

lawinfochina.com > Laws & Regulations > Text	
<div>BookmarkDownloadPrint</div> <div>Search: <input type="text"/></div> <div><input type="checkbox"/> "Fabao" Window</div> <div>Font Size: <small>XS</small> <small>A</small> <small>A</small> <small>XL</small></div> <div> </div> <div>简体繁体</div>	
<div><div>Cybersecurity Law of the People's Republic of China [Effective]</div><div>中华人民共和国网络安全法 [现行有效]</div><div>(法宣引证码)CLL1.1.283838(EN)</div><div><div>Issuing authority : Standing Committee of the National People's Congress</div><div>Document Number : Order No. 53 of the President</div><div>Date issued : 11-07-2016</div><div>Effective date: 06-01-2017</div><div>Level of Authority: Laws</div><div>Area of Law:Public Security,Post and Telecommunications</div></div></div>	
<div>Order of the President of the People's Republic of China</div> <div>中华人民共和国主席令</div>	
<div>(No. 53)</div> <div>(第五十三号)</div>	
<div>The Cybersecurity Law of the People's Republic of China, as adopted at the 24th Session of the Standing Committee of the Twelfth National People's Congress of the People's Republic of China on November 7, 2016, is hereby issued and shall come into force on June 1, 2017.</div> <div>《中华人民共和国网络安全法》已由中华人民共和国第十二届全国人民代表大会常务委员会第二十次会议于2016年11月7日通过，现予公布，自2017年6月1日起施行。</div>	
<div>President of the People's Republic of China: Xi Jinping</div> <div>中华人民共和国主席 习近平</div>	
<div>November 7, 2016</div> <div>2016年11月7日</div>	
<div>Cybersecurity Law of the People's Republic of China</div> <div>中华人民共和国网络安全法</div>	
<div>(Adopted at the 24th Session of the Standing Committee of the Twelfth National People's Congress of the People's Republic of China on November 7, 2016)</div> <div>(2016年11月7日第十二届全国人民代表大会常务委员会第二十次会议通过)</div>	
<div>Table of Contents</div> <div>目录</div>	
<div>Chapter I General Provisions</div> <div>第一章 总 则</div>	
<div>Chapter II Cybersecurity Support and Promotion</div> <div>第二章 网络安全支持与促进</div>	
<div>Chapter III Network Operation Security</div> <div>第三章 网络运行安全</div>	
<div>Section 1 General Provisions</div> <div>第一节 一般规定</div>	
<div>Section 2 Operation Security of Critical Information Infrastructure</div> <div>第二节 关键信息基础设施的运行安全</div>	
<div>Chapter IV Network Information Security</div> <div>第四章 网络信息安全</div>	
<div>Chapter V Monitoring, Early Warning and Emergency Response</div> <div>第五章 监测预警与应急处置</div>	
<div>Chapter VI Legal Liability</div> <div>第六章 法律责任</div>	
<div>Chapter VII Supplementary Provisions</div> <div>第七章 附 则</div>	
<div>Chapter I General Provisions</div> <div>第一章 总 则</div>	
<div>Article 1 This Law is developed for the purposes of guaranteeing cybersecurity, safeguarding cyberspace sovereignty, national security and public interest, protecting the lawful rights and interests of citizens, legal persons and other organizations, and promoting the sound development of economic and social informatization.</div> <div>第一条 为了保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展，制定本法。</div>	
<div>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 within the territory of the People's Republic of China.</div> <div>第二条 在中华人民共和国境内建设、运营、维护和使用的网络，以及网络安全的监督管理，适用本法。</div>	
<div>Article 3 The state shall lay equal stress 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 cultivation of cybersecurity talents, establish and improve the cybersecurity guarantee system, and enhance the capability to protect cybersecurity.</div> <div>第三条 国家坚持网络安全与信息化发展并重，遵循积极利用、科学发展、依法管理、确保安全的方针，推进网络基础设施建设 and 互联互通，鼓励网络技术创新和应用，支持培养网络安全人才，建立健全网络安全保障体系，提高网络安全保障能力。</div>	
<div>Article 4 The state shall develop 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 fields.</div> <div>第四条 国家制定并不断完善网络安全战略，明确保障网络安全的基本要求和主要目标，提出重点领域的网络安全政策、工作任务和措施。</div>	
<div>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 attack, intrusion, interference and damage, punish illegal criminal activities on the network in accordance with the law, and maintain cyberspace safety and order.</div> <div>第五条 国家采取综合、监测、防御、处置来源于中华人民共和国境内外网络的网络安全风险和威胁，保护关键信息基础设施免受攻击、侵入、干扰和破坏，依法惩治网络违法犯罪活动，维护网络空间安全和秩序。</div>	
