Cybersecurity Law of the People's Republic of China (2016)

English translation of the Cybersecurity Law of the People's Republic of China (中华人民共和国网络安全法), created by weber.cloud China

The original legal text can be viewed at http://www.cac.gov.cn/2016-11/07/c_1119867116.htm.

weber.cloud China is a brand of
weber.digital GmbH
Bahnhofstraße 16, 72336 Balingen
Germany

Phone +49 7433 21021-0
Web www.webercloud-china.com
Email info@weber.cloud

Managing Director
Jürgen Weber

Registered office Balingen
CR Amtsgericht Stuttgart
Register No. HRB 411104
VAT No. DE812928233

Bank details
Sparkasse Zollernalb
Account No. 24 055 969, BC 653 512 60
IBAN DE53 6535 1260 0024 0559 69
SWIFT/BIC code SOLA DE S1 BAL

Landesbank Baden-Württemberg
Account No. 24 601 29, BC 600 501 01
IBAN DE40 6005 0101 0002 4601 29
SWIFT/BIC code SOLA DE ST

Cybersecurity Law of the People's Republic of China (2016)

Chapter I. General Provisions

Article 1
This Law is developed for the purposes of guaranteeing cybersecurity, safeguarding cyberspace sovereignty, national security and public interest, protecting 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 the network as well as the supervision and administration of cybersecurity in the territory of the People's Republic of China.

Article 3
The state shall insist on cybersecurity and information-based development, follow the guidelines of positive use, scientific development, legal management and security guarantee, promote the construction of network infrastructure and interconnection, encourage the innovation and application of network technologies, support the training of cybersecurity personnel, establish and improve the cybersecurity guarantee system, and enhance the capability to protect cybersecurity.

Article 4
The state shall enact and continuously improve cybersecurity strategies, specify the basic requirements and major objectives for guaranteeing cybersecurity, and propose cybersecurity policies, work 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 inside and outside the territory of the People's Republic of China, protect critical information infrastructure from attacks, intrusions, interference and damage, punish cyber illegal criminal activities in accordance with the law, and maintain cyberspace security and order.

Article 6
The state shall advocate honest, trustworthy, healthy and civilized network behavior, advance the spreading of core socialist values, and take measures to enhance the awareness and level of cybersecurity of the entire society, so as to form a favorable environment for promoting cybersecurity with the participation of the entire society.

Article 7
The state shall actively carry out international exchange and cooperation in terms of cyberspace governance, research and development of network technologies, formulation of standards thereof, and combating cyber crimes, promote the construction of a peaceful, safe, open and cooperative cyberspace, and establish a multilateral, democratic and transparent system for cyber governance.

Cybersecurity Law of the People's Republic of China (2016)

Article 8
The national cyberspace administration shall be responsible for the overall planning and coordination of cybersecurity work and relevant supervision and administration. The relevant telecommunications department of the State Council, public security departments and other relevant authorities shall be responsible for cybersecurity protection, supervision and administration within the scope of their respective functions in accordance with the provisions of this Law and other relevant laws and administrative regulations.

The cybersecurity protection, supervision and administration functions of relevant departments of local people's governments at or above the county level shall be determined in accordance with relevant provisions of the state.

Article 9
Network operators shall, when conducting business operations and providing services, abide by laws and administrative regulations, respect social morality, observe business ethics, be honest and trustworthy, perform the cybersecurity protection obligation, accept supervision by the government and the public, and assume social responsibilities.

Article 10
For the construction and operation of the network or the provision of services through the network, technical measures and other necessary measures shall be taken in accordance with the provisions of laws and administrative regulations and the mandatory requirements of national standards to ensure network security, stable operation, and effective respond to cybersecurity incidents, prevent illegal criminal activities committed on the network, and maintain the integrity, confidentiality and availability of network data.

Article 11
Network-related industry organizations shall, in accordance with their constitutions, intensify industry self-regulation, formulate codes of conduct on cybersecurity, direct their members to strengthen 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 the network in accordance with the law, promote the popularity of network access, improve the level of network services, provide the public with safe and convenient network services, and guarantee the orderly and free flow of network information in accordance with the law.

