# Cybersecurity Law of the People's Republic of China

| | | | |
|---|---|---|---|
| Promulgation date | 2016-11-07 | Effective region | NATIONAL |
| Promulgator | Standing Committee of the National People's Congress | Document number | Order of the President of the People's Republic of China No. 53 |
| Effectiveness | Effective | Effective date | 2017-06-01 |
| Taxonomy | Computer & Internet ( Science & Technology Law->Computer & Internet ) | | |
| Industry category | Software & Information Technology | | |

Cybersecurity Law of the People's Republic of China

Order of the President of the People's Republic of China No. 53

November 7, 2016

The Cybersecurity Law of the People's Republic of China, adopted at the 24th Session of the Standing Committee of the 12th National People's Congress on November 7, 2016, is hereby promulgated and shall come into force as of June 1, 2017.

Xi Jinping, President of the People's Republic of China

Cybersecurity Law of the People's Republic of China

(Adopted at the 24th Session of the Standing Committee of the 12th National People's Congress on November 7, 2016)

Contents



## Chapter I General Provisions

Article 1 The Cybersecurity Law of the People's Republic of China (hereinafter referred to as the "Law") is formulated for the purposes of ensuring cybersecurity, safeguarding cyberspace sovereignty, national security and public interests, protecting the legitimate rights and interests of citizens, legal persons and other organizations, and promoting the healthy development of economic and social informatization.

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

Article 3 The State adheres to equal focus on cybersecurity and information-based development, follows the guidelines of positive use, scientific development, lawful management and security assurance, promotes the construction of cyber infrastructure and its interconnection, encourages the innovation in and application of cyber technologies, supports the cultivation of talents in respect of cybersecurity, establishes and perfects the cybersecurity guarantee system and raises the ability to protect cybersecurity.

Article 4 The State shall make and continuously improve cybersecurity strategies, specify the basic requirements and main objectives for cybersecurity protection, and propose cybersecurity policies, working tasks and measures in key areas.

Article 5 The State shall take measures to monitor, defend against and deal with cybersecurity risks and threats from both within and outside the territory of the People's Republic of China, to protect critical information infrastructure from attacks, intrusions, interference and damage, to punish illegal criminal activities on the network in accordance with the law and to preserve cyberspace security and order.

Article 6 The State shall advocate honest, faithful, healthy and civilized cyber behaviors, advance the spreading of the core socialist values, and take measures to improve the awareness and level of cybersecurity of the whole of society, forming a sound environment for promoting cybersecurity with the participation of all the public.

Article 7 The State shall actively carry out international exchange and cooperation in terms of cyberspace governance, research and development of cyber technologies, establishment of the standards thereof and fighting against illegal crimes committed on the network and other aspects, promote the construction of a peaceful, safe, open and cooperative cyberspace, and establish a multilateral, democratic and transparent system for network governance.

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

Article 9 Network operators, while carrying out business and service activities, shall abide by laws and administrative regulations, show respect for social moralities, follow business ethics, act in good faith, perform the obligation of cybersecurity protection and accept supervision by the government and social public and undertake social responsibilities.

Article 10 For the construction and operation of a network or the provision of services through a network, it is a requirement to, in accordance with the provisions of laws and administrative regulations and the mandatory requirements of national standards, take technical measures and other necessary measures to ensure the secure and stable operation of the network, effectively respond to cybersecurity incidents, prevent illegal crimes committed on the network, and maintain the integrity, confidentiality and availability of cyber data.

Article 11 Cyber-related industrial organizations shall, in accordance with their regulations, intensify industrial self-discipline, formulate regulations on cybersecurity behaviors, instruct their members to strengthen cybersecurity protection, raise the level of cybersecurity protection and promote the healthy development of relevant industries.

