Cryptography Law of the P.R.C.

2019/10/27 China Law Translate NPC 0

Promulgation Date: 2019-10-26
Title: Cryptography Law of the P.R.C.
Document Number:
Expiration date:
Promulgating Entities: Standing Committee of the National People's Congress
Source of text:
http://www.npc.gov.cn/npc/c30834/201910/6f7be7dd5ae5459a8de8baf36296bc74.shtml

Table of Contents

Cryptography Law of the P.R.C.

Chapter I: General Provisions

Article 1: This law is formulated so as to regulate the use and management of cryptography, to promote the development of the cryptography field, to ensure network and information security, to preserve national security and the societal public interest, and to protect the lawful rights and interests of citizens, legal persons and other organizations.

Article 2: "Cryptography" as used in this Law refers to technologies, products, and services that employ specified transformation methods to encrypt information or carry out security authentication.

Article 3: Cryptography work adheres to an overall national security perspective, and follows the principles of unified leadership, hierarchical responsibility, innovation and development, serving the overall situation, management in accordance with law, and ensuring security.

Article 4: Persist in the leadership of the Communist Party of China over cryptography work. The cryptography leadership body of the Party Central Committee carries out uniform leadership the entire nation's cryptography work, drafts national major directives and policies on cryptography work, and does overall coordination of major matters and important work in the nation's cryptography, advancing the establishment of rule of law for national cryptography.

Article 5: The State Cryptography Administration is responsible for management of the entire nation's cryptography work. Local departments at the county level or above for the management of cryptography are responsible for management of that administrative region's cryptography work.

State organs and units involved with cryptography work are responsible, within the scope of their duties, for that organ, unit, or system's cryptography work.

Article 6: The state implements categorized management of cryptography.

Cryptography is classified as core cryptography, common cryptography, and commercial cryptography.

Article 7: Core cryptography and common cryptography are used in protecting state secret information; the highest classification level that core cryptography can be used to protect is Top Secret, and the highest classification level that common cryptography can be used to protect is Secret.

Core cryptography, and common cryptography are state secrets.Departments for cryptography management follow this law and relevant laws, administrative regulations, and state provisions, to carry out uniform management of core cryptography and common cryptography.

Article 8: Commercial cryptography is used to protect information that is not a state secret.

Citizens, legal persons, and other organizations may lawfully use commercial cryptography to protect network and information security.

Article 9: The state encourages and supports research and applications of cryptographic science and technology, protecting the intellectual property rights of the cryptography field in accordance with law and promoting progress and innovation in cryptographic science and technology.

The state is to strengthen cultivation of talent and team building in cryptography, and give commendations and awards, in accordance with relevant national regulations, to organizations and individuals making outstanding contributions in cryptography work.

Article 10: The state is to employ various methods to strengthen education on cryptographic security, including cryptographic security education in the citizen education system and civil servants education and training system, strengthening citizens, legal persons, and other organizations' awareness of cryptographic security.

Article 11: People's governments at the county level or above shall include cryptography work within the economic and social development plan for that level, and place necessary expenses within the financial budget for that level.

Article 12: The encryption protected information of others must not be stolen by any organization or individual, and cryptographic safeguard systems must not be illegaly trespassed upon.

Cryptography must not be used by any organization or individual to engage in illegal or criminal activities that endanger national security, the societal public interest, or the lawful rights and interests of others, and so forth.

Chapter II: Core Cryptography, Common Cryptography

Article 13: The state is to strengthen the planning, management and use of core and common cryptography science, strengthening the institutional establishment, improving management measures, and strengthening the capacity of cryptographic security safeguards.

Article 14: State secret information sent on cable or wireless telecommunications, as well as information systems storing or processing state secret information, shall use core and common cryptography to carry out encryption protect and security verification in accordance with laws, administrative regulations, and relevant state provisions.