<div>Article 6 The state shall advocate honest, faithful, healthy and civilized network conduct, 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.</div> <div>第六条 国家倡导诚实守信、健康文明的网络行为，推动传播社会主义核心价值观，采取措施提高全社会的网络安全意识和水平，形成全社会共同参与促进网络安全的良好环境。</div>	
<div>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 crackdown on 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 cyber governance.</div> <div>第七条 国家积极开展网络空间治理、网络技术研发和标准制定、打击网络违法犯罪等方面的国际交流与合作，推动构建和平、安全、开放、合作的网络空间，建立多边、民主、透明的网络治理体系。</div>	
<div>Article 8 The national cyberspace administration shall be responsible for the overall planning and coordination of cybersecurity work and relevant supervision and administration. The competent 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.</div> <div>第八条 国家网信部门负责统筹协调网络安全工作和相关监督管理工作。国务院电信主管部门、公安部门和其他有关机关依照本法和有关法律、行政法规的规定，在各自职责范围内负责网络安全保护和监督管理工作。</div>	
<div>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.</div> <div>县级以上地方人民政府有关部门的网络安全保护和监督管理职责，按照国家有关规定确定。</div>	
<div>Article 9 Network operators shall, when conducting business operations and providing services, abide by laws and administrative regulations, respect social morality, observe business ethics, have good faith, perform the cybersecurity protection obligation, accept supervision by the government and the public, and undertake social responsibilities.</div> <div>第九条 网络运营者开展经营和服务活动，必须遵守法律、行政法规，尊重社会公德，遵守商业道德，诚实信用，履行网络安全保护义务，接受政府和社会的监督，承担社会责任。</div>	
<div>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 compulsory requirements of national standards to ensure the safe and stable operation of the network, effectively respond to cybersecurity incidents, prevent illegal criminal activities committed on the network, and maintain the integrity, confidentiality and availability of network data.</div> <div>第十条 建设、运营网络或者通过网络提供服务，应当依照法律、行政法规的规定和国家标准的强制性要求，采取技术措施和其他必要措施，保障网络安全、稳定运行，有效应对网络安全事件，防范网络违法犯罪活动，维护网络数据的完整性、保密性和可用性。</div>	
<div>Article 11 Network-related industry organizations shall, in accordance with their charters, intensify industry self-discipline, 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.</div> <div>第十一条 网络相关行业组织按照章程，加强行业自律，制定网络安全行为规范，指导会员加强网络安全保护，提高网络安全保护水平，促进行业健康发展。</div>	
<div>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, provide better 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.</div> <div>第十二条 国家保护公民、法人和其他组织依法使用网络的权利，促进网络接入普及，提升网络服务水平，为社会提供安全、便利的网络服务，保障网络信息依法有序自由流动。</div>	
<div>Any individual or organization using the network shall comply with the Constitution and laws, follow public order and respect social morality, shall not endanger cybersecurity, and shall not use the network to conduct any activity that endangers national security, honor 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 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.</div> <div>任何个人和组织使用网络应当遵守宪法法律，遵守公共秩序，尊重社会公德，不得危害网络安全，不得利用网络从事危害国家安全、荣誉和利益、煽动颠覆国家政权、推翻社会主义制度、煽动分裂国家、破坏国家统一、宣扬恐怖主义、极端主义、宣扬民族仇恨、民族歧视、传播暴力、宣扬色情信息、编造、传播虚假信息扰乱经济秩序和社会秩序，以及侵害他人名誉、隐私、知识产权和其他合法权益等活动。</div>	
<div>Article 13 The state shall support the research and development of network 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 network, and provide a safe and healthy network environment for minors.</div> <div>第十三条 国家支持研发开发有利于未成年人健康成长的网络产品和服务，依法惩治利用网络从事侵害未成年人身心健康的活动，为未成年人提供安全、健康的网络环境。</div>	
<div>Article 14 Any individual or organization shall have the right to report the conduct that endangers 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.</div> <div>第十四条 任何个人和组织有权对危害网络安全的行为向网信、电信、公安等部门举报。收到举报的部门应当及时依法作出处理；不属于本部门职责的，应当及时移送有权处理的部门。</div>	
<div>The relevant department shall keep confidential the information on the informant, and protect the informant's lawful rights and interests.</div> <div>有关部门应当对举报人的相关信息予以保密，保护举报人的合法权益。</div>	
<div>Chapter II Cybersecurity Support and Promotion</div> <div>第二章 网络安全支持与促进</div>	
<div>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, according to their respective functions, organize the formulation of and revise at appropriate time national and industry standards relating to cybersecurity administration and the security of network products, services and operations.</div> <div>第十五条 国家建立和完善网络安全标准体系。国务院标准化行政主管部门和其他有关部门根据各自的职责，组织制定并适时修订有关网络安全管理以及网络产品、服务和运行安全的国家标准、行业标准。</div>	