Article 12 The State protects the rights of citizens, legal persons and other organizations to use cyberspace according to the law, promotes the popularity of network access, and raises the level of network services, so as to provide the public with secure and convenient network services and guarantee the orderly and free flow of network information in accordance with the law.
Any individual and organization using the network shall comply with the constitution and the laws, follow the public order and respect social moralities, and shall neither endanger cybersecurity, nor engage in activities by making use of the network that endanger the national security, honor and interests, incite to subvert the State power and overthrow the socialist system, incite to split the country and undermine the national unity, advocate terrorism and extremism, propaganda of ethnic hatred and discrimination, spread violent and pornographic information, fabricate or disseminate false information to disturb the economic and social order, or infringe on the fame, privacy, intellectual property and other legitimate rights and interests of others.

Article 13 The State encourages the research and development of network products and services that are favorable to minors' healthy growth and takes punitive measures against acts by making use of the network for those activities that do harm to the physical and psychological health of minors according to the law for the purpose of creating a secure and healthy network environment for minors.

Article 14 Any individual or organization shall have the right to report the behaviors that endanger cybersecurity to the cyberspace administration authorities, telecommunication departments, public security departments, etc. Any department receiving a report shall promptly handle such report in accordance with the law and transfer the report to the department with the jurisdiction if the said report is beyond its own responsibility.
Departments concerned shall maintain the confidentiality of certain information on informants and protect their legitimate rights and interests.

Chapter II Support and Promotion of Cybersecurity

Article 15 The State establishes and improves the 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 responsibilities, organize the formulation of relevant national and industrial standards for cybersecurity administration and the security of network products, services and operations and make revisions at appropriate times.
The State supports enterprises, research institutions, institutions of higher education, and network-related industrial organizations to participate in the formulation of national and industrial standards for cybersecurity.

Article 16 The State Council and the people's governments of all provinces, autonomous regions and municipalities directly under the Central Government shall conduct the overall planning, increase the input, support key cybersecurity technology industries and projects, support the research, development and application of cybersecurity technologies, promote safe and reliable network products and services, and protect the intellectual property rights of network technologies and support enterprises, research institutes, institutions of higher education to participate in national innovation projects related to cybersecurity technologies.

Article 17 The State shall boost the construction of a socialized service system for cybersecurity, and encourage enterprises and institutions concerned to provide such security services as the authentication, detection and risk evaluation of cybersecurity.

Article 18 The State shall encourage the development of technologies for protecting and using network data, promote the availability of public data resources and propel technological innovation and social and economic development.
The State supports the innovation of cybersecurity administrative methods, applying new network technologies and enhancing the level of cybersecurity protection.

Article 19 People's governments at all levels and the relevant departments thereof shall organize and provide regular publicity and education on cybersecurity, and guide, supervise and urge relevant entities to provide such publicity and education on cybersecurity in an effective way.
The mass media shall provide publicity and education on cybersecurity targeted at the public specifically.

Article 20 The State supports enterprises, institutions of higher education, vocational schools and other education training institutions to carry out cybersecurity-related education and training, adopt multiple methods to cultivate talents for cybersecurity and promote the exchange of talents for cybersecurity.

## Chapter III Network Operation Security

### Section 1 General Provisions

Article 21 The State implements the classified protection system for cybersecurity. Network operators shall fulfill the following obligations of security protection according to the requirements of the classified protection system for cybersecurity to ensure that the network is free from interference, damage or unauthorized access, and prevent network data from being divulged, stolen or falsified,
1. Formulate internal security management systems and operating instructions, determine the persons responsible for cybersecurity, and implement the responsibility for cybersecurity protection;
2. Take technological measures to prevent computer viruses, network attacks, network intrusions and other actions endangering cybersecurity;
3. Take technological measures to monitor and record the network operation status and cybersecurity incidents, and preserve relevant web logs for no less than six months according to the provisions;
4. Take measures such as data classification, and back-up and encryption of important data; and
5. Other obligations stipulated by laws and administrative regulations.

Article 22 Network products and services shall comply with the compulsory requirements of the relevant national standards. Providers of network products and services shall not install malwares; when they discover that their network products or services are subject to risks such as security defects or bugs, such providers shall take remedial measures immediately, inform users of the said risks and report the same to the relevant competent departments in accordance with the provisions.
Providers of network products and services shall provide security maintenance for their products and services; and shall not terminate the provision of security maintenance within the stipulated time limit or the time limit agreed by the parties concerned.
Where network products and services have the function of collecting users' information, the providers shall clearly notify their users and obtain their consent. In the case of involving users' personal information, the providers shall also comply with the provisions regarding the protection of personal information as stipulated by this Law, relevant laws and administrative regulations.