Any individual or organization using the Internet shall comply with the Constitution and laws, follow public order and respect social ethics, shall not endanger cybersecurity, and shall not use the Internet to conduct any activity that endangers national security, integrity and interest, incites to subvert the state power or overthrow the socialist system, incites to split the country or undermine national unity, advocates terrorism or extremism, propagates ethnic hatred or discrimination, spreads violent or pornographic information, fabricates or disseminates false

Cybersecurity Law of the People's Republic of China (2016)

information to disrupt the economic and social order, or infringes upon the reputation, privacy, intellectual property rights or other lawful rights and interests of any other person.

Article 13
The state shall support the research and development of online products and services that are conducive to the healthy growth of minors, legally punish the activities that damage the physical and mental health of minors by using the Internet and provide a safe and healthy network environment for minors.

Article 14
Any individual or organization shall have the right to report acts that endanger cybersecurity to the cyberspace administration, telecommunications department, public security authority, and other departments. The department that receives the report shall handle such a report in a timely manner in accordance with the law or transfer the report to the competent department in a timely manner if it falls outside its responsibility.

The relevant department shall keep the information on the informant confidential and protect the informant's lawful rights and interests.

Cybersecurity Law of the People's Republic of China (2016)

Chapter II. Cybersecurity Support and Promotion

Article 15
The state shall establish and improve the system of cybersecurity standards. The standardization administrative department of the State Council and other relevant departments of the State Council shall, in accordance with their respective responsibilities, organize the formulation and timely revision of national and industry standards relating to cybersecurity administration and the security of network products, services and operations.

The state shall support enterprises, research institutions, institutions of higher learning, and network-related industry organizations in participating in the formulation of national and industry standards on cybersecurity.

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

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

Article 18
The state shall encourage the development of technologies for protecting and using network data, promote the availability of public data resources, and promote technological innovation and social and economic development.

The state shall support the innovation of cybersecurity management methods and the application of new network technologies to enhance cybersecurity protection.

Article 19
People's governments at all levels and their relevant departments shall organize regular cybersecurity publicity and education, and direct and urge relevant entities to conduct cybersecurity publicity and education in an effective manner.

Mass media shall offer relevant cybersecurity publicity and education to the public.

Cybersecurity Law of the People's Republic of China (2016)

Article 20
The state shall provide support to enterprises, institutions of higher learning, vocational schools and other education training institutions to conduct cybersecurity-related education and training, take multiple ways to train network security personnel, and promote the exchange of network security personnel.

Cybersecurity Law of the People's Republic of China (2016)

Chapter III. Network Operation Security

Section 1: General Provisions

Article 21

The state shall implement a cybersecurity level protection system. Network operators shall, in accordance with the requirements of the cybersecurity level protection system, fulfill the following security protection obligations, to ensure that the network is free from interference, damage or unauthorized access, and prevent network data from being leaked, stolen or falsified:

(1) Developing internal security management rules and operating procedures, determining the persons in charge of cybersecurity, and implementing cybersecurity protection responsibilities.

(2) Taking technical measures to prevent computer viruses, network attack, network intrusion and other acts endangering cybersecurity.

(3) Taking technical measures to monitor and record the status of network operation and cybersecurity incidents and preserving relevant weblogs for not less than six months as required.

(4) Taking measures such as data categorization, and back-up and encryption of important data.

(5) Performing other obligations as 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 malware. When a provider discovers any risk such as security defect and vulnerability of its network products or services, it shall immediately take remedial measures, inform users in a timely manner, and report it to the competent department in accordance with relevant provisions.

Providers of network products and services shall continuously provide security maintenance for their products and services and shall not terminate the provision of security maintenance within the specified or agreed period upon by the parties.

Where network products and services have the function of collecting users' information, their providers shall explicitly notify their users and obtain their consent. If any user's personal information is involved, the provider shall also comply with this Law and the provisions of relevant laws and administrative regulations on the protection of personal information.