<div>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.</div> <div>国家支持企业、科研机构、高等学校、网络相关行业组织参与网络安全国家标准、行业标准的制定。</div>	
<div>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 input, 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.</div> <div>第十六条 国务院和省、自治区、直辖市人民政府应当统筹规划，加大投入，扶持重点网络安全技术产业和项目，支持网络安全技术的研究开发和应用，推广安全可信的网络产品和服务，保护网络知识产权，支持企业、科研机构 and 高等学校参与国家网络安全技术创新项目。</div>	
<div>Article 17 The state shall boost the construction of a socialized service system for cybersecurity, and encourage relevant enterprises and institutions to provide such security services as cybersecurity authentication, detection and risk assessment.</div> <div>第十七条 国家推进网络安全社会化服务体系建设，鼓励有关企业、机构开展网络安全认证、检测 and 风险评估等安全服务。</div>	
<div>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.</div> <div>第十八条 国家鼓励开发网络数据安全保护和利用技术，促进公共数据资源开放，推动技术创新和经济社会发展。</div>	
<div>The state shall support the innovation of cybersecurity management methods and the application of new network technologies to enhance cybersecurity protection.</div> <div>国家支持创新网络安全管理方式，运用网络新技术，提升网络安全保护水平。</div>	
<div>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.</div> <div>第十九条 各级人民政府及其有关部门应当组织开展经常性的网络安全宣传教育，并指导、督促有关单位做好网络安全宣传教育工作。</div>	
<div>Mass media shall offer pertinent cybersecurity publicity and education to the public.</div> <div>大众传媒媒介应当有针对性地向社会进行网络安全宣传教育。</div>	
<div>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 measures to cultivate cybersecurity talents, and promote the exchange of cybersecurity talents.</div> <div>第二十条 国家支持企业 and 高等学校、职业学校等教育培训机构开展网络安全相关教育与培训，采取多种方式培养网络安全人才，促进网络安全人才交流。</div>	
<div>Chapter III Network Operation Security</div> <div>第三章 网络运行安全</div>	
<div>Section 1 General Provisions</div> <div>第一节 一般规定</div>	
<div>Article 21 The state shall implement the rules for graded protection of cybersecurity. Network operators shall, according to the requirements of the rules for graded protection of cybersecurity, fulfill the following security protection obligations, so as to ensure that the network is free from interference, damage or unauthorized access, and prevent network data from being divulged, stolen or falsified.</div> <div>第二十一条 国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权访问，防止网络数据泄露或者被窃取、篡改：</div>	
<div>(1) Developing internal security management rules and operating procedures, determining the persons in charge of cybersecurity, and carrying out the responsibility for cybersecurity protection.</div> <div>(一) 制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任；</div>	
<div>(2) Taking technical measures to prevent computer viruses, network attack, network intrusion and other acts endangering cybersecurity.</div> <div>(二) 采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施；</div>	
<div>(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.</div> <div>(三) 采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月；</div>	
<div>(4) Taking measures such as data categorization, and back-up and encryption of important data.</div> <div>(四) 采取数据分类、重要数据备份和加密等措施；</div>	
<div>(5) Performing other obligations as prescribed by laws and administrative regulations.</div> <div>(五) 法律、行政法规规定的其它义务。</div>	
<div>Article 22 Network products and services shall comply with the compulsory 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.</div> <div>第二十二条 网络产品、服务应当符合相关国家标准的要求。网络产品、服务的提供者不得设置恶意程序；发现其网络产品、服务存在安全缺陷、漏洞等风险时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。</div>	
<div>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 stipulated period or the period agreed upon by the parties.</div> <div>网络产品、服务的提供者应当为其产品、服务持续提供安全维护；在规定的或者当事人约定的期限内，不得终止安全维护。</div>	
<div>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.</div> <div>网络产品、服务具有收集用户信息功能的，其提供者应当向用户明示并取得同意；涉及用户个人信息的，还应当遵守本法和有关法律、行政法规关于个人信息保护的規定。</div>	