Article 23 Critical network equipment and specialized cybersecurity products shall, pursuant to the compulsory requirements of the relevant national standards, pass the security certification by qualified

institutions or meet the requirements of security detection before being sold or provided. The national cyberspace administration authority shall, in concert with the relevant departments under the State Council, formulate and release the catalog of critical network equipment and specialized cybersecurity products, and promote the mutual recognition of security certification and security detection results, so as to avoid repeated certifications and detections.

Article 24 When network operators handle network access and domain registration services for users, handle network access formalities for fixed-line or mobile phone users, or provide users with information publication services, instant messaging services and other services, they shall require users to provide real identity information at the time of signing agreements with users or confirming the provision of services. Where users do not provide real identify information, network operators shall not provide them with relevant services.
The State implements the strategy of trusted identities in cyberspace, supports the research and development of secure and convenient technologies for electronic identity authentication, and promotes the mutual recognition among different electronic identification authentications.

Article 25 Network operators shall formulate contingency plans for cybersecurity incidents, and promptly deal with system bugs, computer viruses, network attacks and intrusions and other security risks; when any incident endangering cybersecurity occurs, network operators shall immediately initiate contingency plans, take corresponding remedial measures, and report the same to the relevant competent departments in accordance with the provisions.

Article 26 Carrying out such activities as cybersecurity authentication, detection and risk evaluation, and releasing cybersecurity information like system bugs, computer viruses, network attacks and intrusions to society shall comply with the relevant regulations of the State.

Article 27 Any individual or organization shall neither engage in activities endangering cybersecurity, including illegally invading others' networks, interfering with the normal functions of others' networks and stealing cyber data, nor provide programs or tools specifically used for activities endangering cybersecurity, such as network intrusions, interference with the normal functions and protective measures of the network, and theft of cyber data; if such individual or organization knows that a person engages in activities jeopardizing cybersecurity, it shall not provide technical support, advertising promotion, payment and settlement services or other types of assistance to such person or organization.

Article 28 Network operators shall provide technical support and assistance to the public security organs and state security organs in lawfully safeguarding national security and investigating crimes.

Article 29 The State supports the cooperation among network operators in areas such as collection, analysis, and reporting of cybersecurity information and emergency disposal, so as to improve the ability of network operators to safeguard the security.
Relevant industrial organizations shall establish and perfect cybersecurity protection regulations and coordination mechanisms for their own industry, strengthen the analysis and evaluation of cybersecurity risks, regularly give risk warnings to their members, and support and assist members in handling cybersecurity risks.

Article 30 The information acquired by cyberspace administration authorities and relevant departments in the course of their fulfillment of responsibilities for protecting cybersecurity shall be used exclusively for the need of cybersecurity protection rather than for any other purpose.

Section 2 Operation Security of Critical Information Infrastructure

Article 31 The State shall, based on the classified protection system for cybersecurity, focus on protecting both the critical information infrastructure used for public communications and information service, energy, transport, water conservancy, finance, public services, e-government affairs and other important industries and fields and other critical information infrastructure that will result in serious damage to the national security, national economy and people's livelihood and public interests if they are destroyed, there are lost functions or they are subject to data leakage. The specific scope and measures for security protection for critical information infrastructure shall be formulated by the State Council.
The State encourages network operators other than critical information infrastructure to participate in the protective system of critical information infrastructure on a voluntary basis.

Article 32 The departments in charge of protecting the security of critical information infrastructure, in accordance with the responsibilities stipulated by the State Council, shall respectively compile and organize the implementation of critical information infrastructure security plans for their own industry and field, and guide and supervise the work related to the protection of operation security of critical information infrastructure.