Article 15: Entities engaged in work such as the research, production, service, testing, furnishing, use, or destruction of core and common cryptography (hereinafter jointly 'cryptography work bodies') shall follow the requirements of laws, administrative regulations, relevant state provisions, and standards for core and common cryptography to establish and complete security management systems, employing strict confidentiality measures and confidentiality responsibility systems, to ensure the security of core and common cryptography.

Article 16: Departments for cryptography management are to lawfully conduct guidance, oversight, and inspections of the cryptography work bodies' efforts on core and common cryptography, and the cryptography work bodies shall cooperate.

Article 17: As needed for work, departments for management of cryptography, together with relevant departments, are to establish coordination mechanisms such as for security monitoring and alerts, security risk assessment, information circulation, consulting on major matters, and emergency response; to ensure that security management work for core and common cryptography is coordinated and connected, orderly and efficient.

Where cryptography work bodies discover that core or common leaks in core or common cryptography, or major issues and potential risks impacting core and common cryptography security, they shall immediately employ responsive measures, and promptly report to the departments for the administration and

management of secrets, and the departments for the management of cryptography, and those departments are to organize and carry out an investigation and disposition together with relevant departments, and guide related cryptography work bodies in promptly eliminating the potential security risks.

Article 18: The state is to strengthen the establishment of the cryptography work bodies, ensuring their performance of their work duties.

The state is to establish management systems suited to the needs of core and common cryptography work, such as for hiring, transferring, secrecy, evaluating, training, benefits, awards, punishments, communication, and departure of personnel.

Article 19: As need for work, cryptography management departments may follow relevant state provisions to request that public security, transport, customs, and other such departments provide facilitation by waiving inspections of items and personnel related to core and common cryptography, and relevant departments shall provide coordination.

Article 20: The cryptography work bodies shall establish and complete systems for strict supervision and security review, conduct oversight of their staff's compliance with laws and discipline, and lawfully employ necessary measures, organizing periodic or unscheduled security inspections.

Chapter III: Commercial Cryptography

Article 21: The state encourages research and development, academic exchange, achievement transformation, and spreading the use of commercial cryptography, to complete a unified, open, competitive, and orderly market system for commercial cryptography, encouraging the development of the commercial cryptography industry.

All levels of people's government and their relevant departments shall follow the principle of non-discrimination to lawfully give equal treatment to units, including foreign investment enterprises, such as those researching, producing, selling, servicing, or importing or exporting, commercial cryptography (hereinafter jointly referred to as “commercial cryptography work units"). The state encourages technological cooperation on commercial cryptography to be conducted in the course of foreign investment and on the basis of the voluntariness principle and business rules. Administrative organs and their employees must not force the transfer of commercial cryptography technology through administrative measures.

Research, production, sale, service, import, and export of commercial cryptography must not endanger national security, the societal public interest, or the lawful rights and interests of others.

Article 22: The state is to establish and improve a system of standards for commercial cryptography.

On the basis of their individual responsibilities, the State Council administrative department for standardization and the State Cryptography Administration are to organize the drafting relevant national and industry standards for commercial cryptography.

The state supports social groups and enterprises use of their own innovative technologies and drafting group or enterprise cryptography standards that exceed the state and industry standards' requirements.

Article 23: The state promotes participation in activities for the international standardization of commercial cryptography, participation in drafting international standards on commercial cryptography, and advancing conversion for use between Chinese and foreign standards on commercial cryptography.

The state encourages enterprises and social groups, and educational and research bodies, etc., to participate in activities for the international standardization of commercial cryptography.

Article 24: Commercial cryptography work units launching commercial cryptography activities shall comply with the technical requirements of relevant laws, administrative regulations, compulsory state standards on commercial cryptography, as well as the unit's public standards.

The state encourages commercial cryptography work units to employ recommended state and industry standards on commercial cryptography, increasing the defensive capacity of commercial cryptography and preserving users' lawful rights and interests.

Article 25: The state is to advance the establishment of systems for testing and certification of commercial cryptography, drafting technical regulations and rules for testing and certification of commercial cryptography, and encouraging commercial cryptography work units to accept testing and certification to increase their market competitiveness.