<div>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 detection results to avoid repeated certification and detection.</div> <div>第二十三条 网络关键设备和网络安全专用产品应当按照相关国家标准的强制性要求，由具备资质的机构安全认证合格或者安全检测符合要求后，方可销售或者提供。国家网信部门会同国务院有关部门制定、公布网络关键设备网络安全专用产品目录，并推动安全认证和安全检测结束互认，避免重复认证、检测。</div>	
<div>Article 24 Where network operators provide network access and domain registration services for users, handle network access formalities for fixed-line or mobile phone users, or provide users with information release services, instant messaging services and other services, they shall require users to provide true identity information when signing agreements with users or confirming the provision of services. If any user fails to provide his or her true identity information, the network operator shall not provide him or her with relevant services.</div> <div>第二十四条 网络运营者为用户提供网络接入、域名注册服务，办理固定电话、移动电话等入网手续，或者为用户提供信息发布、即时通讯等服务，在与用户签订协议或者确认提供服务时，应当要求用户提供真实身份信息。用户不提供真实身份信息的，网络运营者不得为其提供相关服务。</div>	
<div>The state shall implement the strategy of credible 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.</div> <div>国家实施网络可信身份战略，支持研究开发安全、方便的电子身份认证技术，推动不同电子身份认证之间的互认。</div>	
<div>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.</div> <div>第二十五条 网络运营者应当制定网络安全事件应急预案，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险；在发生危害网络安全的事件时，立即启动应急预案，采取相应的补救措施，并按照规定向有关主管部门报告。</div>	
<div>Article 26 Such activities as cybersecurity authentication, detection 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.</div> <div>第二十六条 开展网络安全认证、检测、风险评估等活动，向社会发布系统漏洞、计算机病毒、网络攻击、网络侵入等网络安全信息，应当遵守国家有关规定。</div>	
<div>Article 27 No individual or organization may conduct any activity endangering cybersecurity, such as illegally intruding into any other person's network, interfering with the normal functions of any other person's network, and stealing network data, or provide programs or tools specifically used for conducting activities endangering cybersecurity, such as network intrusion, interference with normal functions and protective measures of the network, and stealing of network data. Whoever interferes with any other person conducts any activity endangering cybersecurity shall not provide technical support, advertising promotion, payment and settlement services or any other assistance to such a person.</div> <div>第二十七条 任何个人和组织不得从事非法侵入他人网络、干扰他人网络正常功能、窃取网络数据等危害网络安全活动；不得提供专门用于从事侵入网络、干扰网络正常功能及防护、窃取网络数据等危害网络安全活动的程序、工具；明知他人从事危害网络安全的活动的，不得为其提供技术支持、广告推广、支付结算等帮助。</div>	
<div>Dear visitor, you are attempting to view a subscription-based section of lawinfochina.com. If you are already a subscriber, please login to enjoy access to our databases. If you are not a subscriber, please subscribe. You can purchase a single article through Online Pay to immediately view and download this document. Should you have any questions, please contact us at:</div> <div>+86 (10) 8268-9699 or +86 (10) 8266-8266 (ext. 153)</div> <div>Mobile: +86 133-1157-0712</div> <div>Fax: +86 (10) 8266-8268</div> <div>database@china-lawinfo.com</div>	
<div>法宣引证码:CLL1.1.283838(EN) 北大法宝www.lawinfochina.com</div> <div>Translations are by lawinfochina.com, and we retain exclusive copyright over content found on our website except for content we publish as authorized by respective copyright owners or content that is publicly available from government sources.</div> <div>Due to differences in language, legal systems, and culture, English translations of Chinese law are for reference purposes only. Please use the official Chinese-language versions as the final authority. lawinfochina.com and its staff will not be directly or indirectly liable for use of materials found on this website.</div> <div>We welcome your comments and suggestions, which assist us in continuing to improve the quality of our materials.</div>	
<div>Message: Please kindly comment on the present translation.</div> <div><div></div><div>Confirmation Code: <input type="text"/>  Click image to reset code! <input type="button" value="Submit"/></div></div>	
<div>Home Products and Services FAQ Disclaimer Chinese Site Map</div> <div>©2012 Chinainlawinfo Co., Ltd. database@china-lawinfo.com Tel: +86 (10) 8268-9699 京ICP证010230-8</div>	