Article 33 To construct the critical information infrastructure, it shall be ensured that the critical information infrastructure has properties for supporting the stable and continuous operation of the business, and that technical security measures are planned, established and used concurrently.

Article 34 In addition to the provisions of Article 21 herein, critical information infrastructure operators shall also fulfill the following obligations of security protection,
1. Set up independent security management institutions and designate persons responsible for security management, and review the security background of the said responsible persons and personnel in key positions;
2. Periodically conduct cybersecurity education, technical training and skill assessment for practitioners;
3. Make disaster recovery backups of important systems and databases;
4. Formulate contingency plans for cybersecurity incidents, and carry out drills periodically; and
5. Other obligations stipulated by laws and administrative regulations.

Article 35 Where critical information infrastructure operators purchase network products and services, which may influence national security, they shall go through a security review organized by the national cyberspace administration authority in concert with the relevant departments under the State Council.

Article 36 To purchase network products and services, critical information infrastructure operators shall enter into security confidentiality agreements with the providers in accordance with the provisions, in which obligations and responsibilities in terms of security and confidentiality shall be clarified.

Article 37 Critical information infrastructure operators shall store personal information and important data gathered and produced during operations within the territory of the People's Republic of China. Where it is really necessary to provide such information and data to overseas parties due to business requirements, a security assessment shall be conducted in accordance with the measures formulated by the national cyberspace administration authority in concert with the relevant departments under the State Council. Where the laws and administration regulations have other provisions, those provisions shall prevail.

Article 38 Critical information infrastructure operators shall conduct by themselves, or entrust cybersecurity service institutions to conduct, the detection and assessment of their cybersecurity and any potential risk at least once a year; and submit the detection and assessment situations as well as improvement measures to the relevant departments responsible for the security protection of critical information infrastructure.

Article 39 The national cyberspace administration authority shall coordinate with the relevant departments

in an overall way to take the following measures with respect to the security protection of critical information infrastructure,
1. Conduct random detection on security risks related to critical information infrastructure, and propose improvement measures; if necessary, it may entrust professional cybersecurity service institutions to carry out the detection and evaluation of any potential security risks related to the network;
2. Periodically organize critical information infrastructure operators to conduct emergency cybersecurity drills, and enhance the level and ability of coordination and cooperation to respond to cybersecurity incidents;
3. Promote cybersecurity information sharing among the relevant departments, critical information infrastructure operators, relevant research institutions and cybersecurity service institutions; and
4. Provide technical support and assistance for the emergency disposal of cybersecurity incidents and the recovery of network functions.

Chapter IV Network Information Security

Article 40 Network operators shall strictly keep confidential users' personal information that they have collected, and establish and improve the users' information protection system.

Article 41 To collect and use personal information, network operators shall follow the principles of legitimacy, rightfulness and necessity, disclose their rules of data collection and use, clearly express the purposes, means and scope of collecting and using the information, and obtain the consent of the persons whose data is gathered.
Network operators shall neither gather personal information unrelated to the services they provide, nor gather or use personal information in violation of the provisions of laws and administrative regulations or the agreements arrived at; and shall dispose of personal information they have saved in accordance with the provisions of laws and administrative regulations and agreements reached with users.

Article 42 Network operators shall not disclose, tamper with or corrupt the personal information collected by them, and shall not provide any such personal information to any other person without the consent of the person from whom the information was collected, except where information has been processed to the extent that it cannot identify a specific individual and 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 such information from being divulged, damaged or lost. If personal information has been or may be divulged, damaged or lost, it is necessary to take remedial measures immediately, inform users promptly according to the provisions and report the same to the relevant competent departments.

Article 43 Where individuals discover that network operators gather or use their personal information in violation of the provisions of laws and administrative regulations or the agreements arrived at, they have the right to request the network operators to delete their personal information; where they find that their personal information gathered or stored by network operators is subject to any mistake, they have the right to request the network operators to make corrections. Network operators shall take measures to delete or correct the said information.

Article 44 Any individual or organization may neither acquire personal information by stealing or through other illegal ways, nor illegally sell or provide personal information to others.