Article 23

Key network equipment and specialized cybersecurity products shall, in accordance with the compulsory requirements of relevant national standards, pass the security certification conducted by qualified institutions or meet the requirements of security detection before being sold or provided. The national cyberspace administration shall, in conjunction with relevant departments of the State Council, develop and release the catalogue of key network equipment and specialized cybersecurity products, and promote the mutual recognition of security certification and security testing results to avoid repeated certification and testing.

Cybersecurity Law of the People's Republic of China (2016)

Article 24
Where network operators provide network access and domain registration services for users, handle network access formalities for landline or mobile phone users, or provide users with information release services, instant messaging services and other services, they shall require users to provide real identity information when signing agreements or confirming the provision of services. If any user fails to provide his or her real identify information, the network operator shall not provide him or her with relevant services.

The state shall implement the strategy of trusted identity in cyberspace, support the research and development of safe and convenient technologies for electronic identity authentication, and promote mutual recognition among different electronic identity authentication technologies.

Article 25
Network operators shall make emergency response plans for cybersecurity incidents, and deal with system bugs, computer viruses, network attack, network intrusion and other security risks in a timely manner. When any incident endangering cybersecurity occurs, the relevant operator shall immediately initiate the emergency response plan, take corresponding remedial measures, and report it to the competent department in accordance with relevant provisions.

Article 26
Activities such as cybersecurity certification, testing and risk assessment shall be conducted, and cybersecurity information on system bugs, computer viruses, network attack, and network intrusion, among others, shall be released to the public in accordance with relevant provisions of the state.

Article 27
Any individual and organization shall not engage in illegal intrusion into other people's networks, interference with the normal functions of other networks, theft of network data and other activities that endanger network security; shall not provide programs and tools specifically designed to engage in network intrusion, interference with the normal functions of the network and protective measures, theft of network data and other activities that endanger network security; knowing that others are engaged in activities that endanger network security, they shall not provide technical support, advertising and promotion, payment settlement and other assistance.

Article 28
Network operators shall provide technological support and assistance to public security organs and national security organs acting to maintain national security and to investigate crime.

Article 29
The State supports cooperation between network operators in areas such as collecting, analyzing, reporting and responding to cybersecurity information, to increase the security safeguard capacity of network operators.

Cybersecurity Law of the People's Republic of China (2016)

Relevant industry organizations shall establish cybersecurity protection rules and coordination mechanisms for their industry, strengthen their analysis and evaluation of cybersecurity, and within a designated period shall undertake risk warnings for members, and shall support and coordinate members' responses to cybersecurity risks.

Article 30
Information obtained by the cybersecurity and informatization department and relevant departments when carrying out cybersecurity protection duties, may only be used for cybersecurity needs, and may not be used for other purposes.

Section 2: Operations Security For Critical Information Infrastructure

Article 31
The State implements focus protection for critical information infrastructure in important sectors and areas such as public telecommunications and information services, energy, transportation, water resources, finance, public services, e-government, etc., as well as other critical information infrastructure that, whenever it is destroyed, loses its ability to function or encounters data leaks, may gravely harm national security, the national economy, the people's livelihood and the public interest, on the basis of the cybersecurity level protection system. The concrete scopes of critical information infrastructure and security protection rules are formulated by the State Council.

The State encourages network operators outside of critical information infrastructure to voluntarily participate in the critical information infrastructure protection system.

Article 32
In accordance with responsibilities provided by the State Council, departments responsible for the security protection of critical information infrastructure respectively formulate and organize the implementation of critical information infrastructure security plans for that industry or field, and guide and supervise the security protection efforts for critical information infrastructure.

Article 33
The construction of critical information infrastructure shall ensure that it has the capability of supporting business stability and sustained operations, and ensures that technical security measures are planned, established and used concurrently.