Commercial cryptography testing and certification bodies shall obtain credentials in accordance with law and carry out commercial cryptography testing and certification in accordance with law laws, administrative regulations, and technical regulations for commercial cryptography testing and certification.

Commercial cryptography testing and certification bodies shall bear an obligation to maintain the secrecy of state secrets and commercial secrets that they learn of in the course of commercial cryptography testing and certifications.

Article 26: Commercial cryptography products that involve national security, the national welfare and the people's livelihood, or the societal public interest, shall be lawfully entered into the catalogs of critical network equipment and specialized cybersecurity products, and must pass testing and certification by qualified bodies before being sold or provided. Testing and certification of commercial cryptography products is to apply the relevant provisions of the "People's Republic of China Cybersecurity Law", to avoid repetitive testing.

Where commercial cryptography services use critical network equipment and specialized cybersecurity products, it shall be after that commercial cryptography service is certified as up to standards by a commercial cryptography certification body.

Article 27: Where laws, administrative regulations, and relevant state provisions require that critical information infrastructures use commercial cryptography protections, their operators shall use commercial cryptography protections and carry out commercial cryptography application security assessments either on their own or by retaining a commercial cryptography testing body. Security assessments of commercial cryptography applications shall be connected to critical information infrastructure security testing assessments and network security classification level assessments to avoid repetitive assessments and evaluations.

Where operators of critical information infrastructure purchase network products or services that involve commercial cryptography, and might impact national security, they shall follow the provisions of the "People's Republic of China Cybersecurity Law" to pass national security review organized by the State Internet Information Department, together with the State Cryptography Administration, and other relevant departments.

Article 28: The State Council department for commercial affairs and the State Cryptography Administration are to lawfully carry out import permitting for commercial cryptography that involves national security or the societal public interest that have cryptographic protection functions, and carry out export controls on commercial cryptography that involves national security, the societal public interest, or international

obligations that China has undertaken. The lists of import permits and export controls for commercial cryptography are to be drafted and published by the State Council department for commercial affairs together with the State Cryptography Administration and General Customs Administration.

Import permitting and export control systems are not implemented for commercial cryptography for mass consumption.

Article 29: The State Cryptography Administration is to conduct certification of entities using commercial cryptography technology to engage in e-governance e-certification services, and collaborate with relevant departments responsible for managing the use of electronic signatures and data messaging in government activities.

Article 30: Industry associations for the commercial cryptography field and other organizations are to follow laws, administrative regulations, and their charters to provide services such as information, technology, and training to commercial cryptography work units, guiding and urging them to lawfully carry out commercial cryptography activities, strengthen industry self-discipline, promote the establishment of industry creditworthiness, and promote the healthy development of the industry.

Article 31: Cryptography management departments and relevant departments are to establish systems for regulation of commercial cryptography, during and after the fact, that combine routine oversight and random sampling inspections, establish a unified platform for commercial cryptography oversight and management information, advance the establishment of connections between regulation during and after the fact and the social credit system, and strengthen commercial cryptography work units' self-discipline and public oversight.

Cryptography management departments and relevant departments, as well as their staffs, must not require commercial cryptography work units and commercial cryptography testing and certification bodies to disclose source code and other proprietary information related to cryptography; and are to strictly preserve the secrecy of commercial secrets and personal private information learned of in the performance of their duties, and must not leak or illegally provide it to other people.

Chapter IV: Legal Responsibility

Article 32: Where article 13 of this Law is violated by stealing other's encryption protected information, illegally trespassing on others' cryptography protected systems, or using cryptography to engage in illegal activities such as endangering national security, the societal public interest, or the lawful rights and interests of others; the relevant departments are to follow the "People's Republic of China Cybersecurity Law" and other relevant laws and administrative regulations to pursue legal responsibility.

Article 33: Where article 14 of this law is violated by failure to follow the requirements for using core and common cryptography, the departments for cryptography management are to order corrections or that the illegal conduct be stopped, and give a warning; where the circumstances are serious, the departments for cryptography management are to recommend that the relevant state organs and units lawfully give sanctions or punishments to the directly responsible managers and other directly responsible personnel.