Article 45 The departments and their staff members responsible for the supervision and management of cybersecurity in accordance with the law shall strictly maintain the confidentiality of personal information, privacy and trade secrets known thereby in fulfilling their duties, and shall not divulge, sell or illegally provide the same to others.

Article 46 Any individual or entity shall be responsible for their use of the network, but shall neither create a website or set up a group for communications for illegal and criminal activities, such as defrauding, passing on crime methods, or producing or selling prohibited or controlled goods, nor disclose information by taking advantage of the network that is related to such illegal and criminal activities as defrauding and producing or selling prohibited or controlled goods.

Article 47 Network operators shall strengthen the management of the information published by their users, and upon discovery of the information whose publication or transmission is prohibited by the laws and administrative regulations, shall immediately stop the transmission of such information, take disposal measures such as deletion to prevent the information from spreading, save relevant records, and report the same to the relevant competent departments.

Article 48 The electronic information sent by and application software provided by any individual or organization shall neither be installed with malwares, nor contain any information whose publication or transmission is prohibited by laws and administrative regulations.
Electronic information distribution service providers and application software download service providers shall fulfill their security administration duties; and where the said providers learn that their users have conducted behaviors stipulated in the preceding paragraph, they shall stop the provision of services, take disposal measures such as deletion, keep relevant records and report the same to the relevant competent departments.

Article 49 Network operators shall set up complaint and reporting systems for network information security, disclose the ways of complaint and reporting and other information, and promptly accept and handle complaints and reports related to network information security.
Network operators shall cooperate with the supervision and detection implemented by cyberspace administration authorities and the relevant departments according to the law.

Article 50 The national cyberspace administration authority and relevant departments shall fulfill their obligations of supervising and managing cybersecurity information in accordance with the law, and upon discovery of any information whose publication or transmission is prohibited by laws and administrative regulations, shall request the network operators to stop the transmission, take disposal measures such as deletion, and keep relevant records; for the above information sourced from outside the territory of the People's Republic of China, they shall notify the relevant organizations to take technological measures and other necessary measures to block the transmission.

Chapter V Monitoring, Early Warning and Emergency Disposal

Article 51 The State shall establish a cybersecurity monitoring and early warning and information notification system. The national cyberspace administration authority shall coordinate with the relevant departments to strengthen the work on collection, analysis and notification of cybersecurity information under an overall plan, and shall uniformly release cybersecurity monitoring and early warning information in accordance with regulations.

Article 52 The departments responsible for protecting critical information infrastructure security shall establish and perfect the cybersecurity monitoring and early warning and information notification system for their respective industry or field, and submit the cybersecurity monitoring and early warning and information notification in accordance with the relevant provisions.

Article 53 The national cyberspace administration authority shall coordinate with the relevant departments to establish and perfect the cybersecurity risk evaluation and emergency work mechanism, make

contingency plans for cybersecurity incidents and organize drills periodically.
The departments responsible for protecting critical information infrastructure security shall formulate contingency plans for cybersecurity incidents for their respective industry or field, and periodically organize drills.
In cybersecurity incident contingency plans, the cybersecurity incidents shall be classified on the basis of factors such as the degree of harm and the scope of influence after the incident occurs, and corresponding emergency disposal measures shall be prescribed.

Article 54 When the probability of causing cybersecurity incidents increases, relevant departments of the people's governments at provincial level or above shall, in accordance with the authorization and procedures stipulated, adopt the following measures according to the characteristics of and possible harm from the cybersecurity risks.
1. Request the relevant departments, institutions and personnel to promptly collect and report relevant information, and strengthen the monitoring over cybersecurity risks;
2. Organize the relevant departments, institutions and professionals to analyze and assess cybersecurity risks information and predict the likelihood of the occurrence of, scope of influence of and degree of harm from the incidents; or
3. Release an early warning concerning cybersecurity risks to the public and take measures to prevent and mitigate any harm arising therefrom.

Article 55 For the occurrence of cybersecurity incidents, it is necessary to activate contingency plans for cybersecurity incidents immediately, investigate and assess such incidents, require network operators to take technical measures and other necessary measures to eliminate potential security hazards, prevent expansion of the harm, and promptly issue warning information in relation to the public to society.