Article 34
In addition to the provisions of Article 21 of this Law, critical information infrastructure operators shall perform the following security protection duties:
(1) Set up specialized security management institutions and persons responsible for security management, and conduct security background checks on those responsible persons and personnel in critical positions;
(2) Periodically conduct cybersecurity education, technical training and skills assessment for employees;
(3) Conduct disaster backups of important systems and databases;

Cybersecurity Law of the People's Republic of China (2016)

(4) Formulate emergency response plans for cybersecurity incidents, and periodically organize drills;
(5) Other obligations as provided by law or administrative regulations.

Article 35
Critical information infrastructure operators purchasing network products and services that might influence national security shall go through a security inspection organized by the national cyberspace administration and relevant departments of the State Council.

Article 36
Critical information infrastructure operators purchasing network products and services shall sign a security confidentiality agreement with the providers according to regulations, clarifying duties and responsibilities for security and confidentiality.

Article 37
Personal information and important business data collected and produced by critical information infrastructure operators during their activities within the territory of the People's Republic of China, shall be stored within the territory; where due to business requirements it is truly necessary to provide it outside the mainland, a security assessment shall be conducted according to the measures jointly formulated by the national cyberspace administration and the relevant departments of the State Council. Where laws or administrative regulations provide otherwise, those provisions apply.

Article 38
At least once a year, critical information infrastructure operators shall conduct an inspection and assessment of their networks security and risks that might exist either on their own, or through retaining a specialized organization; and report the monitoring and assessment situation as well as improvement measures to the relevant department responsible for security protection of critical information infrastructure.

Article 39
The State cybersecurity and informatization department shall comprehensively coordinate relevant departments to adopt the following measures in order to protect the security of critical information infrastructure:
(1) Conduct spot testing of critical information infrastructure security risks, propose measures for improvement, and when necessary to do so may appoint a cybersecurity specialist inspection and detection institutions to undertake testing and evaluation for security risks;
(2) Periodically organize operators of critical information infrastructure to conduct cybersecurity emergency drills, increasing the level of responses and coordination of responses to cybersecurity incidents;
(3) Promote cybersecurity information sharing among relevant departments, the operators of critical information infrastructure, cybersecurity services institutions and relevant research institutions;

Cybersecurity Law of the People's Republic of China (2016)

(4) Provide technical support and assistance for cybersecurity emergency management and recovery etc.

Cybersecurity Law of the People's Republic of China (2016)

Chapter IV. Network Information Security

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

Article 41
Network operators collecting and using personal information shall abide by the principles of legality, legitimacy and necessity, publish their rules for its collection and use, explicitly stating the purposes, means and scope for collecting or using information, and obtaining the consent of the person whose data is gathered.

Network operators must not gather personal information unrelated to the services they provide; must not violate the provisions of laws, administrative regulations or agreements between the parties to gather or use personal information; and shall follow the provisions of laws, administrative regulations or agreements with users to process personal information they have saved.

Article 42
Network operators must not disclose, distort or damage personal information they collect; without the agreement of the person whose information is collected, personal information may not be provided to others. Except where it has been processed in such a manner that it is impossible to distinguish a particular individual and it cannot be retraced.

Network operators shall adopt technological and other necessary measures to ensure the security of personal information they collect, and prevent information leaks, damage or loss. Where a situation of information leakage, damage or loss occurs, or might have occurred, they shall promptly take remedial measures, timely notify users and report the matter to the competent departments in accordance with regulations.

Article 43
Where an individual discovers network operators have violated the provisions of laws, administrative regulations or agreements between the parties in collecting or using their personal information, they have the right to request the network operators to delete their personal information; where discovering that personal information gathered or stored by network operators contains errors, they have the right to request the network operators to make corrections. Network operators shall adopt measures for deletion or correction.

Article 44
Individual or organization must not steal or use other illegal methods to acquire personal information and must not sell or unlawfully provide others with citizens' personal information.

Cybersecurity Law of the People's Republic of China (2016)

Article 45
Departments and their personnel with duties in cybersecurity supervision and management in accordance with law, must keep personal information, private information and commercial secrets they learn of in performing their duties strictly confidential, and must not leak, sell, or unlawfully provide it to others.

