, winding up for rectification, close of website, and revocation of business license may be imposed by competent authorities. A fine of RMB10,000-RMB100,000 shall be imposed on the immediate responsible management and other immediate responsible persons.

Providers of electronic information transmission and application download services who fail to perform the obligations prescribed in Article 46.2 shall be subject to penalty prescribed in Article 65.1.

Article 66 Network operators violating provisions of this Law by any of the following shall be warned and ordered by competent authorities to make rectifications. A fine of RMB50,000-RMB500,000 shall be imposed in case of refusal to make rectifications or severe violations and a fine of RMB10,000-RMB100,000 shall be imposed on the immediate responsible management and other immediate responsible persons.

1. Failure to report network security risks and/or events to competent authorities;

2. Failure to halt transmission of and delete the information prohibited by laws and administrative regulations from publication or transmission;

3. Refusing or impeding supervisions and/or inspections conducted by competent authorities pursuant to law; and

4. Refusing to provide technical support and/or assistance to the public security and national security authorities.

Article 67 Publication or transmission of the information prohibited by Article 12.2 and applicable laws and administrative regulations from publication or transmission shall be subject to penalties pursuant to applicable laws and administrative regulations.

Article 68 Violations of this Law shall be put into credit records and made public pursuant to applicable laws and administrative regulations.

Article 69 Operators of the government networks of state organs who fail to perform the network security obligations prescribed in this Law shall be ordered by their superior or competent authorities to make rectifications. Penalties shall be imposed on the immediate responsible management and other immediate responsible persons.

Article 70 Staff members of the authorities legitimately bearing regulatory responsibilities for network security who commit neglect of duty, abuse of authority and malpractices for personal gains which do not constitute crimes shall be subject to penalties.

Article 71 Violations of this Law which cause damage to others shall be subject to civil liabilities.

Violations of this Law which constitute violation of public security regulations shall be subject to public security administrative penalties, and violations constituting crimes shall be subject to investigations into criminal liabilities.

Chapter VII. Supplementary Provisions

Article 72 Terminology

1. Network shall refer to the system comprising computers or other information terminals and equipment that collects, stores, transmits, exchanges and processes information based on specific rules and procedures.

2. Network security shall refer to the ability to prevent network attack, intrusion, interference, damage, unauthorized use and unexpected accidents through necessary measures, in order to maintain the steady and reliable operation of network and safeguard the integrity, confidentiality and usability of network data.

3. Network operators shall refer to the owners, managers of networks and providers of network services.

4. Network data shall refer to the diverse electronic data collected, stored, transmitted, processed and generated through network.

5. Citizen's personal information shall refer to the diverse information which are recorded in electronic or other formats and used alone or in combination with other information to recognize citizens' identities, including but not limited to citizen' names, dates of birth, ID numbers, biological identities, addresses and telephone numbers.

Article 73 The operation security of networks that store and process confidential information of the State shall abide by, in addition to this Law, applicable laws and administrative regulations on confidentiality.

Article 74 Rules on the security of military networks shall be formulated by the Central Military Commission.

Article 75 This Law shall come into effect on .