Article 56 The relevant departments of the people's governments at provincial level or above may hold an interview with the legal representatives or principals of the network operators in accordance with prescribed authorizations and procedures upon discovery of relatively high security risks or security incidents on the network. Network operators shall take measures to effect rectification and eliminate hidden dangers as required.

Article 57 Emergency incidents or work safety accidents caused by cybersecurity incidents shall be handled in accordance with the Emergency Response Law of the People's Republic of China, the Work Safety Law of the People's Republic of China and other relevant laws and administrative regulations.

Article 58 In the case of demands to protect the national security and social public order, and respond to major social emergent security incidents, upon the decision or approval by the State Council, the competent departments may take restriction and other temporary measures on network communications within specific regions.

## Chapter VI Legal Liability

Article 59 Network operators, who fail to perform the obligation of protecting cybersecurity as stipulated by Article 21 or Article 25 of this Law, shall be ordered to effect rectification and be warned by the relevant competent departments. Where they refuse to effect rectification, or such consequences as endangering cybersecurity are caused, a fine of no less than CNY10,000 but no more than CNY100,000 shall be imposed; as for the persons directly in charge, a fine of no less than CNY5,000 but no more than CNY50,000 shall be imposed.
Operators of critical information infrastructure who fail to perform the obligation of cybersecurity protection as stipulated by Article 33, Article 34, Article 36 and Article 38 of this Law, shall be ordered to effect rectification and be given a warning. Where they refuse to effect rectification, or such consequences as

endangering cybersecurity are caused, a fine of no less than CNY100,000 but no more than CNY1 million shall be imposed; as for the persons directly in charge, a fine of no less than CNY10,000 but no more than CNY100,000 shall be imposed.

Article 60 Where any person conducts any of the following acts in violation of Paragraph 1 and Paragraph 2 of Article 22, Paragraph 1 of Article 48 hereof, he shall be ordered to effect rectification and be warned by the relevant competent departments; where he refuses to effect rectification or such consequences as endangering cybersecurity are caused, a fine of no less than CNY50,000 but no more than CNY500,000 shall be imposed; as for the persons directly in charge, a fine of no less than CNY10,000 but no more than CNY100,000 shall be imposed,

1. Installing malwares;
2. Failing to take remedial measures immediately against risks, such as security defects and bugs of their products or services; or failing to promptly inform users of such risks and reporting the same to the relevant competent departments in accordance with the relevant provisions; or
3. Arbitrarily terminating the provision of security maintenance for their products and services.

Article 61 Network operators who in violation of Paragraph 1 of Article 24 hereof, fail to request users to provide authentic identity information, or provide services for those failing to provide authentic identity information, shall be ordered to effect rectification by the relevant competent departments; where they refuse to effect rectification or if the circumstances are serious, a fine of no less than CNY50,000 but no more than CNY500,000 shall be imposed, and the relevant competent departments may order them to suspend operation, stop doing business for internal rectification, close down the website, or may revoke relevant business permits or their business licenses; and a fine of no less than CNY10,000 but no more than CNY100,000 shall be imposed on the persons directly in charge and other directly responsible persons.

Article 62 Anyone that carries out cybersecurity authentication, detection, risk evaluation and other activities or released system bugs, computer viruses, network attacks and intrusions and other cybersecurity information to the public in violation of Article 26 hereof, shall be ordered by the relevant competent departments to make rectification; where they refuse to make rectification or if the circumstances are serious, a fine of between CNY10,000 and CNY100,000 shall be imposed, and the relevant competent departments may order them to suspend the relevant operation, suspend business for internal rectification, close down the website, or may revoke the relevant business permits or their business licenses; and a fine of between CNY5,000 and CNY50,000 shall be imposed on any directly liable manager or any other directly liable person.