Article 46
Any person and organization shall, when using the Internet, be responsible for their actions. They must not allow to establish websites or communications groups used to commit fraud, disseminate criminal methods, produce or sell prohibited or controlled goods, or other such unlawful and criminal activities, they may not use the network to disseminate information concerning committing fraud, producing or selling prohibited controlled goods, or other such unlawful and criminal activities.

Article 47
Network operators shall strengthen management of information published by users, and where they discover information of which the publication or dissemination is prohibited by laws and regulations, they shall immediately stop dissemination of that information, take measures such as deleting it, prevent the information from spreading, save relevant records, and report to the relevant departments in charge.

Article 48
No electronic information sent or application software provided by any individual or organization may install malicious programs, or may contain information that laws and administrative regulations prohibit the publication or transmission of.

Electronic information distribution service providers and application software download service providers shall perform security administration duties; where they know their users commit actions as provided in the previous Paragraph, they shall stop the providing services and take measures such as deletion, save relevant records and report to the relevant departments in charge.

Article 49
Network operators shall establish network information security complaint and reporting systems, publicly disclosing information such as the methods for making complaints or reports, and promptly accepting and handling complaints and reports relevant to network information security.

Network operators shall cooperate with the cybersecurity and informatization departments and relevant departments conducting monitoring and investigations according to the law.

Article 50
The national cyberspace administration and relevant departments shall perform cybersecurity supervision and administration responsibilities in accordance with the law; and where discovering information, the release or transmission of which is prohibited by laws of administrative regulations, shall request the network operators to stop transmission, take disposal measures such

Cybersecurity Law of the People's Republic of China (2016)

as deletion, and save relevant records; for information described above that comes from outside the People's Republic of China, they shall notify the relevant institutions to take technological measures and other necessary measures to block the transmission of information.

Cybersecurity Law of the People's Republic of China (2016)

Chapter V. Monitoring, Early Warnings and Emergency Response

Article 51
The State establishes cybersecurity monitoring and early warning and information notification systems. The national cyberspace administration shall do overall coordination of relevant departments to strengthen collection, analysis and reporting efforts for cybersecurity information, and release unified cybersecurity monitoring and early warning information in accordance with regulations.

Article 52
Departments responsible for critical information infrastructure security protection efforts shall establish and improve cybersecurity monitoring and early warning and information reporting systems for their respective industry or field, and report cybersecurity monitoring and early warning information in accordance with regulations.

Article 53
The national cyberspace administration coordinates relevant departments to establish and improve mechanisms for cybersecurity risk assessment and emergency response efforts, formulate cybersecurity incident emergency response plans, and periodically organize drills.

Departments responsible for critical information infrastructure security protection efforts shall formulate cybersecurity incident emergency response plans for their respective industry or field, and periodically organize drills.

Cybersecurity incident emergency response plans shall rank cybersecurity incidents on the basis of factors such as the degree of threat after the incident occurs and the scope of impact and provide corresponding emergency response handling measures.

Article 54
When cybersecurity incidents are about to occur or where their probability of occurring increases, relevant departments of people's governments at the provincial level and above shall, in accordance with the prescribed competences and procedures and the characteristics of the cybersecurity risk and the harm it may cause, take the following measures:
(1) Require that relevant departments, institutions and personnel promptly gather and report relevant information and strengthen the monitoring of cybersecurity risks;
(2) Organize relevant departments, institutions and specialist personnel to undertake analysis and evaluation of data from the cybersecurity incidents, and predict the incidents' likelihood of occurrence, scope of impact and level of harm;
(3) Issue warnings about the cybersecurity risks to society, and publish measures to avoid or mitigate harm.

Article 55
On occurrence of cybersecurity incidents, the cybersecurity incident emergency response plan shall

Cybersecurity Law of the People's Republic of China (2016)

be immediately initiated, an evaluation and assessment of the cybersecurity incident shall be conducted, network operators will be requested to adopt technological and other necessary measures, potential security shall be removed, the threat shall be prevented from growing, and warnings promptly released to the public.

