君合研究简讯

JUNHE

2015 年 7 月 8 日

电信法律热点问题

网络安全法草案公布征求意见

2015 年 7 月 6 日，全国人大常委会公布了于 2015 年 6 月 25 日经过第一次审议的《网络安全法》草案[1]（以下简称“**《草案》**”），向社会公开征求意见。征求意见截止日期为 2015 年 8 月 5 日。网络安全法于 2013 年被列入第十二届全国人大常委会（任期 2013 年 3 月至 2018 年 3 月）立法规划[2]，并于 2014 年开始列入全国人大常委会年度立法工作计划[3]，但目前网络安全法具体出台时间尚未公布。

《草案》的出台，与今年 7 月 1 日出台的《国家安全法》密切相关。《国家安全法》首次以法律形式提出“维护国家网络空间主权”、将网络和信息安全作为国家安全的重要组成部分，并提出建立对各类影响和可能影响国家安全的事项和活动（包括网络信息技术产品和服务）的国家安全审查和监管制度。《草案》则进一步以“维护国家网络空间主权”作为基本的立法宗旨，从网络安全战略、规划与促进，网络运行安全，网络信息安全，以及监测预警与应急处置等方面对维护网络空间主权和国家安全、保障网络安全作出了具体规定。

一、 适用范围

根据《草案》，《网络安全法》适用于在中华人民共和国境内建设、运营、维护和使用网络，以及网络安全的监督管理。对网络的定义则包括由计算机或者其他信息终端及相关设备组成的按照一定的规则和程序对信息进行收集、存储、传输、交换、处理的网络和系统。对于《网络安全法》之中重要的义务主体网络运营者，《草案》将其定义为“网络的所有者、管理者以及利用他人所有或者管理的网络提供相关服务的网络服务提供者，包括基础电信运营者、网络信息服务提供者、重要信息系统运营者等（第六十五条）。”

二、 网络安全主管机关

《草案》规定，中央层面负责统筹协调网络安全工作和相关监督管理工作的为国家网信部门，即中央网信办，并进一步规定工业和信息化部和公安部（及其他有关部门）在各自职责范围内负责网络安全保护和监督管理工作（第六条）。

三、 与网络运营者相关的主要法律规定

《草案》中与网络运营者相关的主要法律规定总结如下：

- **加强网络运营者的安全义务。**《草案》对网络产品和服务提供者规定了一系列安全义务，包括不得设置恶意程序，及时向用户告知安

[1] 全文请见 http://www.npc.gov.cn/npc/xinwen/lfgz/flca/2015-07/06/content_1940614.htm。

[2] 第 12 届全国人大常委会立法规划 http://news.xinhuanet.com/politics/2013-10/30/c_117939129.htm.

[3] 全国人大常委会 2014 年度立法计划 http://www.npc.gov.cn/npc/xinwen/lfgz/2014-04/17/content_1859742.htm，全国人大常委会 2015 年度立法计划 http://www.npc.gov.cn/npc/xinwen/lfgz/lfdt/2015-05/25/content_1936926.htm。

全缺陷、漏洞等风险，持续提供安全维护服务等（第十八条）。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、行业标准的强制性要求，由具备资格的机构安全认证合格或者安全检测符合要求后方可销售（第十九条）。《草案》将实施网络安全等级保护制度上升为网络运营者的法律义务，要求网络运营者采取数据分类、重要数据备份和加密等保护措施（第十七条）。另外，网络运营者也有配合国家安全和侦查犯罪的需要向侦查机关提供必要的支持与协助的义务（第二十三条）。

- **关键信息基础设施的安全保障。**《草案》对关键信息基础设施提出了更高的保护要求，具体包括（a）设立内部机构、从业人员训练、数据备份、制定应急预案等要求（第二十八条）；（b）关键信息基础设施的运营者应在中华人民共和国境内存储公民个人信息等重要数据（第三十一条）；（c）对关键信息基础设施的运营者采购网络产品或服务进行安全审查（第三十条）；（d）建立网络安全风险年度评估机制（第三十一条）。

  “关键信息基础设施”是指公共通信、广播电视传输等服务的基础信息网络；能源、交通、水利、金融等重要行业和供电、供水、供气、医疗卫生、社会保障等公共服务领域的重要信息系统；军事网络；设区的市级以上国家机关等政务网络；及用户数量众多的网络服务提供者所有或者管理的网络和系统（第二十五条）。然而《草案》并未对该定义的适用进行更具体的解释，例如何种情况可以被认定为 “用户数量众多的网络服务提供者”以及包括何种类型的网络服务。