Article 34: Where article 14 of this law is violated in cases of leaks of core or common cryptography, the departments for secrecy administration and for cryptography management are to recommend that the relevant state organs and units lawfully give sanctions or punishments to the directly responsible managers and other directly responsible personnel

Where paragraph 2 of article 17 of this law is violated by failure to immediately take responsive measures to or promptly report the discovery of leaks of core or common cryptography, or other major issues or latent threats impacting core or common cryptography security, the departments for secrecy administration and for cryptography management are to recommend that the relevant state organs and units lawfully give sanctions or punishments to the directly responsible managers and other directly responsible personnel

Article 35: Where commercial cryptography testing and certification bodies violate the second or third paragraph of article 25 of this Law in carrying out commercial cryptography testing and certification, the market regulatory departments are to order corrections or that the illegal conduct be stopped, give warnings, and confiscate unlawful gains; where the unlawful gains are of 300,000 RMB or more, a fine of between 1-3 times the amount of unlawful gains may be given; where there are no unlawful gains or the unlawful gains are less than 300,000 RMB a fine of between 100,000 RMB and 300,000 RMB may be given; and where circumstances are serious lawfully revoke related qualifications.

Article 36: Where article 26 of this Law is violated by selling or providing commercial cryptography products that have not been tested and certified or did not pass testing and certification, or by providing commercial cryptography services that have not been tested and certified or did not pass testing and certification, the market regulatory departments, together with the departments for cryptography management, are to order corrections or that the illegal conduct be stopped, give warnings, and confiscate unlawful gains from the illegal products or services; where the unlawful gains are of 100,000 RMB or more, a fine of between 1-3 times the amount of unlawful gains may be given; where there are no unlawful gains or the unlawful gains are less than 100,000 RMB a fine of between 30,000 RMB and 100,000 RMB may be given.

Article 37: Where critical information infrastructure operators violate the first paragraph of article 27 of this law by failing to use commercial cryptography as required or failing to carry out security assessments of commercial cryptography applications, the departments for management of cryptography are to order corrections and give warnings; where corrections are refused or it leads to serious consequences such as endangering cybersecurity, a fine of between 100,000 and 1,000,000 RMB is to be given; the persons who are directly in charge are to be fined between RMB 10,000 and 100,000 RMB.

Where critical information infrastructure operators violate paragraph 2 of article 27 of this law by using 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 give 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 RMB 10,000 and 100,000.

Article 38: Where article 28 of this Law is violated in carrying out import permits or export controls for the import-export of commercial cryptography, the State Council departments for commerce or customs are to give punishments in accordance with law.

Article 39: Where article 29 of this Law is violated by engagement in e-governance electronic authentication services without certification, the departments for cryptography management, are to order corrections or that the illegal conduct be stopped, give warnings, and confiscate unlawful gains from the illegal products or services; where the unlawful gains are of 300,000 RMB or more, a fine of between 1-3 times the amount of unlawful gains may be given; where there are no unlawful gains or the unlawful gains are less than 300,000 RMB a fine of between 100,000 RMB and 300,000 RMB may be given.

Article 40: Where the employees of departments for cryptography management, and relevant departments or units, abuse their authority, neglect their duties, or misuse their power for personal benefit, or where they disclose or unlawfully provide others with the trade secrets and personal private information they learn of in the course of performing their duties, they are to be given sanctions in accordance with law.

Article 41: Where violations of the provisions of this law constitute a crime, criminal liability is to be pursued in accordance with law; and where losses are caused to others, civil liability is to be borne in accordance with law.

Chapter V: Supplementary Provisions

Article 42: The State Cryptography Administration is to follow laws and administrative regulations to draft rules for managing cryptography.

Article 43: The Central Military Commission is to formulate management measures for cryptography work by the Chinese People's Liberation Army and the Chinese people's armed police forces.

Article 44: This Law takes effect on January 1, 2020.