Article 56
Where relevant departments of people's governments at the provincial level or above, in the process of carrying out their cybersecurity supervision and management duties, discover that networks have a large security risk or they discover security incidents, they may, in accordance with the prescribed competence and procedures, conduct an interview with the legal representative or the main responsible persons for the operator of that network. Network operators shall take measures to rectify the situation and eliminate dangers in accordance with the requirements.

Article 57
Where sudden emergencies or production safety accidents occur because of cybersecurity incidents, it shall be handled in accordance with the "Emergency Response Law of the People's Republic of China" and the "Production Safety Law of the People's Republic of China" and other relevant laws and administrative regulations.

Article 58
To fulfill the need to protect national security and social public order, and to respond to major social security incidents, temporary measures, with the approval or by the decision of the State Council, regarding network communications in certain regions may be taken, such as restricting it.

Cybersecurity Law of the People's Republic of China (2016)

Chapter VI. Legal Responsibility

Article 59
Where network operators fail to fulfill its obligations to protect network security as provided for in Articles 21 and 25 of this Law, the relevant departments will order corrections and give warnings; where corrections are refused or it leads to endangerment of cybersecurity or other such consequences, a fine of between 10.000 yuan and 100.000 yuan shall be imposed; and the directly responsible management personnel shall be fined between 5.000 yuan and 50.000 yuan.

Where critical information infrastructure operators do not perform cybersecurity protection duties provided for in Articles 33, 34, 36 and 38 of this Law, the relevant departments will order corrections and give warnings; where corrections are refused or it leads to endangerment of cybersecurity or other such consequences, a fine of between 100.000 yuan and 1.000.000 yuan shall be imposed; and the directly responsible management personnel shall be fined between 10.000 yuan and 100.000 yuan.

Article 60
Where, in violation of the provisions of Article 22 Paragraphs 1 and 2, or Article 48 Paragraph I, one of the following acts occurs, the relevant competent department orders corrections and gives warnings; where corrections are refused or it causes endangerment of cybersecurity or other consequences, a fine of between 50.000 yuan and 500.000 yuan shall be imposed; and the persons who are directly in charge are fined between 10.000 yuan and 100.000 yuan:
(1) Installing malicious programs;
(2) Where risks such as security flaws or vulnerabilities exist in their products or services, but they do not immediately take remedial measures, or not timely inform users and report the matter to the relevant controlling departments in accordance with regulations;
(3) Unauthorized termination of the security maintenance of its products and services.

Article 61
Network operators violating the provisions of Article 24 Paragraph 1 of this Law in failing to require users to provide real identity information or providing relevant services to users who do not provide real identity information, are ordered to make corrections by the relevant competent department; where corrections are refused or if the circumstances are serious, a fine of between 50.000 yuan and 500.000 yuan is imposed, and the relevant competent department may order a temporary suspension of operations, a suspension of business for corrections, closing down of websites, revocation of relevant operations permits, or the cancellation of business licenses; persons who are directly in charge and other directly responsible personnel are fined between 10.000 yuan and 100.000 yuan.

Article 62
Those who, in violation of the provisions of Article 26 of this Law, conduct cybersecurity certification, testing or risk assessments, or publish cybersecurity information such as system leaks, computer viruses, cyber-attacks, etc. to society, will be ordered to rectify matters and be

Cybersecurity Law of the People's Republic of China (2016)

given a warning by the relevant competent departments; where rectification is refused or if the circumstances are serious, a fine of 10.000 yuan to 100.000 yuan is imposed, and the relevant controlling department is permitted to order a temporary suspension of business, a suspension of business for rectification, the closure of websites, cancellation of relevant business permits or revocation of the business licence; directly responsible persons in charge and other directly responsible shall be fined not less than 5.000 yuan but not more than 50.000 yuan.

Article 63
Those who, in violation of the provisions of Article 27 of this Law, engage in activities harming cybersecurity, or provide programs or tools for the special purpose of engaging in acts harming cybersecurity, or provide technological support, advertising and promotion, payment, accounting and other such forms of assistance to others engaging in acts harming in cybersecurity, where it does not yet constitute a crime, will have their unlawful income confiscated by the public security organs, and are sentenced to five days or less of detention, and a fine of 50.000 to 500.000 yuan may additionally be imposed; where circumstances are serious, they are to be punished by five to fifteen days of detention, and additionally a fine of 100.000 yuan to 1.000.000 yuan may be imposed.