- **加强网络信息安全保护。**《草案》包含了对网络运营者保护用户个人信息的要求，这些规定在基本重复了现有法律法规规定的基础上，增加了一些要求，例如在发生或者可能发生信息泄露、毁损、丢失的情况时告知可能受影响的用户的要求（第三十四条至三十八条）。《草案》还要求网络运营者记录用户的真实身份，加强对用户发布信息的管理，停止和阻止非法和有害信息的传输，保存有关记录并向政府主管部门报告（第二十条、第四十条和第四十一条）。

- **建立网络安全监测预警和应急响应机制。**《草案》要求国务院相关部门建立网络安全监测预警和信息通报制度、网络安全应急工作机制，制定网络安全事件预案，并规定因维护国家安全和社会公共秩序，处置重大突发社会安全事件的需要，国务院或者省、自治区、直辖市人民政府经国务院批准，可以在部分地区对网络通信采取限制等临时措施（第四十四条至第五十条）。

四、 法律责任

《草案》对于违反法律规定的网络运营者设置了一系列罚则，视具体情况和情节轻重包括罚款、暂停相关业务、停业整顿、关闭网站、撤销相关业务许可或者吊销营业执照等不同形式的罚则（第五十一条至第六十四条）。

五、 简 评

《网络安全法》是我国第一部专门针对网络安全问题的法律，是在互联网时代对网络入侵和攻击、信息泄露、维护网络国家主权和安全等问题的直接回应。一旦正式发布实施，《网络安全法》将成为我国互联网管理方面一部基础性的法律。《网络安全法》将之前一些网络管理方面的规定，例如网络实名制、网络安全等级保护制度等上升为法律要求，并提出设置网络安全审查制度、界定关键信息基础设施并加强对其进行重点保护、建立网络监测预警与应急处置机制等重要的制度和要求。《网络安全法》提出的制度和要求一旦实施，将对我国科技和互联网行业的业态产生重要影响，并可能影

响到金融、能源、交通、医疗卫生等公共服务领域企业的运作。目前《网络安全法》草案刚开始征求意见，尚待讨论和各类相关主体的反馈。我们将密切关注《网络安全法》立法的进展。

董　潇　合伙人　电话：86 010 8519 1233　邮箱地址：dongx@junhe.com
蔡克蒙　律　师　电话：86 010 8519 1255　邮箱地址：caikm@junhe.com

JUN HE BULLETIN

JUNHE

July 8, 2015

Telecommunication Law

Draft of Cyber Security Law Released for Public Comments

The National People's Congress Standing Committee released the draft Cyber Security Law ("CSL") on July 6, 2015 to solicit public comments[1] before August 5, 2015, after the first deliberation on June 26, 2015[2]. CSL was first included in the legislative plan of the 12th National People's Congress (which is in session from 2013 to 2018) in 2013[3] and was included in the annual legislative working plan of the National People's Congress Standing Committee since 2014[4], however, no further schedule of its adoption has been published.

The publication of the draft CSL is closely related to the National Security Law ("NSL") issued on July 1, 2015. NSL, for the first time, provides for "safeguarding the national cyberspace sovereignty", and adds cyber and information security as an important part of national security. NSL further requires the state to establish a national security review system to review matters and activities that influence or may influence national security, including that relating to network information technology products and services. The draft CSL further provides for "safeguarding the national cyberspace sovereignty" as a fundamental principle, and, for that purpose, the draft includes provisions on, *inter alia*, the strategy, plan and promotion of cyber security, network operation security, network information security, and alarm and emergency response systems.

Application Scope

According to the draft, CSL applies to the construction, operation, maintenance and use of the network and supervision and administration of cyber security within the territory of the PRC. "Network" includes networks and systems that are composed of computers and other information terminals and the relevant facilities and are used for purpose of collecting, storing, transmitting, exchanging and processing information in accordance with certain rules and procedures. A "network operator", an important subject of legal obligations under CSL, is defined in the draft as "the owners, administrators and network service providers which use the network owned or administrated by others to provide relevant services, including basic telecommunication operators, network information service providers and important information system operators (Art. 65)".

---

1 http://www.npc.gov.cn/npc/xinwen/lfgz/flca/2015-07/06/content_1940614.htm

2 http://media.people.com.cn/n/2015/0708/c40606-27269420.html

3 http://news.xinhuanet.com/politics/2013-10/30/c_117939129.htm

4 2014 Annual Legislative Working Plan of National People's Congress Standing Committee, http://www.npc.gov.cn/npc/xinwen/lfgz/2014-04/17/content_1859742.htm, 2015 Annual Legislative Working Plan of National People's Congress Standing Committee http://www.npc.gov.cn/npc/xinwen/lfgz/lfdt/2015-05/25/content_1936926.htm.