Article 63 Where, in violation of Article 27 hereof, anyone is engaged in activities endangering cybersecurity, provides programs or tools specifically used for conducting activities endangering cybersecurity, or provides technical support, advertising promotion, payment and settlement support or other kinds of assistance to others for conducting activities endangering cybersecurity, if such activities do not constitute a crime, public security organs shall confiscate their illegal gains, enforce detention of up to five days and may, in addition, impose a fine of between CNY50,000 and CNY500,000, and if the circumstances are serious, the period of detention shall be no less than 5 days but no more than 15 days and, in addition, the fine imposed may be no less than CNY100,000 but no more than CNY1,000,000.

Where an entity commits any of the violations stipulated in the preceding paragraph, public security organs shall confiscate its illegal gains, impose a fine of no less than CNY100,000 but no more than CNY1,000,000, and punish the persons directly in charge and the other directly responsible persons in accordance with the provisions of the preceding paragraph.

Any person who violates Article 27 hereof shall be forbidden from practicing cybersecurity management and taking key positions in the field of network operation either within five years if he or she is subject to public security punishment or for life if he or she is subject to criminal punishment.

Article 64 Where, in violation of the third paragraph of Article 22 or Article 41, 42 or 43 of the Law, a network operator or provider of any cyber product or service commits an infringement of any personal information right that is legally protected, the competent authority shall order it to make rectification, and may, depending on the circumstances of the case, impose on it separately or combined, a warning, the confiscation of illegal gains, and a fine of between one and ten times the illegal gains, or a fine of up to CNY1 million if there is no illegal gain; impose a fine of between CNY10,000 and CNY100,000 on any directly liable manager or any other directly liable person of the organization; and may, if the circumstances are serious, order it to suspend the relevant business, suspend business for rectification, or close down the website, or revoke its relevant business permit or its business license.
In the case of a theft of or otherwise illegal acquisition, or illegal sale or illegal provision of personal information to another in violation of Article 44 of the Law that does not constitute a criminal offense, the person committing the violation shall be confiscated of the illegal gains and subject to a fine of between one and ten times the illegal gains or a fine of up to CNY1 million if there are no illegal gains by the public security.

Article 65 Where operators of critical information infrastructures, in violation of Article 35 hereof, use network products or services that have neither been examined for security nor passed the security examination, they shall be ordered by the relevant competent departments to stop using such products or services, and a fine of no less than one but no more than ten times the purchase amount shall be imposed; as for the persons directly in charge or other directly responsible persons, a fine of no less than CNY10,000 but no more than CNY100,000 shall be imposed.

Article 66 Operators of critical information infrastructures who, in violation of Article 37 hereof, store network data overseas, or provide network data overseas, the relevant competent departments shall order them to effect rectification, give a warning, confiscate illegal gains, and impose a fine of no less than CNY50,000 but no more than CNY500,000; and may order them to suspend relevant business, stop business for rectification, close down the website, or revoke the relevant business permits or their business licenses; as for the persons directly in charge or other directly responsible persons, a fine of no less than CNY10,000 but no more than CNY100,000 shall be imposed.

Article 67 For network operators who violate Article 46 hereof by creating a website or setting up a communications group for illegal or criminal activities, or disclosing information by making use of the network that relates to any illegal or criminal activity to be committed, if such activities do not constitute a crime, public security organs shall put them into detention for up to five days and may, in addition, impose a fine of no less than CNY10,000 but no more than CNY100,000; and if the circumstances are serious, such operators shall be detained for no less than 5 days but no more than 15 days and may, in addition, be fined no less than CNY50,000 but no more than CNY500,000. Websites and communication groups used for conducting illegal and criminal activities shall be closed down.
Where an entity commits any of the violations stipulated in the preceding paragraph, public security organs shall confiscate its illegal gains, impose a fine of no less than CNY100,000 but no more than CNY500,000, and punish the persons directly in charge and the other directly responsible persons in accordance with the provisions of the preceding paragraph.