Where units commit acts as provided in the previous paragraph, the public security organ confiscates the unlawful income, imposes a fine of 100.000 to 1.000.000 yuan, and fines the directly responsible person in charge and other responsible persons according to the provisions of the previous Paragraph.

Persons who violate the provisions of Article 27 of this Law and are subject to public security management penalties shall not be allowed to work in key positions of cybersecurity management and network operation for five years; persons who are subject to criminal penalties shall not be allowed to work in key positions of cybersecurity management and network operation for life.

Article 64
Network operators and network product or service providers violating the provisions of Article 22 Paragraph 3 and Articles 41 to 43 of this Law in infringing the protection and rights of citizens' personal information, are ordered to make corrections by the relevant competent department and may, according to the circumstances, be given warnings, confiscation of unlawful gains, and/or fined between 1 to 10 times the amount of unlawful gains; where there are no unlawful gains, fined up to 1.000.000 yuan and persons who are directly in charge and other directly responsible personnel are fined between 10.000 yuan and 100.000 yuan; where the circumstances are serious the relevant competent department may order a temporary suspension of operations, a suspension of business for corrections, closing down of websites, revocation of relevant operations permits, or cancellation of business licenses.

Where Article 44 of this Law is violated in stealing or using other illegal means to obtain, illegally sell of illegally provide others with citizens' personal information, and this does not constitute a crime, the public security organs confiscate unlawful gains and impose a fine of between 1 and 10

Cybersecurity Law of the People's Republic of China (2016)

times the amount of unlawful gains, and where there are no unlawful gains, impose a fine of up to 1.000.000 yuan.

Article 65
Where critical information infrastructure operators violate Article 35 of this Law by using network products or services that have not had safety inspections or did not pass safety inspections, the relevant competent departments order the usage to stop, and impose a fine in the amount of 1 to 10 times the purchase price; the persons who are directly in charge and other directly responsible personnel are fined between 10.000 yuan and 100.000 yuan.

Article 66
Where critical information infrastructure operators violate the provisions of Article 37 of this Law by storing network data outside the mainland territory, or provide network data outside of the mainland territory, the relevant competent department orders corrections, gives warnings, confiscates unlawful gains, imposes fines between 50.000 yuan and 500.000 yuan, and may order a temporary suspension of operations, a suspension of business for corrections, closing down of websites, revocation of relevant operations permits, or cancellation of business licenses; persons who are directly in charge and other directly responsible personnel are fined between 10.000 yuan and 100.000 yuan.

Article 67
Those establishing websites or communications groups for use in committing illegal or criminal activities in violation of the provisions of Article 46 of this Law or use the Internet to publish information related to the commission of illegal or criminal, but a crime has not been committed, will be detained by public security organs for five days or less, and a fine of 10.000 yuan or more but less than 100.000 yuan may additionally be imposed; where circumstances are serious, a detention of five days or more but less than fifteen days is imposed, and a fine of 50.000 yuan or more but less than 500.000 yuan may additionally be imposed. The websites and communications groups used for illegal or criminal activities are also closed.

Where units have engaged in conduct covered by the preceding paragraph, public security organs impose a fine of 100.000 yuan or more but less than 500.000 yuan and their directly responsible person in charge and other directly responsible personnel will be punished in accordance to the provisions of the previous paragraph.

Article 68
Where network operators violate the provisions of Article 47 of this Law by failing to stop the transmission of information that laws or administrative regulations prohibit the publication or transmission of, failing to take disposition measures such as deletion or failing to save relevant records, the relevant competent department orders corrections, gives warnings, and confiscates unlawful gains; where corrections are refused or circumstances are serious, fines between 100.000 and 500.000 yuan are imposed, and a temporary suspension of operations, a suspension of business for corrections, closing down of websites, revocation of relevant operations permits, or

Cybersecurity Law of the People's Republic of China (2016)

cancellation of business licenses may be ordered; persons who are directly in charge and other directly responsible personnel are fined between 10.000 and 100.000 yuan.