Responsible Authorities

The draft CSL provides that the national cyberspace administration authority, namely the Cyberspace Administration of China, is responsible for the coordination of cyber security work and the relevant supervision and administration work on a national level. It further provides that the Ministry of Industry and Information Technology, the Ministry of Public Security and other relevant government departments shall be responsible for the protection and supervision of cyber security within their respective authority (Art. 6).

Legal Requirements relating to Network Operators

The key provisions of the draft relating to network operators are summarized below.

- **Strengthened network operation security obligations.** The draft provides various security obligations of network product and service providers, such as not installing malware in products, informing customers of security defects and bugs, and providing constant security maintenance services for their products and services (Art. 18). Key network facilities and special products used for protecting network security shall comply with the relevant national standards and compulsory certification requirements, and may only be offered for sale after being certified by the qualified security certification authority or passing the relevant security tests (Art. 19). The draft also makes classified network security protection a legal obligation of network operators, which shall adopt measures including classifying data as well as backing up key data and encrypting the same (Art. 17). Network operators are also required to provide necessary assistance and support to investigation authorities where necessary for protecting national security and investigating crimes (Art. 23).

- **Security of key information infrastructure facilities.** The draft provides heightened protection for the operation of key information infrastructure facilities, in particular including (a) internal organization, training, data backup and emergency response requirements (Art. 28); (b) requiring key information infrastructure facility operators to store personal information of citizens and other important data within the PRC territory, in principle (Art. 31); (c) establishing security review requirements on the procurement of network products and services by key information infrastructure operators (Art. 30); (d) annual valuation of network security risks (Art. 31). "Key information infrastructure facilities" are defined as including the base information network that provides public communication, broadcasting and television transmission services, etc., important information systems in the public service sector including water and gas supply, medical treatment and healthcare and social security, etc., military networks, government networks of state organs of cities divided into districts and higher levels, and networks and systems owned or managed by internet service providers with a significant number of users (Art. 25). However, the draft CSL provides no specific explanations as to how such definition is to be applied, for example what circumstances would be deemed as providing internet services to a "significant number of users" and what types of internet services would be included.

- **Strengthened network information security.** The draft includes requirements

for network operators on the protection of personal information of users (Art. 34-Art. 38). Such requirements are primarily based on the requirements of existing laws and regulations, with a few new requirements such as notifying users who may be affected in the event of a data breach. The draft also requires network operators to record the real identity of users, to cease and prevent the dissemination of unlawful and harmful information, and to make records and report to government (Art. 20, Art. 40 and Art. 41).

- **Establishing network security alarm and emergency response system.** The draft requires the relevant departments of the State Council to establish a network security alarm and information report system, to establish a network security emergency response system and to formulate emergency plans. The draft also allows the State Council, or the provincial governments upon approval by the State Council, to restrict network communication for the purpose of safeguarding internet security and public order or dealing with major emergent social security accidents (Art. 44-Art. 50).

Legal Liabilities

The draft CSL provides a series of punishments for violations of the relevant provisions. Punishments, including monetary fines, suspension of business and making corrections, closing websites, repealing the relevant business permits and licenses, may be imposed on the basis of specific situations and the seriousness of violations (Art. 51-Art. 64).

Our Observations

Once adopted, CSL will be the first law in the PRC specially focusing on cyber security matters, in response to the increasing prevalent problems such as cyber invasion and attack, information leakage, cyberspace sovereignty and security, and it will become a fundamental law of the PRC in the administration of telecommunications and the Internet.

The draft CSL adopts some existing provisions on cyberspace administration, such as real identity requirements and classified data protection requirements, which were, in the past, scattered in implementing measures and rules as legal requirements. The draft CSL also introduces certain new important concepts and requirements, such as the establishment of a network security review system, the definition of key information infrastructure facilities and related strengthened protection, and the establishment of cyber security alarms and emergency response mechanisms. Once adopted and implemented, CSL may influence the technology and Internet industries significantly, and may even impact enterprises in finance, energy, transportation, medical and health services and other public service areas. At this stage, the draft CSL is only published for public comments and is still open to public discussion and feedback from the interested parties. We will follow the development of CSL closely.

Marissa (Xiao) DONG	Partner	Tel：86 10 8519 1233	Email：dongx@junhe.com
Clement (Kemeng) CAI	Associate	Tel：86 10 8519 1255	Email：caikm@junhe.com