Article 68 Network operators, who, in violation of Article 47 hereof, fail to stop transmitting or take disposal measures to remove the information, or save relevant records regarding information that the relevant departments prohibit from being published or transmitted, they shall be ordered to effect rectification and be given a warning, and their illegal gains shall be confiscated by the relevant competent departments; where the operators refuse to effect rectification or the circumstances are serious, a fine of no less than CNY100,000 but no more than CNY500,000 shall be imposed, and they may be ordered to suspend relevant business, stop business for rectification or close down the website, and the relevant business permits or their business licenses may be revoked; as for the persons directly in charge and other directly responsible

persons, a fine of no less than CNY10,000 but no more than CNY100,000 shall be imposed.
Electronic messaging service providers or application software download service providers who fail to fulfill their security management obligations stipulated in Paragraph 2 of Article 48 hereof, shall be punished in accordance with the preceding paragraph.

Article 69 Network operators who, in violation of the provisions hereof, conduct any of the following acts shall be ordered to effect rectification by the competent departments; where they refuse to effect rectification, or the circumstances are serious, a fine of no less than CNY50,000 but no more than CNY500,000 shall be imposed; as for the persons directly in charge or other directly responsible persons, a fine of no less than CNY10,000 but no more than CNY100,000 shall be imposed,
1. Fail to take disposal measures such as stopping transmission or removing information whose publication or transmission is prohibited by the laws or administrative regulations as required by the relevant departments.
2. Refuse or impede the supervision and detection implemented by the relevant departments according to the law; or
3. Refuse to provide technical support and assistance to public security organs and state security organs.

Article 70 Releasing or transmitting information whose publication or transmission is prohibited by Paragraph 2 of Article 12 hereof, or by other laws or administrative regulations, shall be punished in accordance with the provisions of the relevant laws and administrative regulations.

Article 71 Any violation as stipulated in this Law shall be recorded in the credit files in accordance with the provisions of the relevant laws and administrative regulations and be publicized.

Article 72 Where operators of government affairs networks for state organs fail to perform their obligation of cybersecurity protection as stipulated in this Law, their administrations at the next higher level or relevant administrations shall order them to effect rectification and impose sanctions on the persons directly in charge and other directly responsible persons.

Article 73 Where cyberspace administration departments and the relevant departments violate Article 30 hereof by using information acquired when they fulfill their responsibilities for cybersecurity protection for any other purpose, sanctions shall be imposed on the persons directly in charge and other directly responsible persons.
Where a functionary in the cyberspace administration departments or relevant departments, neglects his duty, abuses his power, and seeks personal gains in his work, but does not constitute a crime, he shall be imposed sanctions according to the law.

Article 74 For a violation of the provisions hereof which causes damage to others, civil liabilities shall be borne in accordance with the law.
For a violation of the provisions hereof which constitutes a violation of public security administration, a public security administration punishment 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 any overseas organization, institution or individual engages in any activity that endangers critical information infrastructure of the People's Republic of China through attacks, invasions, interference or destruction, and results in serious consequences, it shall be investigated for its liabilities according to the law; the public security organ of the State Council and relevant departments may decide to freeze the assets of such organization, institution or individual or take other necessary punitive measures against it.

Chapter VII Supplementary Provisions

Article 76 For the purpose of the Law, the following terms shall have the following meanings ascribed

thereto,
1. Cyber refers to the system that is constituted by computers or other information terminals and relevant equipment to collect, save, transmit, exchange, and process information.
2. Cybersecurity refers to taking necessary measures to prevent attacks, intrusions, interference, sabotage on the network, illicit use of the network, and accidents, to make sure the network is under stable and reliable operation conditions, and the capabilities for ensuring the integrity, confidentiality and availability of the network data.
3. Network operators refer to owners, administrators of the network and network service providers.
4. Network data refers to all kinds of electronic data collected, saved, transmitted, processed and generated through the network.
5. Personal information refers to all kinds of information recorded by electronic or otherwise that can be used to independently identify or be combined with other information to identify natural persons' personal information including but not limited to: natural persons' names, dates of birth, ID numbers, biologically identified personal information, addresses and telephone numbers, etc.

Article 77 For the protection of the operation security of the network, and saving or processing of information involving state secrets, the provisions of laws and administrative regulations concerning confidentiality shall be complied with in addition to this Law.

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

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