Where electronic information services providers and application software download service providers, have not performed their security management duties in accordance to Article 48 Paragraph 2 of this Law, they will be punished according to the provisions of the previous paragraph.

Article 69
Network operators in who violate the provisions of this law by committing one of the following acts shall be ordered by the relevant competent department to make corrections; if they refuse to make corrections or the circumstances are serious, they shall be fined not less than 50.000 yuan and not more than 500.000 yuan; responsible personnel who are directly liable and other directly liable personnel shall be fined not less than 10.000 yuan and not more than 100.000 yuan:
(1) Failure to take disposal measures such as stopping transmission or eliminating information whose publication or transmission is prohibited by laws or administrative regulations in accordance with the requirements of the relevant departments;
(2) Refusal or obstruction of the relevant departments in their lawful supervision and inspection;
(3) Refusal to provide necessary technical support and assistance to public security organs and national security organs.

Article 70
Those publishing or transmitting information of which the publication or transmission is prohibited by the provisions of Article 12 Paragraph 2 of this Law, or other laws and administrative regulations, are punished in accordance with the provisions of relevant laws and administrative regulations.

Article 71
Acts committed in violation of the provisions of this Law, will be entered into credit files and published, in accordance with the provisions of relevant laws and regulations.

Article 72
Where an operator of a government service network of a state organization does not perform cybersecurity protection duties as prescribed by this Law, the organization at the level above or relevant departments will order corrections; sanctions are given to the managers directly responsible and other directly responsible personnel.

Article 73
Where cybersecurity and information departments and relevant departments violate the provisions of Article 30 of this Law, and use information acquired while performing cybersecurity protection duties for other purposes, the directly responsible person in charge and other directly responsible personnel will be punished according to the law.

Cybersecurity Law of the People's Republic of China (2016)

Where work personnel of cybersecurity and information departments and relevant departments neglect their duties, abuse their power, or distort the law for personal gain, and it does not constitute a crime, sanctions are imposed in accordance with the law.

Article 74
Where violations of the provisions of this Law cause harm to others, civil liability is borne in accordance with the law.

Where violations of the provisions of this Law constitute an act violating public order management, public order management punishment will be imposed according to the law; where it constitutes a crime, criminal liability will be prosecuted according to the law.

Article 75
Where foreign institutions, organizations or individuals engage in attacks, intrusions, interference, destruction and other such acts harming the critical information infrastructure of the People's Republic of China, resulting in serious consequences, legal liability will be prosecuted according to the law. The public security departments of the State Council and relevant departments may also decide to freeze the assets of said institutions, organizations or individuals, or take other necessary punitive measures.

Cybersecurity Law of the People's Republic of China (2016)

Chapter VII. Supplementary Provisions

Article 76

For this Law, the terms below have the following meanings:

(1) "Networks" refers to a system comprised of computers or other information terminals and related equipment that follow certain rules and procedures for information gathering, storage, transmission, exchange and processing.

(2) "Cybersecurity" refers to taking necessary measures to prevent attacks, intrusions, disturbance, sabotage and unlawful use of networks, as well as unexpected accidents, causing the networks to be in a state of stable and reliable operation, as well as safeguarding the integrity, secrecy and usability of network information.

(3) "Network operators" refers to the owners and administrators of networks, as well as network service providers.

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

(5) "Personal data" refers to all kinds of information, stored in electronic or other form, which individually or in combination with other information allows the identification of a natural person's individual identity, including but not limited to their name, date of birth, identity card number, personal biometric information, address, telephone number, etc.

Article 77

The operational security protection of networks storing and processing information involving state secrets shall, in addition to complying with this Law, also comply with the provisions of laws and administrative regulations on confidentiality.

Article 78

Military network and information security protection will be regulated separately by the Central Military Commission.

Article 79

This Law shall come into force on June 1, 2017.